2024

BIOMETRIC DIGITAL IDENTITY FLAGSHIP PRISM REPORT

A new paradigm for the emerging digital identity ecosystem.

the-prism-project.com

The Prism Project

ACUITY MARKET INTELLIGENCE

Thank You to Our Sponsors and Partners

The 2024 Flagship Biometric Digital Identity Prism Report is made possible thanks to the participation of our sponsors and partners. The biometric digital identity ecosystem depends on collaboration, and we are grateful to work with the following organizations.

SPONSORS

SITA
AWARE
KEYLESS
kantara INITIATIVE
incode
authID BIOMETRIC AUTHENTICATION
iiDENTIFii
AUTHENTICID
veriff
TECH5
ideem
inverid Creators of ReadID
IDENTY.IO
wicket
Anonybit
INNOVATRICS building a world of instant trust
ba
DESKO
IDEMIA
Daon
iProov
sodec TECHNOLOGIES
PANINI
veratad
iddataweb

PARTNERS

TECH
IDENTITYWEEK GLOBAL • TRUSTED • VISIONARY
PEAK iDV

The Prism is proudly independent. While participants benefit from increased visibility and vendor profiles in this report, sponsorship does not affect a vendor's evaluation of placement within any aspect of the Prism Project.

©Acuity Market Intelligence 2024: All rights reserved. www.acuitymi.com. The material contained within this document was created by and is protected under copyright by Acuity MI, LLC. The Author and Publisher do not guarantee the views, opinions, or forecasts contained herein. Non-sponsor vendors are not guaranteed inclusion. Sponsors are guaranteed inclusion but sponsorship has no impact on vendor evaluations and assessments. No part of this report including analysis, charts, forecasts, text extracts, quotes, nor the report in its entirety may be reproduced for any reason without explicit consent of Acuity Market Intelligence.

Table of Contents

Prism Ver. 1.0 © 2024 The Prism Project

Prism Ver. 1.0 © 2024 The Prism Project

Introduction

Welcome to the 2024 Flagship Edition of the Biometric Digital Identity Prism Report. This is the second annual flagship report dedicated to laying out the digital identity landscape with biometrics at the core. Collecting, collating, and analyzing the Prism Project's 2024 research into digital transformation as it intersects with identity in financial services, government services, and travel and hospitality, and generalizing the common findings more broadly across market sectors, this report aims to illuminate the complex and shifting ecosystem that is enabling safer and more convenient user experiences in every aspect of modern digital life.

The Prism Project was created by Acuity Market Intelligence to bridge the gap between the identity technology intelligentsia and the enterprise executives evaluating and deploying digital identity solutions to meet the challenges of digital transformation. It is built on the foundational premise that biometrics literally provide the link between humans and the digital world and therefore must be a core component of secure, reliable digital identity ecosystems, not a technology feature or capability attached at the edge. Utilizing a holistic framework informed by hundreds of vendor and relying party evaluations, the Prism Project is grounded in a philosophy of identity based on four key pillars:

- Digital identity belongs to the user it describes.
- True ID empowerment relies on government systems of record.
- Identity must be consistently and continuously orchestrated to remain secure.
- Biometrics must be at the core of any sustainable reliable, and secure digital ecosystem.

To achieve growth and improved profitability in the midst of the current state of technology-driven evolution, enterprises must meet the expectations of customers, their own workforce, and their own suppliers. As you will find in this report, those expectations each deal with digital identity. The continued evolution of global commerce therefore demands a trusted, reliable identity ecosystem that every enterprise and SMB can engage with and depend on.

Relying Parties:

- Financial Services
- Entertainment Venues
- Airlines
- Hospitality
- Government Agencies
- Healthcare and Hospitalis
- Gaming and Gambling
- Telecom
- Retailers (Including eCommerce)

Key Use Cases:

- Onboarding
- Authentication
- Identity Verification
- Reverification
- Automated Account Recovery
- Record Deduplication
- Transations
- Age Verification
- Compliance / KYC
- Physical and Digital Security
- Deepfake Defense
- Account Takeover Defense
- Ransomware Defense
- Financial Inclusion
- Government Inclusion
- Enhanced Customer Experience
- Improved Conversion Rates
- Membership and Loyalty Programs

Prism Ver. 1.0 © 2024 The Prism Project

In this report you will find:

- A holistic analysis of the biometric digital identity landscape.
- Original market forecasts from Acuity Market Intelligence, spotlighting the global opportunity for biometric digital identity, broken down by region and sector.
- An updated edition of the proprietary Biometric Digital Identity Prism.
- Evaluations of vendors, relying parties, and infrastructure organizations operating at the intersection of digitization and identity.
- Profiles of significant players in the biometric digital identity ecosystem.

This multimodal biometric-centric approach to understanding and evaluating the global digital identity ecosystem is the basis for creating this and all Prism Reports as practical tools for assessing the market, its opportunities, and the vendors providing the technology required to bring carbon life forms into online spaces.

Throughout this year, our investigations into key vertical markets have further refined our novel framework, thanks in particular to the addition of illustrative concepts like the Couch-to-Destination Guest Journey in the travel and hospitality market, and the Prism Identity Hierarchy, introduced to evaluate government services. Indeed, while this 2024 Flagship Prism Report does standalone as a broad industry overview, to get the most out of this document we recommend that you supplement it with our previous verticalized publications:

- The Financial Services Prism Report
- The Travel and Hospitality Prism Report
- The Government Services Prism Report

The Prism Project's intense market-focus has revealed digital transformation challenges, common to all markets, that can be addressed with orchestrated biometric technologies. Looking ahead to 2025, the Prism Project will evaluate the digital identity ecosystem through the lens of some of the most prominent of those shared critical issues, such as:

- Deepfakes and synthetic identities
- Privacy and compliance
- Customer experience and fraud

As ever, my collaborators and I are evangelists of strong identity and believe that the only way to safely move forward in our time of digital transformation is to take human identity seriously.

Download the 2024 Vertical Market Prism Reports:

Prism Ver. 1.0 © 2024 The Prism Project

By reading and sharing our vision of a secure, convenient, and privacy-first future of user-empowered identity, you are participating in the positive change required to close the hazardous gaps in our increasingly virtual lives and usher in a more intuitive future for all.

Sincerely,

Maxine Most

Founder
The Prism Project.

Prism Ver. 1.0 © 2024 The Prism Project

Executive Summary

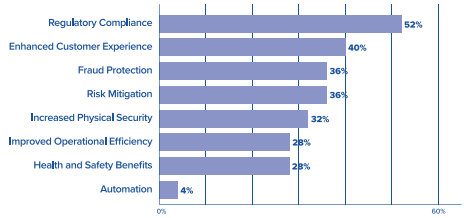
The 2024 Biometric Digital Identity Flagship Prism Report collects, synthesizes and generalizes The Prism Project's analysis and key findings from the financial services, government services, and travel and hospitality reports we published this year. In each of these verticalized Prism reports, we applied a holistic viewpoint to bring insight and clarity to this current moment of significant digital transformation. Our research distilled the role of biometric digital identity in the ways we spend money, interact with our governments, and travel through the world. In this report, we have collected and expanded our findings and highlighted common elements to offer a broader view of the global biometric digital identity market—its challenges and opportunities—and the future of digital life with biometrics at the core.

Total biometric digital identity revenue from 2024-2028 is expected to generate $315 billion globally, representing 5.6 trillion transactions.

Digital Transformation Around the Globe

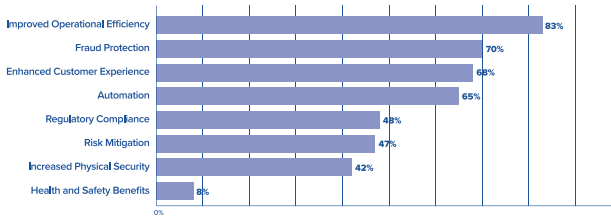
Digital transformation is impacting each vertical market in unique ways. However, the overall trends from our collated survey findings from relying parties in financial services, government, and travel and hospitality indicate regulatory compliance, enhanced customer experience, fraud protection, and risk mitigation are the primary motivations for adopting digital identity solutions. This is consistent with survey findings that reflect the widespread belief that digital identities can indeed protect against fraud and boost automation, while enabling regulatory compliance and enhancing customer experience. Interestingly, while there is an overall understanding that digital identity technologies have automation applications, that is the least cited reason these companies are adopting these solutions.

Which benefits of digital transformation motivate your organization to adopt new digital technologies?



The Prism Project also surveyed vendors and stakeholders in the biometric digital identity industry that predominantly serve financial services, government services, and travel and hospitality markets. The results, when compared to the relying party data, reveal that the companies providing identity solutions for companies undergoing digital transformation see improved efficiency, fraud protection, enhanced customer experience and automation as the top motivators for adoption. Regulatory compliance, surprisingly, ranks lower. This reveals an interesting dissonance, with vendors perhaps overvaluing the automation capabilities of digital identity while underappreciating the technology's capabilities in terms of enabling compliance.

Which benefits of digital transformation motivate your customers to adopt new digital identity technologies?



Prism Ver. 1.0 © 2024 The Prism Project

Whatever the reasons for adoption, in terms of market growth, the global view of biometric digital identity is positive for all involved stakeholders. The Prism Project is powered by Acuity Market Intelligence, which has developed proprietary market models for each of the three verticals analyzed in 2024. The five-year outlook from 2024 to 2028 illuminates an incredible potential for biometric digital identity solutions during the digital transformation market evolution. The opportunity is massive and global in scale.

In financial services, nearly 1.2 trillion transactions are projected for the forecast period, generating $40 billion globally. North America leads in revenues with 35% of the market share, followed closely by Europe and Asia Pacific. APAC, will lead in transactions, contributing 48% of the global volume.

In travel and hospitality, 262 billion identity transactions worldwide are forecast to generate a total of $72 billion in revenue, with Asia Pacific leading in transaction volumes, followed by North America and Europe. Air travel will be responsible for nearly half of the market share, followed by hotels and resorts, which are expected to generate 33% of that total revenue. Theme parks will contribute 11% to the market, while more targeted destinations like stadiums, arenas, casinos, and conference venues will account for the remainder.

Finally, in government services, the Total Addressable Market (TAM) for biometric digital identity is projected to reach approximately $295 billion over the forecast period with Europe contributing the largest share. That's powered by a 6.4 trillion transactions, with Asia Pacific generating half of that traffic. About 57% of those transactions are expected to materialize, generating an actual $202.5 billion in global revenue (representing 69% of the Total Addressable Market) spread relatively evenly between North America, Europe, and Asia Pacific.

All of this is to say, digital transformation is increasing the number of ways users can transact with public and private sector organizations around the world. And with so many of these transactions necessitating a biometric verification, identity is becoming central to all aspects of life. The market stands to benefit greatly, but so do the users this technology protects.

Prism Ver. 1.0 © 2024 The Prism Project

Biometrics Beyond the Checkbox

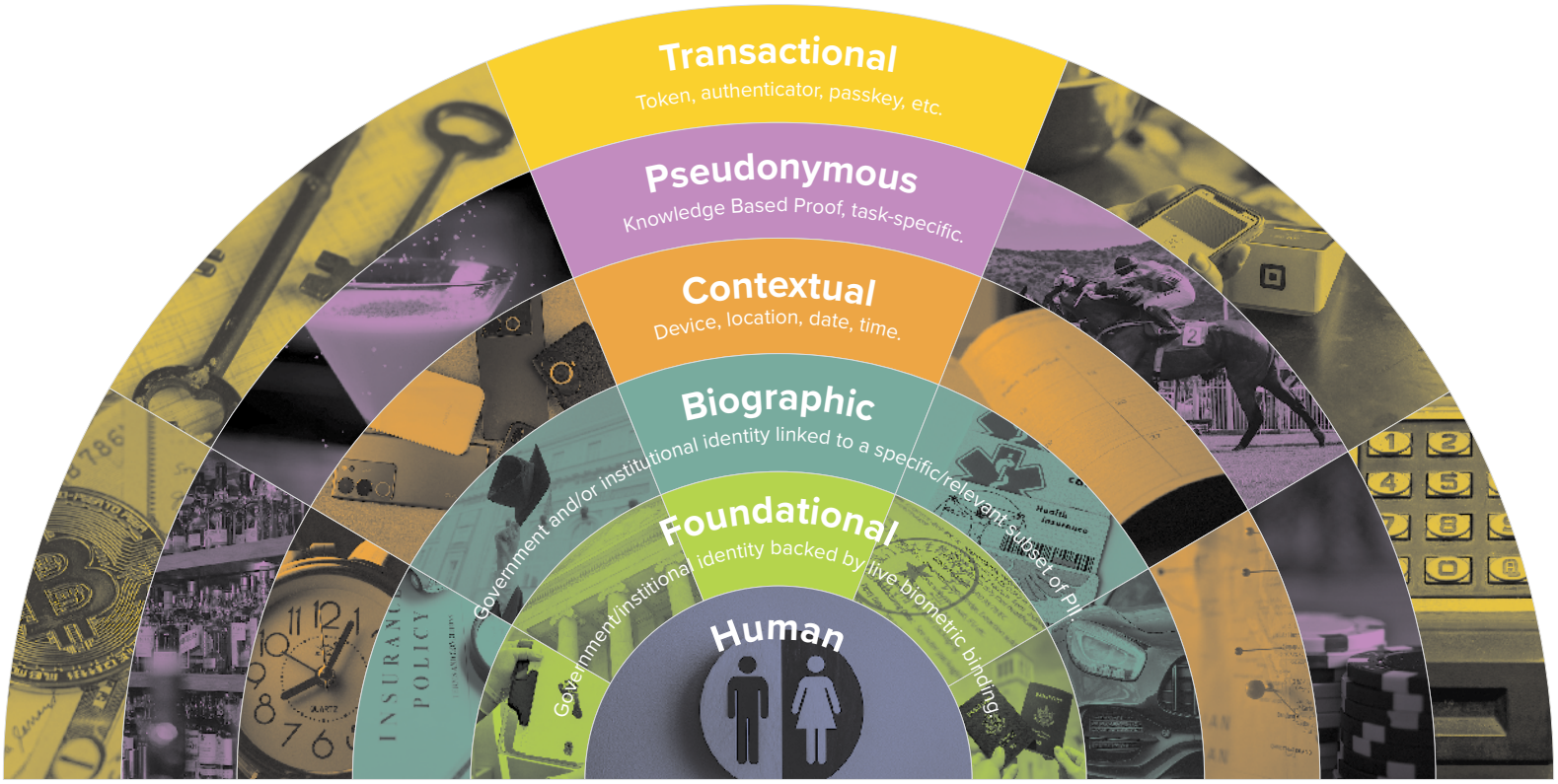
Regulatory compliance is among the eight significant digital transformation challenges shared between the Prism Project's focus markets for 2024. Many of the vendors profiled in the evaluations section of this report offer turn-key compliance solutions, and some have even developed future-proof products for addressing this challenge—technologies that forgo the storage of biometric data altogether and rely on biometrics on-demand. That spirit of going beyond the regulatory checkbox is increasingly common in the biometric digital identity landscape as illustrated in this report.

In addition to compliance, fraud continues to be an active and costly challenge, especially in the age of AI-empowered scammers and easily accessible deepfake technology. Operational efficiency is proving an obstacle for organizations struggling to manage digital channels in addition to the physical ones they continue to maintain. Security and privacy remain paramount as digitization increases the likelihood and severity of cyberattacks and users struggle to control their sensitive information. And these concerns aren't going away. Driven by customer demand, there is no getting off the digital transformation train. The challenges inherent to digitization are non-negotiable, but thankfully there is a solution: biometric digital identity.

Prism Ver. 1.0 © 2024 The Prism Project

The Prism Identity Hierarchy

To understand how biometric digital identity is capable of solving the challenges presented by digital transformation, it is crucial to understand how various types of information and transaction work in relation to a human being. To illustrate this, the Prism Project has built the Identity Hierarchy model, which premiered in our 2024 Government Services Prism Report and is referenced throughout this document.



The model shows multiple strata radiating out from the human at the center of the hierarchy, representing how far removed a level of identity is from the carbon lifeform it is supposed to represent. Crucially, while ascending the hierarchy, the human identity is carried forward from level to level. The same cannot be said from the top down. For each level to carry the assurance of a human being's true identity, that identity must stem from levels before it. For example: biographical identity can only be fully trusted as belonging to the human claiming it when it is built on the foundational identity underneath it, which is bound to the human through biometrics.

Prism Ver. 1.0 © 2024 The Prism Project

But what does that foundational biometric binding look like in practice? It only requires two elements: a human and a government issuing authority. The government is the arbiter of the most authoritative and definitive identity data describing a document holder. But the credentials it issues are still one step removed from the actual object of the identity (ie. the person it identifies). This becomes a serious problem when transacting over remote channels, because the documents and the information therein can be presented by impersonators, by virtue of their transferability. By collecting the document holder's biometrics and binding the resulting template to the foundational identity documents issued by the government, the cornerstone of identity is created.

That biometrically-bound foundational identity is the basis for the next two additive layers of the Hierarchy: biographical, based on what a person has done (where they have lived, what they have accomplished); and contextual, based on where they are and what they are doing now. These layers of the identity hierarchy build on the foundation of a government-vetted real human identity to give permissions like driving vehicles or accessing online portals, and to enhance assurance.

On the outer layers of the hierarchy, we see the privacy enhancing and practical aspects of identity. Unlike the layers underneath, the pseudonymous layer doesn't add data to build the identity up, but obscures what is there so that a person is only asserting the parts of their identity they want to. For age restricted substances like alcohol or cannabis, or regulated services like gambling, pseudonymous identity represents the act of confirming you have permission to participate without having to share the actual information that proves it.

The outermost layer, transactional identity, represents access. This is the identity of keys and locks, passwords and login pages, payments and purchases. In digital spaces, we are most familiar with transactional identity because, as the outer layer of the hierarchy, the actions it represents can be performed without the deeper layers of identity. That is to say: transactions can be performed without trust, security, or privacy. While that might be the case when using knowledge-based authentication (KBA) or security tokens and passkeys that have no foundational element, when supported by the full identity hierarchy, transactional identity can be asserted with greater ease, benefit from stronger security, and be easily recovered.

With the full spectrum of the Prism Identity Hierarchy behind it, as enabled by government organizations and the infrastruc-

Six Levels of the Prism Identity Hierarchy:

- Human
- Foundational
- Biographical
- Contextual
- Pseudonymous
- Transactional

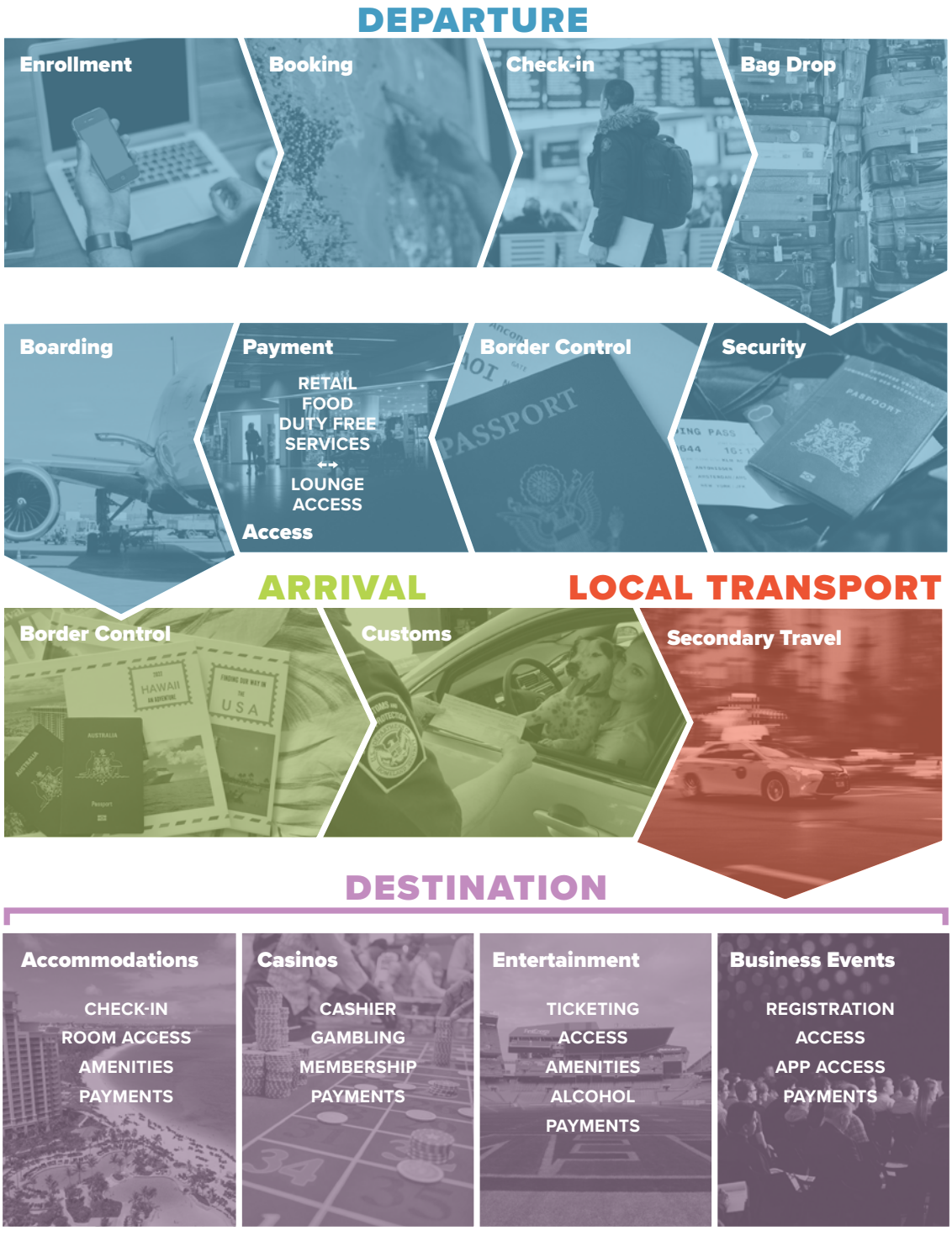
Prism Ver. 1.0 © 2024 The Prism Project

ture supporting them, biometric digital identity can meet the extremely wide-ranging demands of private and public sector organizations and the citizens, businesses, and consumers they collaborate with and serve. Using the hierarchy as a guide, we can see how digital identity, when supported by biometrically-bound foundational ID, can facilitate the various digital and physical transactions required by modern life. And to see that at work, we need look no further than the modern travel and hospitality experience.

Prism Ver. 1.0 © 2024 The Prism Project

The Guest Journey

The journey undertaken by modern travelers between their homes and their destinations is the perfect example of how we use identity as we navigate various facilities, transaction types, services, and technologies. The Prism Project has refined this journey into an intuitive flow. Unveiled in the 2024 Travel and Hospitality Prism Report, this is the Couch-to-Destination Guest Journey:



Prism Ver. 1.0 © 2024 The Prism Project

While the minutia of each touchpoint is complex—with security screening, access, and payments all at play in different phases—the underlying identity principle represented by this model is elegant. Anchoring a guest's foundational identity at the beginning of their journey through the use of biometrics allows every subsequent transaction to reference their enrollment and carry forward the assurance that they are who they claim to be. The ideal guest journey is not a complex web that a user must navigate as the cost of doing business, it's a unique and personalized straight line from couch-to-destination, maintained by the trust, security, and privacy of biometrics at the core.

As a guest moves through the journey, they ascend and descend the Identity Hierarchy as they interact with each touchpoint. The Guest Journey requires everything from foundational and biographical identity to transactional and potentially pseudonymous identity, depending on the various requirements of their preferred activities. It is not difficult to transpose this guest journey to the way we move through the world in day-to-day life when we aren't traveling by plane. Every time you leave your house, log on to your computer, or open up your phone, you are embarking on a new, unique identity journey. Whether it's safe, secure, and convenient depends on the technology in play and how it facilitates the assertion of your identity data.

A Unified Theory of Identity

Moving through the world and negotiating various relationships with merchants, public services, workplaces, utilities, and each other, we are constantly transacting using identities, whether we are aware of it or not. The technologies showcased in this report ensure our identities are trustworthy, reliable, safe, and under our control, every step of the way.

By taking a holistic view of digital transformation, concepts of identity begin to overlap and we can start to see how human beings fit in our increasingly virtual society. When implemented thoughtfully, with liveness detection, orchestration, and trust rooted in foundational identity, biometric digital identity is the bridge that can successfully bring people into the digital ecosystem growing all around us. We are on the brink of witnessing the next generation of community, orchestrated and secured by the leading vendors represented in the Biometric Digital Identity Prism.

Prism Ver. 1.0 © 2024 The Prism Project

How to Read the Prism Report

The 2024 Biometric Digital Identity Flagship Prism Report is divided into six sections:

Digitization Trends

The first section collects and analyzes the results of a survey examining how digital identity organizations view the role of identity in their customers' digital transformation journeys. This data is compared to results from complementary vertical market surveys focused on digitization in financial services, government, and travel and hospitality. **This high-level content is the starting point for the Biometric Digital Identity Prism.**

The Prism Lens (Challenges and Solutions)

The second section draws on aggregate industry research from leading analysts, government organizations, and NGOs such as McKinsey, Deloitte, GSMA, Kaspersky, World Bank, and Fenegro, as well as trusted international news sources. It provides a holistic visualization of eight core digitization challenges shared across vertical markets, then breaks them out individually to demonstrate how biometric digital identity can address them. The graphic visualization is supported by further written analysis. **The pain points highlighted in the Prism Lens serve as the basis for the practical applications of biometric digital identity technology profiled later in the report.**

Market Forecasts

The third section presents original proprietary market research from Acuity Market Intelligence, forecasting the total global revenue and transactions volumes for biometric digital identity, broken down by region and vertical. **The charts depict the immense market potential for the vendors, relying parties, and identity titans in the current four-year period.**

The Prism

The fourth section is the proprietary biometric digital identity industry ecosystem framework: The Prism. This version of

Prism Ver. 1.0 © 2024 The Prism Project

the Prism is fine-tuned to show how various biometric digital identity parties collaborate with relying parties and infrastructure players in a landscape defined by identity titans. . **The Prism is a living research program, providing a framework for understanding how the digital identity community is working together to fight fraud, improve user experience, and empower people.**

Evaluations and Profiles

The fifth section lists the vendors depicted in the Prism framework next to their evaluations. Each vendor is evaluated in context—based on their capabilities, accomplishments and market aspirations—and grouped according to their Prism Beam. After each set of evaluations profiles are presented to demonstrate how the solutions offered by sponsors of this report can address the challenges identified in the Prism Lens section. **The evaluations and profiles demonstrate how digital identity vendors currently operate in the biometric digital identity ecosystem.**

The Prismatic Future of Identity

The sixth and final section contains strategic guidance and recommendations based on this report's research. It also contains author information, an overview of The Prism Project, and ways to get involved with future iterations of the Prism, including 2025 reports focused on deepfakes and synthetic identity, compliance and privacy, and user experience and fraud. **The conclusion lights your way to the next steps on your digital identity roadmap.**

Each section of this report stands on its own, but taken together the end-to-end report offers a unique, comprehensive view of the current state of digital identity and the massive potential for its biometrics-enabled future.

Prism Ver. 1.0 © 2024 The Prism Project

Digitization Trends and the Identity Landscape

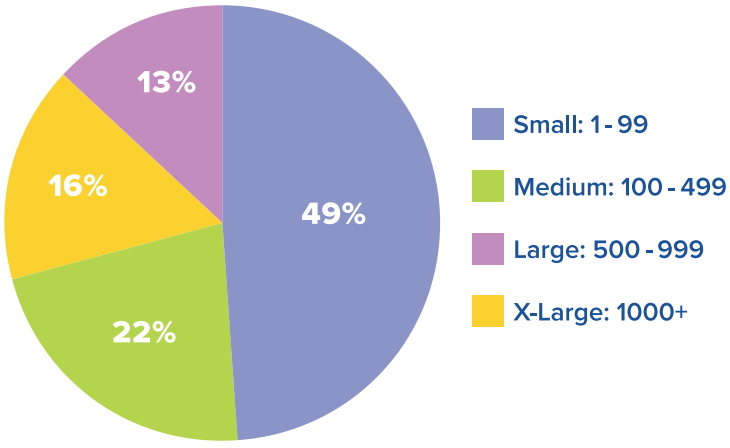
The Prism Project emerged from survey data comparing how biometric digital identity vendors' perception about identity's role in digital transformation lined up with the experience and views of end users in vertical markets. Enhancing customer service, reducing fraud, and creating operational efficiency were identified as main adoption priorities for both vendors and end-users, and data showed a prevailing support of converged physical and digital access. At large, we found biometric digital identity was moving from a paradigm of application-based point solutions to a holistic concept based on human users navigating digital spaces with a single ID.

For 2024, we once again polled vendors in the biometric digital identity space, as well as relying parties in financial services, government services, and travel and hospitality.

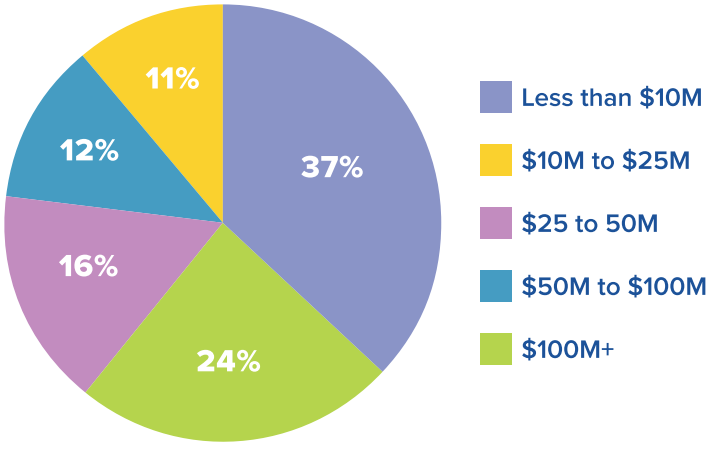
Survey Scope: The Vendors

The Prism Project's 2024 digital transformation survey reached vendors and organizations operating in the biometric digital identity space. With annual revenues running the gamut, nearly half of identity industry respondents hailed from small organizations, reflecting the continued preponderance of startups in this space. Meanwhile, 29% of surveyed vendors have more than 500 employees.

How big is your organization?



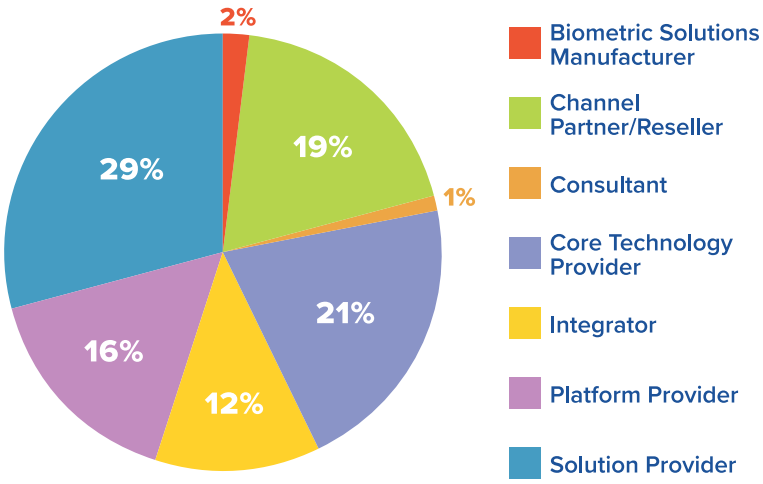
What is your organization's annual revenue?



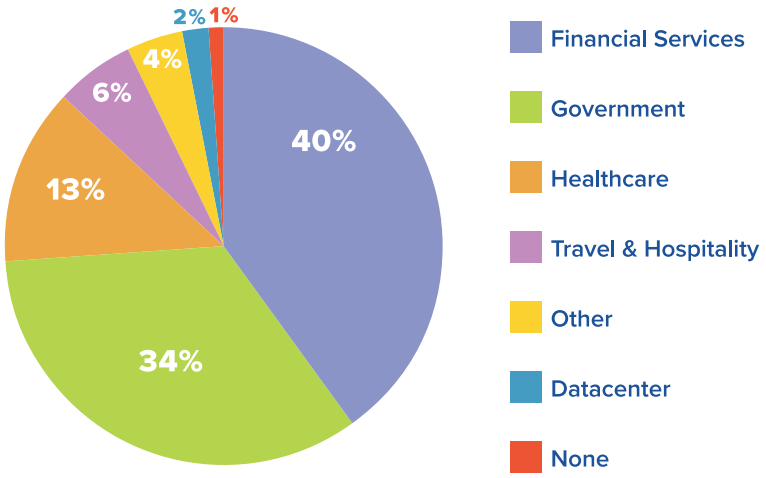
Prism Ver. 1.0 © 2024 The Prism Project

The organizations surveyed included players from the full spectrum of identity players—from solutions and platform providers to resellers and integrators—and their highest priority markets are financial services and government.

How do you primarily characterize your organization's relationship to digital identity technologies?

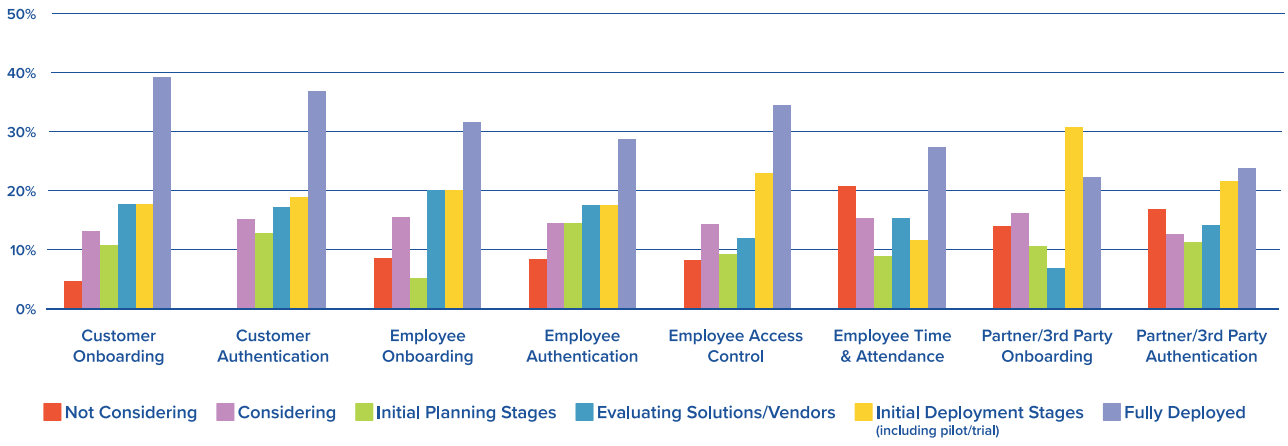


What are your organization's highest priority markets?



The customers the surveyed organizations serve in those priority markets are in various stages of deploying digital identity solutions as they undergo digital transformation. Customer-facing applications and employee access control have the highest rate of full deployment, while identity solutions for partner and 3rd party applications seem less of a priority. Employee time and attendance is the application with the lowest interest, short-term contracts, and gig work.

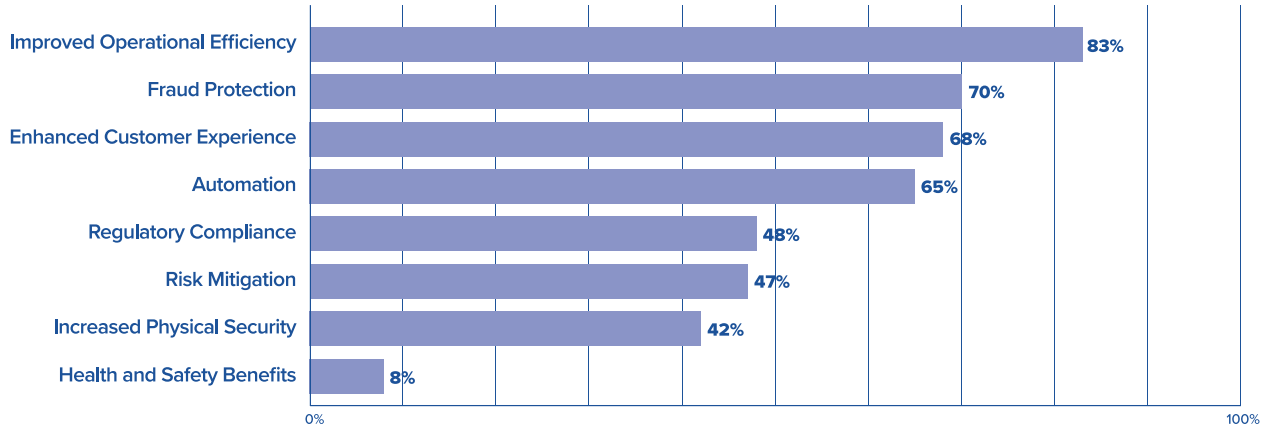
Where would you place the following processes on your customers' digital identity roadmaps?



Prism Ver. 1.0 © 2024 The Prism Project

From the vendors' perspective, that adoption of digital identity technologies is motivated by a desire for improved operational efficiency and fraud protection, as well as enhanced customer experience and automation. Fascinatingly, regulatory compliance—a costly challenge for relying parties that can be easily solved by biometrics—is not widely seen as a motivator.

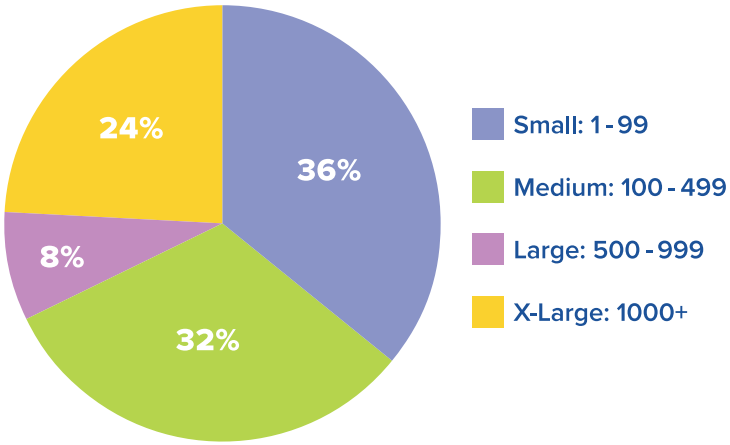
Which benefits of digital transformation motivate your customers to adopt new digital identity technologies?



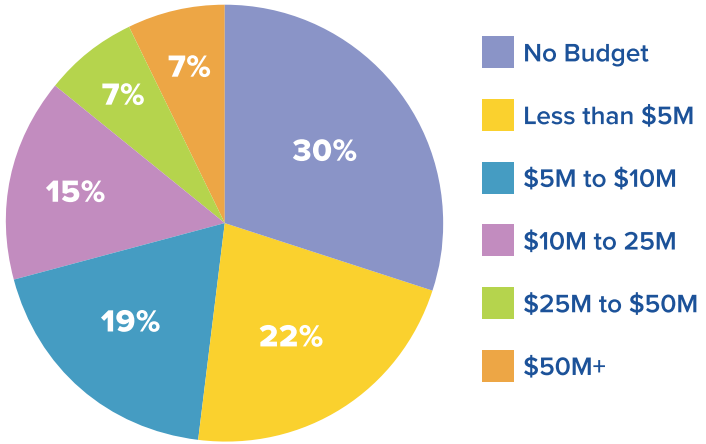
Relying Parties

To compare and contrast the identity organization perspective, The Prism Project also polled professionals from key vertical markets identified as having the greatest potential for biometric digital identity adoption. Spanning financial services, government services, and travel and hospitality, the group represented stakeholders of all sizes, with modest-to-no budgets for digital transformation projects.

How big is your organization?

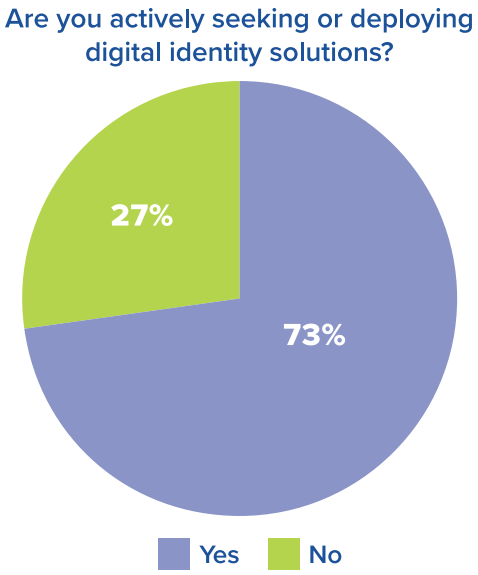


What is your approximate budget (in USD) for digital transformation projects for 2024 and 2025?



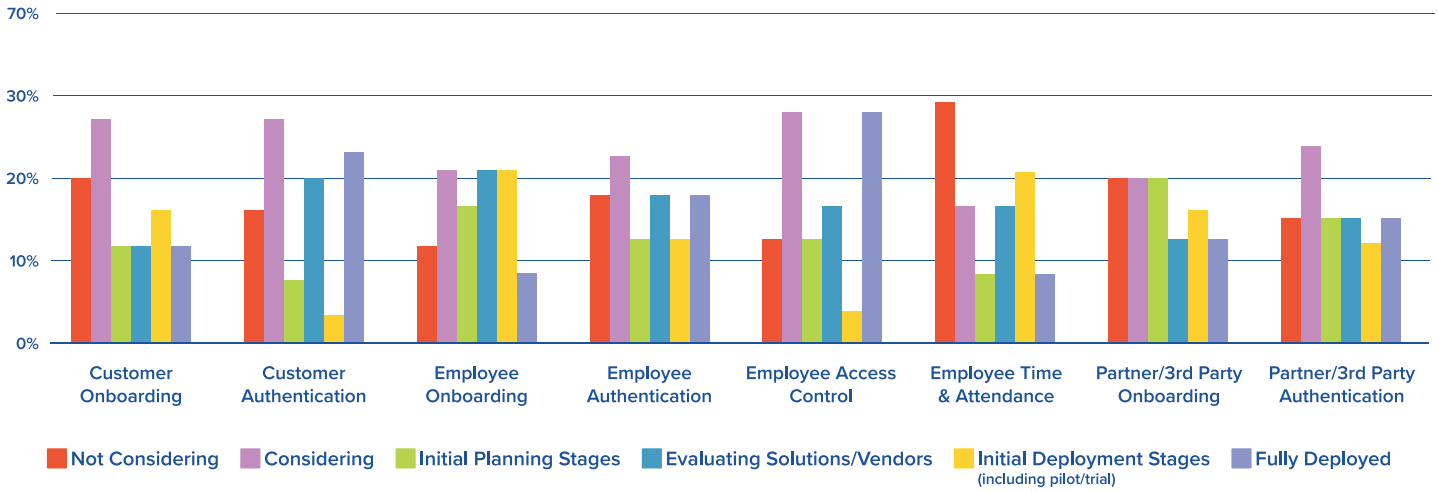
Prism Ver. 1.0 © 2024 The Prism Project

Those budgetary constraints are notable, because nearly three quarters of relying party respondents report that they are actively seeking or deploying digital identity solutions.



As for how they are deploying digital identity solutions, we see the strongest uptake in authentication and access control for customers and employees, with onboarding applications gaining traction in the consideration and evaluation phases. Lining up with identity vendor perceptions, employee time and attendance is low priority. Given the historical prominence of time and attendance as an application of biometrics, this represents a generational shift in how digitization is affecting how we work and why we transact using identity.

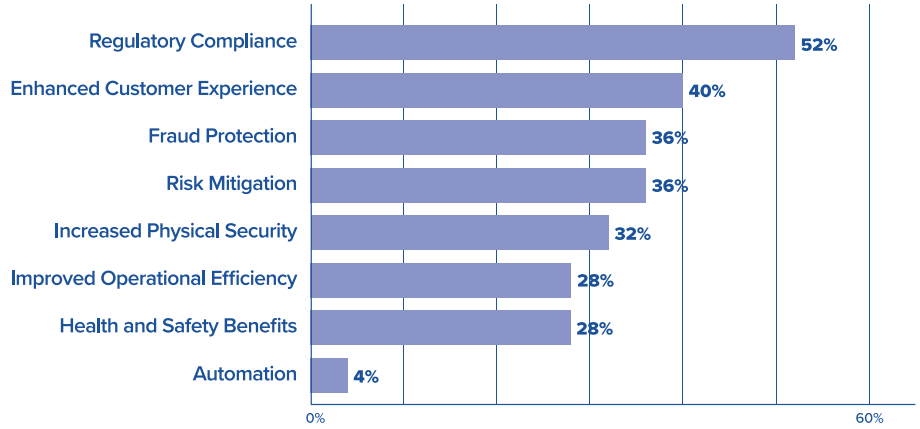
Where would you place the following processes on your digital identity roadmap?



Prism Ver. 1.0 © 2024 The Prism Project

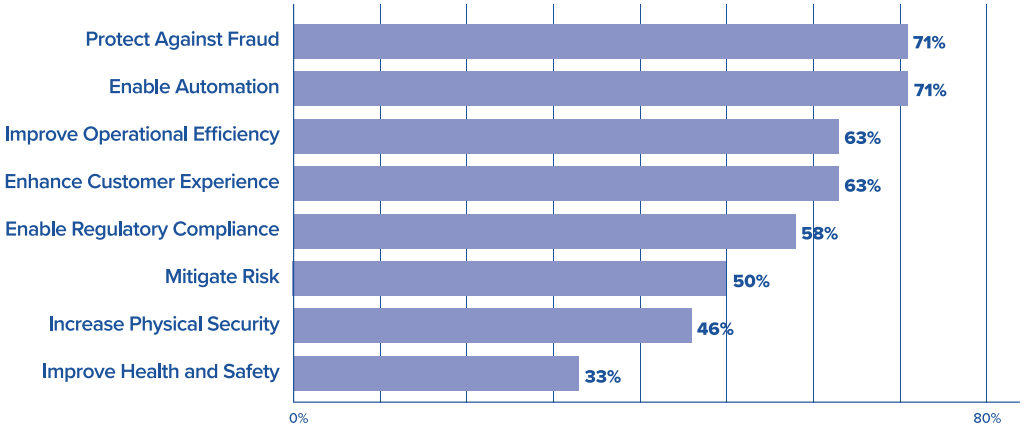
As for why relying parties are adopting digital identity technologies, we see that regulatory compliance is the primary motivator, while automation barely registers. This contrasts significantly with the perspective reported by identity vendors in the previous subsection, which illustrated a viewpoint that automation was a stronger adoption driver than compliance, which was rated poorly.

Which benefits of digital transformation motivate your organization to adopt new digital technologies?



To add further context, we have insight into the confidence that relying parties have regarding digital identity solutions' efficacy in a variety of application areas. Interestingly, the most cited reasons for adoption—regulatory compliance and enhanced customer experience—are middle-of-the-road when it comes to relying party confidence. High confidence in digital identity's ability to enable automation, meanwhile, has no evident correlation to relying party adoption.

Mostly confident that digital identity solutions can:



The key takeaway from this exercise in perspectives on digital identity is that certain identity related challenges are significant enough to relying parties that they are adopting technologies even with medium level confidence. This phenomenon of need preceding confidence will be important to keep in mind as we dig into the challenges in the coming sections of this report.

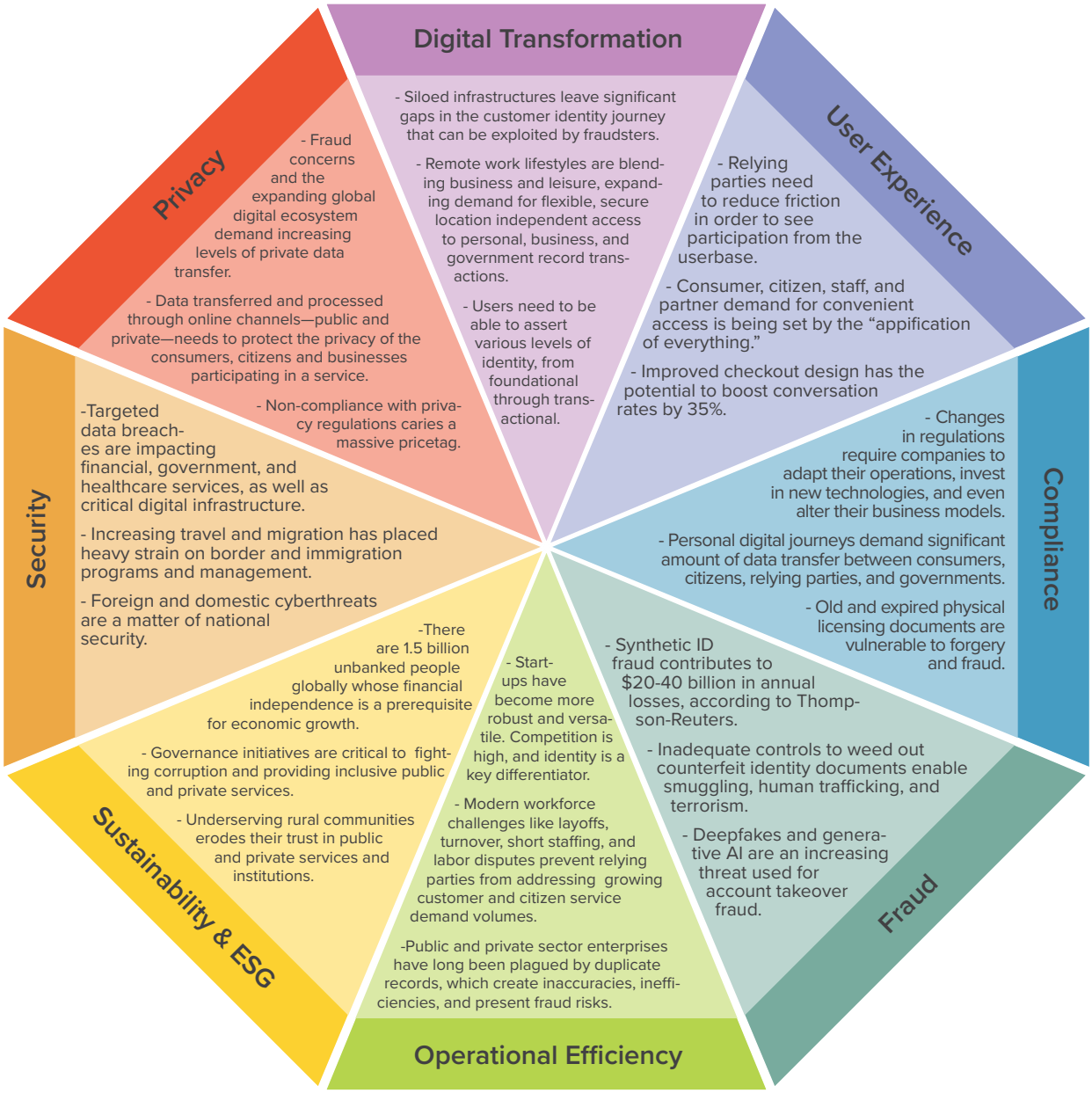
Prism Ver. 1.0 © 2024 The Prism Project

The Prism Lens

To understand how the broad benefits of biometric digital identity can be applied to critical market challenges, we use the **Prism Lens.** As with our vertical Prism Lenses, each segment of the octagon represents one significant market challenge.

In each of our previous vertical reports—financial services, travel and hospitality, and government services—these challenges were highly targeted and vertically specific. For the Flagship, we have generalized the challenges to fit more broadly and to be relevant across all key global vertical markets.

By understanding each of these challenges holistically through the Prism Lens, we can see common obstacles on the path to achieving the end-to-end user journey.



Prism Ver. 1.0 © 2024 The Prism Project

Biometric Solutions

Biometric digital identity solutions can be applied to each segment of the **Prism Lens** to address the digital transformation challenges faced by stakeholders across vertical markets as securing and effectively engaging in the global digital ecosystem becomes table stakes for 21rst century private and public sector enterprises. For each challenge below, biometric digital identity solution examples are drawn from a range of high impact market sectors.

Digital Transformation

- Orchestrated biometric digital identity platforms eliminate data silos, closing identity gaps and paving the way for innovative new products and services.

- Leading relying parties—like arports—rely on biometric digital identity to deliver on new customer demands.

- Biometric digital identity puts users in control of how much identity data they share in a given transaction, whether it's high risk, low risk, personal or pseudonymous.

User Experience

- Biometric digital identity technology removes friction from enrollment and authentication processes, making transactions as smooth as looking into a camera, scanning a fingerprint, or tapping a phone.

- Biometric digital identity reduces time customers need to spend on administrative and security procedures allowing them to focus on the experience they purchased.

- Biometric digital identity makes transactions intuitive, solidifying trust and improving conversion rates along the way.

Compliance

- Biometric solutions enable fast and effective know your customer (KYC) and anti-money laundering (AML) compliance.

- Decentralized biometric digital identity solutions supported by government systems of record prioritize user consent in data sharing.

- Biometric digital identity allows for remote renewal of licenses and doesn't leave a paper trail of expired documents.

Operational Efficiency

- Relying parties benefit from heavily orchestrated, easy-to-implement technology that can enable digital services securely and with natural compliance.

- Remote onboarding and check-in offloads front of house burden, while increased automation onsite reduces workloads for customer-facing staff and security.

- Binding identity data to a biometric means that all government records can be coalesced and linked to a single human being via a 1:N search and match process.

Fraud

- Identity verification solutions weed out counterfeit documents preventing travel of uncleared passengers.

- Biometric IDV technology at the first user touchpoint ensures that the person enrolling is who they claim to be, while 1:N search functions can clear up databases that already contain synthetic accounts.

- Liveness detection can spot AI generated impersonations and reject them from logging into an account.

ESG & Sustainability

- Biometric digital identity lowers barriers to economic participation, empowering users to open accounts and transact with trust wherever and whoever they are.

- The best biometric technologies are unbiased, facilitating equal treatment for users at all levels of participation.

- Biometric digital identity enables equal service and participation for all citizens, fostering trust through inclusion.

Security

- Cyberattack threats are solved by replacing authentication mechanisms from vulnerable passwords and tokens with biometrics.

- Biometric digital identity solutions such as Digital Travel Credentials maintain border security, improve the customer experience and focus limited human resources on potential critical threat

- Biometric digital identity protects networks through strong authentication and unimpeachable audit controls, ensuring every moment of access can be traced to a specific, authorized human being.

Privacy

- Centralized gallery-of-the-day approaches to biometric storage purge consumer and customer data at regular intervals, while enabling high levels of intelligent friction.

- With foundational identity bound to human biometrics, transactional an pseudonymous activity still benefits from the highest levels of trust while protecting a user's PII.

- Decentralized biometric digital identity solutions supported by government systems of record prioritize user consent in data sharing.

Prism Ver. 1.0 © 2024 The Prism Project

Looking through the Prism Lens

Taking a closer look at the challenges and solutions represented by the 2024 Flagship Prism Lens, and applying powerful concepts like the Prism Identity Hierarchy, reveals how integral identity is in this era of widespread digitization. We apply insight from our 2024 vertical market research to frame this analysis of how identity has become central to the way we transact—how we travel, how we spend money, how we engage with government—and as digital technologies blend those activities between physical and online channels, how we increasingly find ourselves in need of biometric digital identity.

Digital Transformation

Digital transformation is largely driven by a demand for convenience and efficiency, which traditionally runs counter to principles of security and safety. In the online realm, security and safety are directly correlated to identity data—how it is collected, stored, managed, and matched. In the financial services space, enthusiastic adoption of digital technologies like AI, blockchain, and mobile banking help streamline existing operations and offer new products in the name of better serving customers. To date, the industry has built patchwork identity controls out of various point solutions without orchestration. The average financial institution uses about nine discrete solutions to manage identity, resulting in siloes of user data. It's the gaps between those siloes—and for many established players the reliance on archaic legacy core IT systems—that are vulnerable to modern fraudsters.

The average financial services firm is deploying solutions from ten or more vendors to build a custom identity stack across a number of data silos, according to Jenna Hoffart, an investor at 9Yards Capital. In 2022, she noted the emergence of orchestration players that can address the unnecessarily complex nature of this load-out.

The public sector faces the same challenge, but on a grander scale, and compounded by the burden of restrictive budgets, bureaucratic processes for funding and approval, and its own reliance on legacy systems. A digitized service needs to be vetted, approved, and implemented successfully without disrupting the current services being offered, but it also needs to consistently and accurately verify user identities. Without biometrics at the core, and without proper orchestration, vulnerabilities flourish.

Silos within a single relying party's identity management system are a challenge of their own. But when we look to the travel and hospitality sector, we can see how a lack of orchestration inevitably leads to poor customer experiences, threatening to make the

Prism Ver. 1.0 © 2024 The Prism Project

entire endeavor of digitization redundant by introducing interstitial friction between transaction types.

The service gap between seamless guest experiences and legacy friction illustrates this best. Entry into events venues or airport terminals is being streamlined, but access to amenities like concessions, merchandise, and VIP areas like lounges or private boxes operate in their own silo. Outside of the facility ecosystems, traveler and guest journeys experience uneven levels of friction between modes of travel, types of services, and categories of destinations. The challenge faced by travel and hospitality relying parties is how to facilitate the seamless transfer between touchpoints to enable a full couch-to-destination journey that's consistent.

The solution to this silo challenge can be found by introducing the foundational level of the identity hierarchy. With a digital ID, supported by a government system of record and bound to a human being with biometrics, the groundwork is set for allowing users to traverse those gaps, whether they are present in a single relying partly like their bank, or across a variety of touchpoints managed by multiple stakeholders, as we see in an airport. Interoperability and standards play an integral role in the future of this concept, which will empower users to easily and securely transact with trust, without being subject to the vulnerabilities of silos and identity half-measures.

User Experience

User experience drives digital adoption, and it is often framed in terms of prioritizing customers by putting them in control of their identity data. While this empowerment is beneficial, it is important that relying parties aren't simply offloading work or liability onto the consumer, especially when that burden can be automated. As we have seen with widespread disregard for password and 2FA best practices, when identity security is onerous, the end user frequently choses convenient risk over laborious security.

Biometric digital identity technologies can ease account creation, checkout, and form-filling, removing user friction while enhancing security. This is especially true on mobile, which accounts for 76.16% of abandoned carts globally, according to Dynamic Yield.

In the financial services space, we see the business case for user experience in the area of eCommerce conversion rates. Research from The Baymard Institute shows that an average large-sized eCommerce website can gain a 35% conversion rate simply by improving its checkout design. Broadly speaking, that conversion rate has the potential to bring in $260 billion in the EU and US alone.

In the highly competitive travel and hospitality industry, meanwhile, the customer base is largely motivated by their

Prism Ver. 1.0 © 2024 The Prism Project

attitudes on prevailing trends in leisure and business. And their choices define the market. In the 2024 Travel and Hospitality Prism Report we found these trends included a desire for customization, seamless experiences, an increased awareness of health and wellness, concern for eco-friendly practices, and remote work lifestyles that allow travelers to combine business and leisure for extended trips and working vacations.

Traveler dissatisfaction with high-friction travel touchpoints has increased 4-6% year over year, according to SITA's 2023 Passenger IT Insights report.

Likewise, government agencies must also appeal to user experience. That means reducing friction without compromising security. A big part of that is minimizing the number of onboarding touchpoints. When a citizen needs to re-enroll for a new government service, not only does the process contribute to inefficiency and expand the fraud surface by adding another onboarding touchpoint, it introduces another obstacle between the person and their service.

With a biometric digital ID, a single enrollment can be used to bind a citizen to their foundational identity, and from there expand to encompass the entirety of modern identity, from biographical details to contextual circumstances and beyond. In financial services, that means being able to checkout without the added friction of manual account creation. In travel and hospitality, that means fewer barriers between users and the experiences they most desire. The use of biometric digital identity, from a consumer standpoint, feels natural and frictionless, which, thanks to the security of biometrics and modern liveness detection, doesn't come at the expense of safety or security. And in government services, putting biometrics at the core of citizen life means a person can confidently and easily assert their identity across a variety of use cases, in person or online, without needing to reintroduce themselves every time they encounter a new branch of government.

Compliance

Compliance with data privacy regulations is a major challenge for all organizations undergoing digital transformation, but especially those that deal with outside end users like customers. How and when a relying party captures, transfers, stores, and deletes user data is subject to an increasingly large set of rules. And those rules are stringent and enforced by heavy non-compliance fines.

In travel and hospitality, these regulations can present sizeable hurdles, given the significant amount of data transfer between users, governments, and corporate entities required to facilitate

Prism Ver. 1.0 © 2024 The Prism Project

a seamless guest journey. But the challenge of compliance is severe in simpler ecosystems too. In 2023, financial institutions around the world faced $6.6 billion in penalties for not complying with KYC, AML, ESG, and CDD regulations.

The government agencies that administer these non-negotiables aren't immune to them, either. Regulations like GDPR, PSD2, and CCPA have sharp teeth when it comes to taking reprisal on non-compliant organizations. For instance, in the European Union, individuals can claim compensation if they suffered a material or non-material loss as a result of a public body running afoul of GDPR.

Biometric digital identity solutions built with privacy by design concepts can enable regulatory compliance on all of these fronts, while also giving users more control and visibility regarding their information. When a user's digital identity is biometrically bound to a government system of record, they naturally adhere to the principles behind KYC and AML regulations, which demand relying parties transact with trusted customers. Meanwhile, mobile and digital IDs eliminate the need for weak authentication controls that risk running afoul of authentication laws. And data hygiene practices are made simple when a 1:N biometric search can help ensure duplicate accounts are merged or deleted as needed

"...biometric identification will strengthen security and enhance facilitation with more accurate passenger information. This will, in turn, reduce the number of inadmissible passengers with improper documentation and the chances of human error in letting wrongly documented passengers fly."

- Yvonne Manzi Makolo, Chair of the IATA Board of Governors

Fraud

Overtly identity related threats are on the ascent, thanks to digitization trends. Just look at the financial services sector, where AI-empowered scammers stole $1.2 trillion globally between 2022 and 2023. In the travel and hospitality space, meanwhile, we see the threat of fraud turn dangerous. The proliferation of fake IDs plagues both international and domestic travel, with mass produced counterfeits able to pass most human inspections—a vulnerability helping fuel smuggling, terrorism, and human trafficking. Without fraud controls to weed out bad actors, watchlist programs are left to flounder while both citizens and businesses are at risk of experiencing devastating financial consequences.

And that's not to mention synthetic ID fraud, which according to Thompson-Reuters, contributes to $20-40 billion in annual losses. The average synthetic identity—95% of which make it through the onboarding process—has a credit score of 650, which Deloitte describes as "just shy of what agencies consider 'good.'" This all adds up to a significant fraud threat, with mobs of

Prism Ver. 1.0 © 2024 The Prism Project

non-existent persons transacting in digital systems, able to take out loans, collect benefits, and scam services.

Impersonations are also a problem exacerbated by AI, with easy-to-access deepfake technology able to render weaker biometric security methods useless, making them vulnerable to account takeover. In 2024, this proved to be an increasing threat in Singapore, after a series of unreported data breaches led to the proliferation of know your customer documents and selfie data on the dark web.

Biometric digital identity is the ideal prevention measure, able to minimize fraud threats, thanks to its nature: when biometrics—combined with liveness and deepfake detection—link a person to their ID, it proves they are who they claim to be. From a scamming perspective, biometrics cannot be stolen, phished, or otherwise transferred to a bad actor trying to gain access to an account. Neither can that bad actor open an account under an assumed identity downstream when biometric onboarding is used in the enrollment process. And when it comes to synthetic identities, biometric digital identity can solve the problem on two fronts. With biometrics at the front door, relying parties are ensuring that only confirmed human beings are opening accounts, while biometric 1:N search functionality allows stakeholders to weed out both duplicate and synthetic accounts, ensuring every profile in their system corresponds to the rightful user in the physical world.

Operational Efficiency

Staffing and labor challenges are ubiquitous, and digital transformation is promising new levels of automation aimed at relieving the stress caused by increasing customer demand. In travel and hospitality this is most apparent. The air travel industry has almost fully recovered from the impact suffered during the COVID pandemic, with 2023 passenger volumes in the range of 8.7 billion.

1:N biometric searches enable duplicate records to be coalesced, merged, or deleted as needed, cleaning databases and reducing operational workloads.

Without the workforce to meet the demands of pre-pandemic service numbers, facilities are incapable of operating safely at full capacity, closing entry lanes, help desks, and in some cases even canceling or rescheduling important parts of a guest's itinerary. The issues are quite punctuated in the air travel experience of recent years, with mass cancellations, historic customer complaint levels, and a high-profile epidemic of lost baggage.

Looking at financial services, operational efficiency is a matter of competition. Startups and new technology firms are challenging traditional institutions by offering agile, innovative products. Legacy players are forced to compete through innovation, acqui-

Prism Ver. 1.0 © 2024 The Prism Project

sition, and collaboration. Meanwhile, in the wake of the 2022 FinTech bust, startups have become more robust and versatile. In this highly competitive environment, quick and automated service is a key differentiator.

Both of these operational challenges are reflected in the government space, where a shrinking public workforce and an influx of immigration in many countries are conspiring to cause severe delays in service delivery. Digital transformation might promise easier access and better experiences, but when balanced with the still existent physical channels, operations are slowing even further, contributing to worker burnout, user frustration, and citizen disengagement.

Biometric digital identity lightens the operational load in all these respects, allowing for high risk transactions to be processed accurately and efficiently through digital channels. Processing time required for identity proofing is shrunk by orders of magnitude, with operations that used to require lengthy transit and manual checks replaced by AI-supported biometric matching. These speeds are possible thanks to biometric binding that links a human to their foundational identity data. That core identity can be subjected to a 1:N search, enabling duplicate records to be coalesced, merged, or deleted as needed. With biometrics at the core, relying parties can count on clean records, reduced toil, and a competitive user experience powered by identity-safe automation

Luminaries in the Targeted Travel and Hospitality Solutions Prism Beam have allowed for a 75% reduction in entry lanes at stadiums that use biometric access for guests, leading to major operational savings.

Sustainability & ESG

In 2024, the Prism Project investigated areas of of Environmental, Social, and Governance (ESG) affected by identity. The most prominent common thread we found was inclusion and accessibility. This is most apparent when considering the underserved and unbanked populations around the world. Financial participation in an economy is a prerequisite for its sustainability, and reliable means through which to assert one's identity is foundational to owning a bank account which is essential for self-reliance and autonomy.

According to FDIC, mobile banking in the US is more common among underbanked households. Meanwhile, McKinsey reports mobile payments are popular in Latin America because of their security, convenience, and low cost.

There are approximately 1.5 billion unbanked people in the world—a number representing every economy on Earth. And even beyond economic participation, those people need to be reached by the government agencies meant to represent them. While it is tempting to exaggerate how connected our world is when discussing digitization, the fact remains that many people are underserved by virtue of where they live, even if they do have the

Prism Ver. 1.0 © 2024 The Prism Project

basic privileges afforded by identification. Citizens in rural regions may have to travel long distances to participate in government or financial services, while those in digital deserts might not have the connectivity to use digital channels at all. This digital divide is crucial to address because rural and urban populations are equally engaged in political, economic, and social life, but underserved populations show an understandable lack of institutional trust when they are neglected due to logistics that favor city dwellers.

Biometrically-bound foundational identity can solve problems of inclusion. Identity proofing can be performed on smartphones, tablets, laptops, and desktop computers. Once a citizen is onboarded and their biometrics are bound to a system of record, their mobile ID can be digitally signed, allowing for offline use. This and other redundancies are methods currently being used in Africa to ensure service and boost inclusion. Meanwhile, for those without smartphone technology, digital ID is making its way into the physical world thanks to innovative biometric barcode technology.

By enabling inclusion with biometrics at the core, vendors and stakeholders are contributing to an active, accessible, and sustainable economy.

Security

10% of the 30,659 information security incidents reported by US Federal Agencies in 2022 were directly related to phishing, according to the Government Accountability Office.

The move to digital channels accelerated by the pandemic has made cybersecurity a major concern in all sectors. Targeted data breaches are of paramount concern for private enterprises, with Kaspersy pricing a single targeted attack at $891,000 in associated costs. Governments, meanwhile face threats from bad actors on all fronts, from the border, to the internet, to its own communities. Increases in travel and migration are straining border control for tourism, visa programs, and immigration. Agencies need to be able to welcome visitors while maintaining national security.

On both digital and physical fronts, biometric digital identity addresses security concerns without hindering the user experience. Through online channels, biometrics secure accounts and databases, while providing an unimpeachable audit trail. Biometric authentication supported by a strong foundation and unbroken trust chain makes breaking into databases significantly more challenging. And decentralized storage methods, as exemplified by Prism Luminary Anonybit, makes compromised data useless even if it is leaked. Meanwhile, end users can rest easy knowing their data is only accessible to themselves, since biometrics

Prism Ver. 1.0 © 2024 The Prism Project

cannot be stolen or shared.

In the physical world, biometric digital identity solves even the most complex and high risk security challenges. Border control solutions like Digital Travel Credentials (DTC), which allow trusted travelers to perform pre-screening from their homes, use strong identity and verifiable credentials to lessen the burden and alleviate bottlenecks at the border. But that's secondary to the accurate identity checks that are made possible through the DTC, which is already maintaining security in countries as far-apart as Aruba and Finland

Privacy

Information wants to be free, but when it comes to personal data, we need to fight against that maxim. As demonstrated in the previous sections of the Prism Lens, digital identity data is extremely valuable. Your identity is your key to finance, government participation, healthcare treatment, travel, and even entertainment. But it also has a monetary value to bad actors. And that's not to mention the simple fact that it belongs to you. Your personal safety and peace of mind hinges on your ability to control what information you share with whom, and under what terms.

In addition to enabling compliance with privacy laws, biometric digital identity empowers users with visibility and control over their most valuable data. When biometrics is at the core of foundational identity, it can be associated with a variety of biographical and contextual data. When asserted via a mobile or digital ID, that data carries forward the integrity of government vetted ID without needing to reveal non-relevant sensitive data.

This biometrics-supported pseudonymous identity is a powerful concept best illustrated through the example of ages checks. For age restricted substances like alcohol or cannabis, or regulated services like gambling, pseudonymous identity represents the act of confirming you have permission to participate without having to share the actual information that proves it. The concept can be applied to all identity transactions, putting user consent first when identity is on the line.

.

Prism Ver. 1.0 © 2024 The Prism Project

The Biometric Digital Identity Market Forecasts

Bolstered by constantly improving identity literacy and the converging industry trends illustrated in the previous section, which lend themselves to biometrics adoption, the Biometric Digital Identity Market is on track for significant growth, globally.

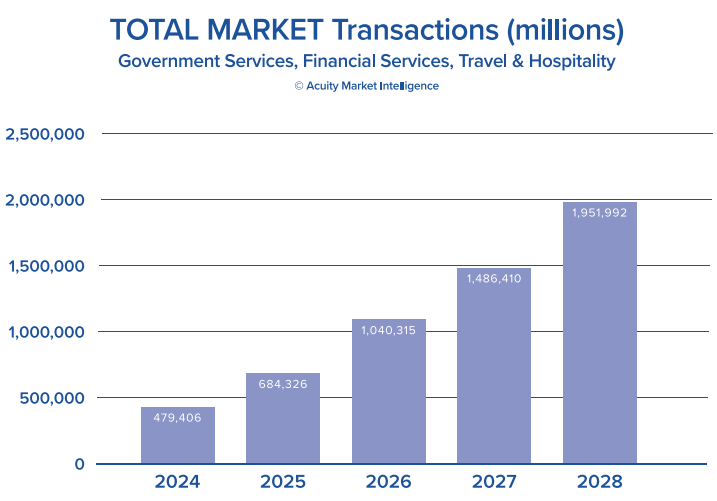
The following forecasts are based on original market research from Acuity Market Intelligence. This proprietary analysis includes primary research, third party data, vendor reported data, and industry expert assessments.

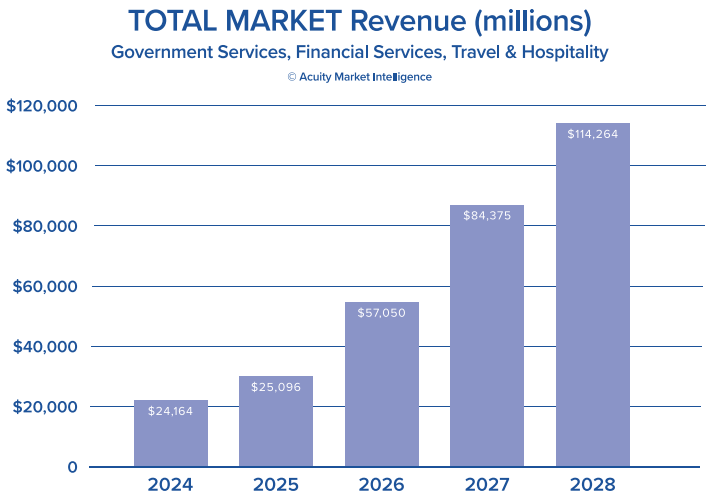
Interactive spreadsheets of these forecasts with further visibility into the market are available for purchase.

Contact cmaxmost@acuity-mi.com for inquiries.

Global Forecasts

The annual revenue for biometric digital identity transactions for the three key verticals analyzed in 2024—financial services, travel and hospitality, and government services—is projected to grow from $24B to $114B annually from 2024 to 2028, while transaction volumes grow from less than half a trillion to nearly 2 trillion annually. While these verticals present only a partial view of the total global market opportunity, they are large critical markets that provide significant insight into the scale and scope of the growth opportunity for biometric digital identity.



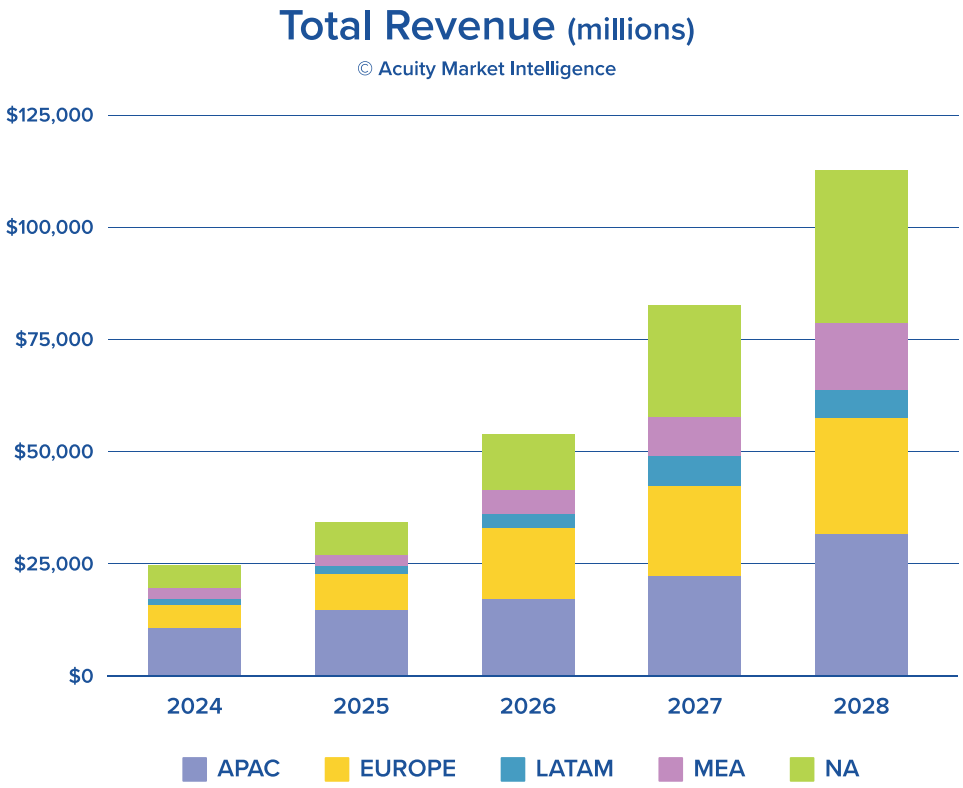


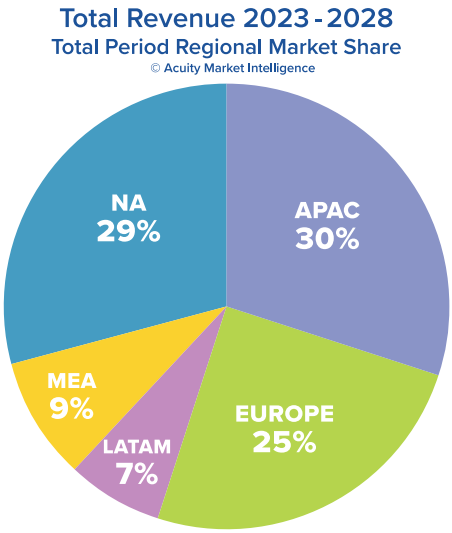
Prism Ver. 1.0 © 2024 The Prism Project

Global Forecasts by Region

Total biometric digital identity revenue from 2024-2028 is expected to grow at an overall compound annual growth rate (CAGR) of 47.5%, generating nearly $315 billion globally.

The Asia Pacific region leads in market share, closely followed by North America and Europe, while Latin America, the Middle East, and Africa trail in terms of revenue.



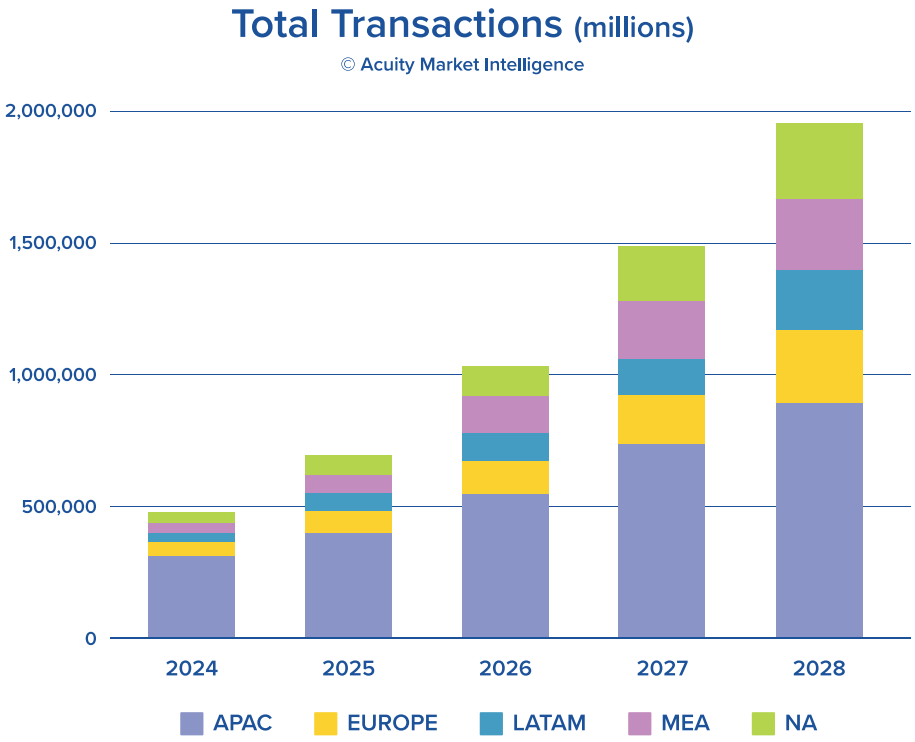


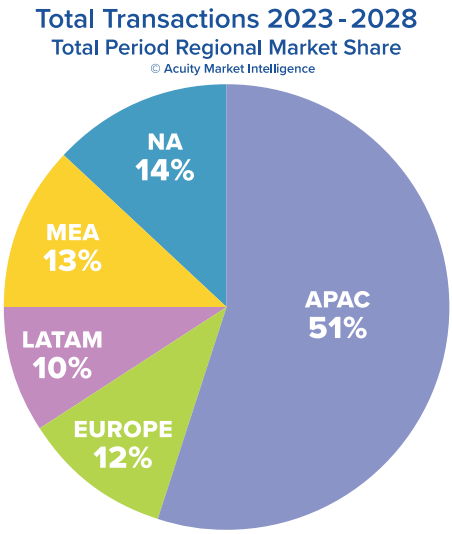
Total Revenue (millions)					
	2024	2025	2026	2027	2028
APAC	$9,915	$12,724	$17,572	$23,357	$29,498
EUROPE	$6,351	$9,174	$14,763	$21,192	$28,311
LATAM	$1,422	$2,139	$3,617	$6,136	$8,470
MEA	$1,695	$2,855	$5,018	$7,925	$10,886
NA	$4,782	$8,204	$16,080	$25,765	$37,099
Total	**$24,164**	**$35,096**	**$57,050**	**$84,375**	**$114,264**

Prism Ver. 1.0 © 2024 The Prism Project

Global Transaction Volumes by Region

That revenue is driven by 5.6 trillion transactions globally, the vast bulk of which belong to the APAC market, which accounts for 51% of the market with 2.9 trillion. The remaining regions account for the remaining verifications, with North America ahead of MEA by a percentage point, which likewise is itself ahead of Europe by a percentile. LATAM fills out the transaction volumes with a tenth of the market.



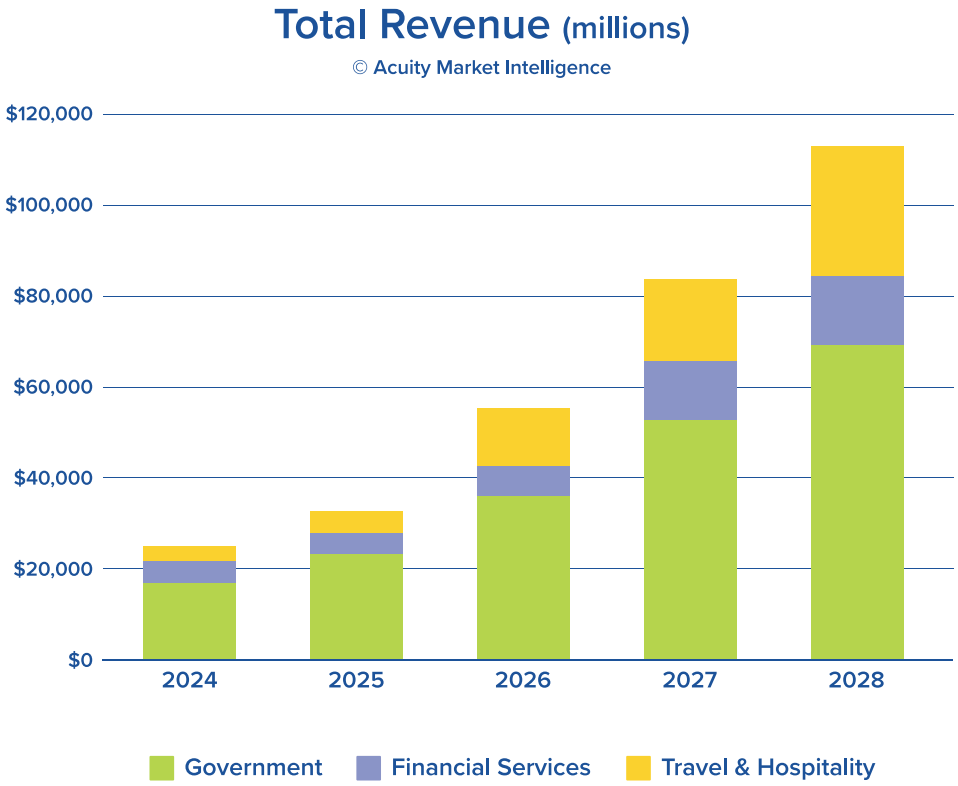


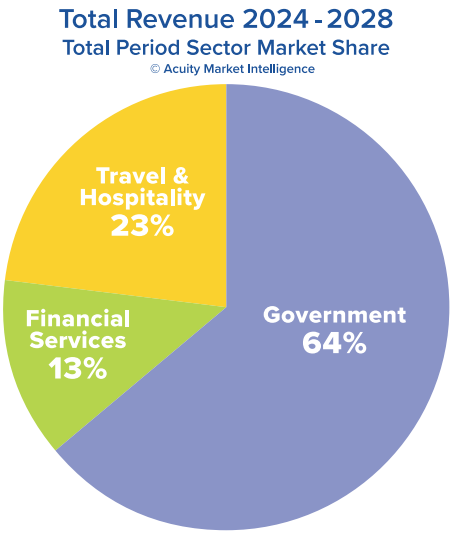
Total Transactions (millions)					
	2024	2025	2026	2027	2028
APAC	291,818	389,402	544,876	723,919	903,922
EUROPE	56,668	83,166	129,933	186,507	246,309
LATAM	44,593	66,371	105,475	156,579	213,578
MEA	47,057	75,337	128,902	202,811	280,876
NA	39,269	70,051	131,129	216,594	307,307
Total	**479,406**	**684,326**	**1,040,315**	**1,486,410**	**1,951,992**

Global Forecasts by Sector

When we shift focus and break down the market by sector we see that government services accounts for two full thirds of the revenue. Travel and hospitality makes up nearly a quarter, and financial services rounds out the arena with 13%.

Considering the outsize focus placed on financial services by the identity industry in the past decade, these results may come as a shock. But as we will see on the next page, this market share breakdown offers insights into the importance of transaction value.





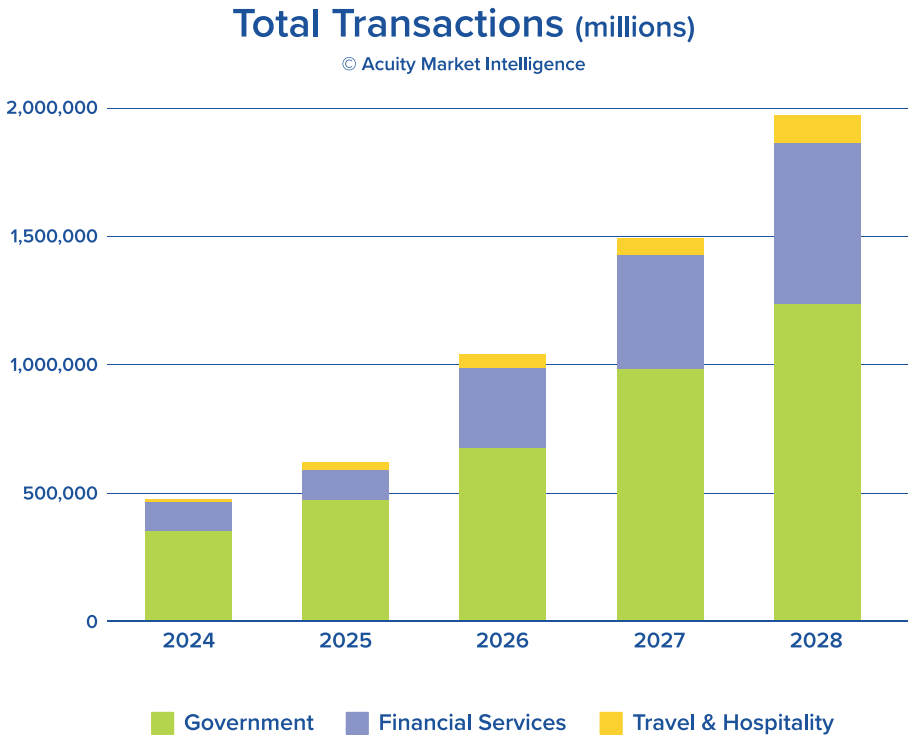
Total Revenue (millions)					
	2024	2025	2026	2027	2028
Government	$18,110	$25,506	$37,718	$53,282	$67,909
Financial Services	$3,739	$4,442	$7,246	$9,963	$14,858
Travel & Hospitality	$2,316	$5,148	$12,086	$21,130	$31,497
Total	**$24,164**	**$35,096**	**$ 57,050**	**$ 84,375**	**$114,264**

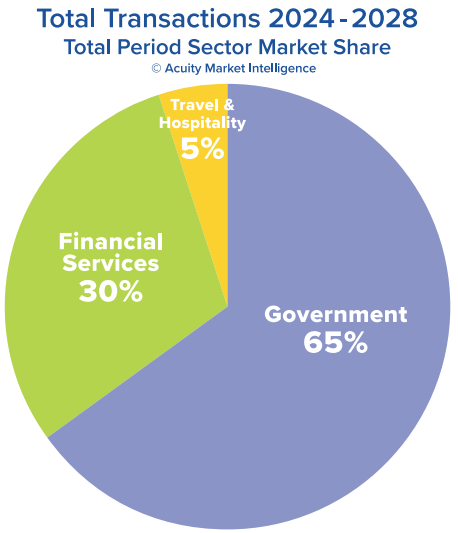
Prism Ver. 1.0 © 2024 The Prism Project

Global Transaction Volumes by Sector

While government applications of biometric digital identity make up just over two thirds of the transaction market share during the forecast period (a nearly 1:1 correlation with revenue), financial services accounts for 30%, while travel and hospitality only make up 5%.

It's a startling contrast: 30% of global biometric digital identity transactions in financial services will contribute to only 13% of the world wide revenue for the next four years. This is a reflection of the comparative low cost associated with financial verifications. In travel and hospitality, meanwhile, a single verification goes further—with only 5% of the transaction volumes it will contribute to 23% of the overall revenue.





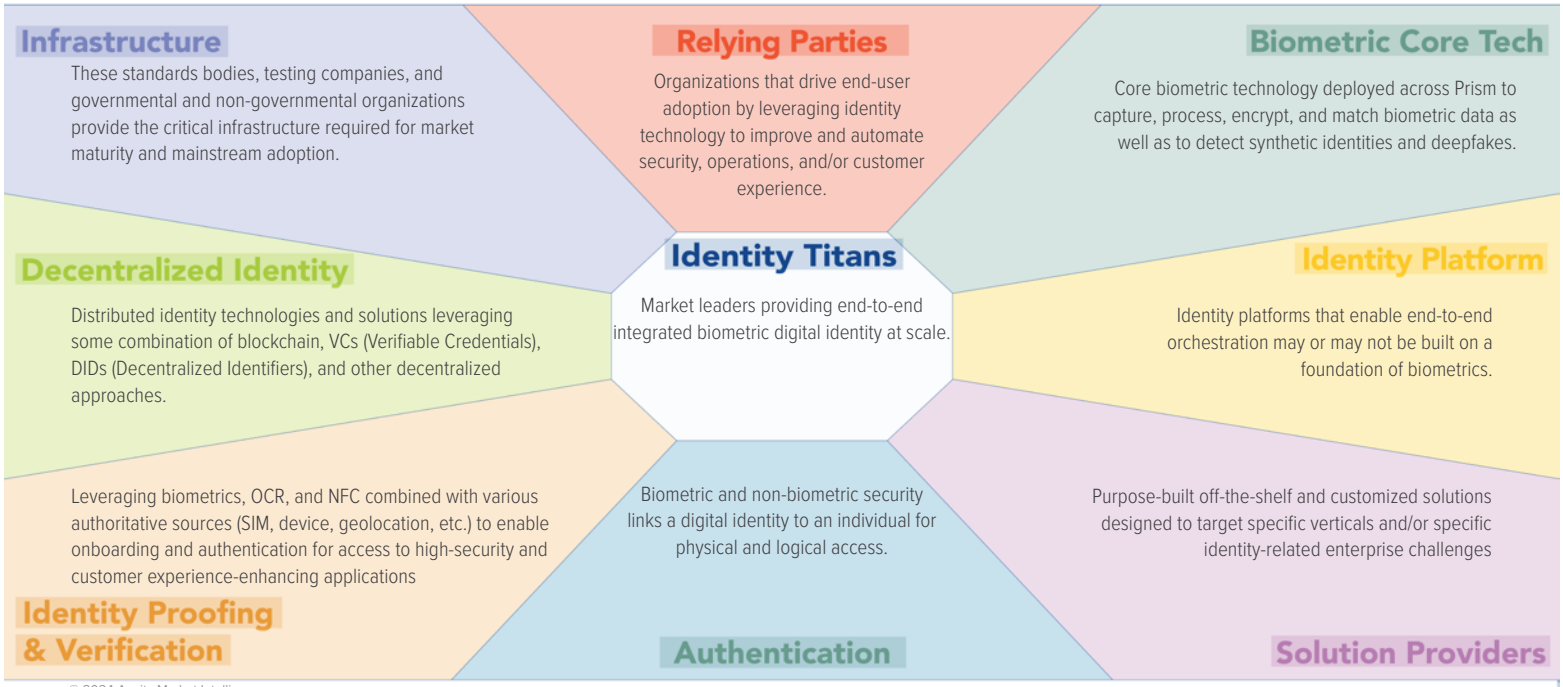
Total Transactions (millions)					
	2024	2025	2026	2027	2028
Government	338,514	473,132	692,231	955,104	1,198,245
Financial Services	132,574	189,877	300,280	454,770	644,802
Travel & Hospitality	8,318	21,318	47,805	76,536	108,945
Total	**479,406**	**684,326**	**1,040,315**	**76,536**	**1,951,992**

Prism Ver. 1.0 © 2024 The Prism Project

The Biometric Digital Identity Prism

Just as a beam of light contains all colors, the biometric digital identity ecosystem is comprised of many vendors contributing to the grand idea of digital identity. The Prism Project conceptualizes this relationship through the Prism: a proprietary market landscape model intended to help reflect the components of the emerging reality of identity in a digitized world.

Biometric Digital Identity Prism



Vendors are positioned in one of nine Prism Beams. Each Beam representing a critical component of the biometric digital identity landscape. For some vendors, it can be challenging to select one beam that represents their singular position in the marketplace. Many appear to span multiple beams. In these cases, we have selected the beam that most accurately reflects the breadth and depth of their product and service offerings and is most closely aligned with their unique differentiators.

How to Read the Prism

Within each beam, there are three Vendor Categories: Pulsars, Catalysts, and Luminaries.

Pulsar

Pulsars are the bright upstarts and pivoting legacy vendors prioritizing the crucial elements of biometric digital identity. Startups with promising technology or established names with a proven aptitude for adapting to the new identity ecosystem, Pulsars have strong potential to influence the Prism landscape.

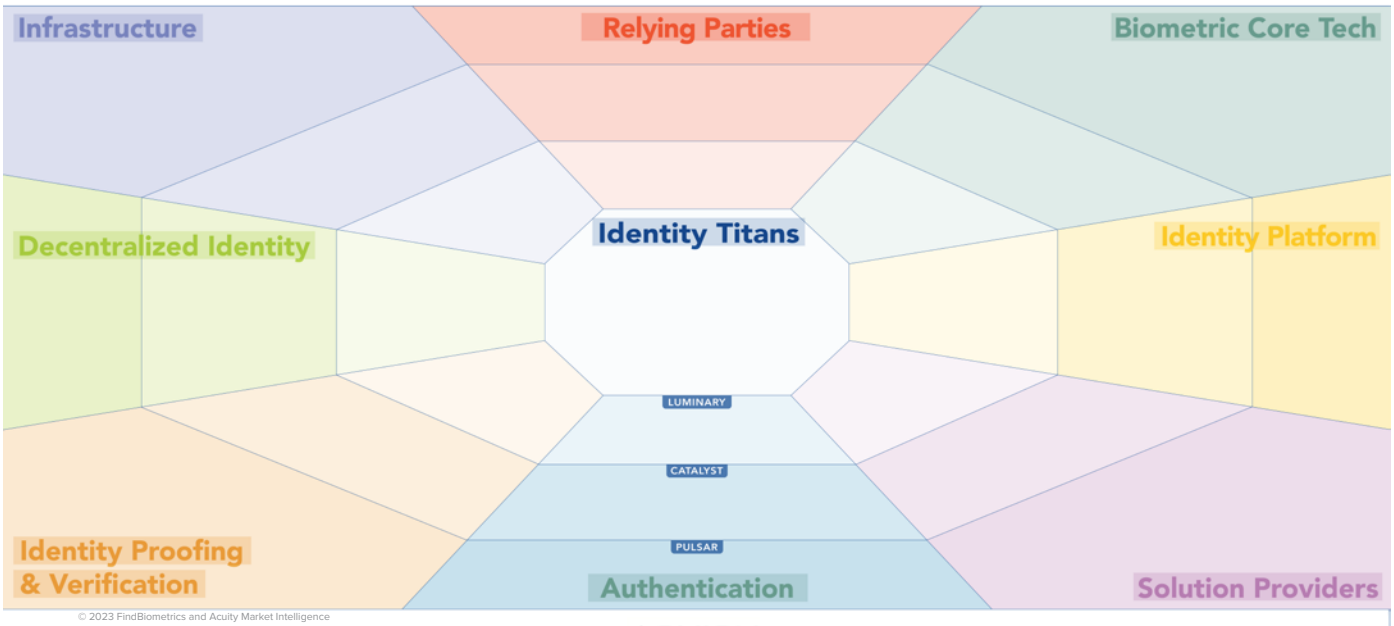
Catalyst

Catalysts are established disruptors, innovators, and agents of acceleration. With high proficiency in certain areas of assessment, Catalysts are often one step away from ascending to Luminary status, whether it's through an acquisition, a technological innovation, or an injection of resources.

Luminary

Luminaries are the guiding lights of their industry segment. They show the highest level of proficiency in their beam and are often responsible for setting trends in their fields.

Biometric Digital Identity Prism



Prism Ver. 1.0 © 2024 The Prism Project

Refractors and the Identity Titans

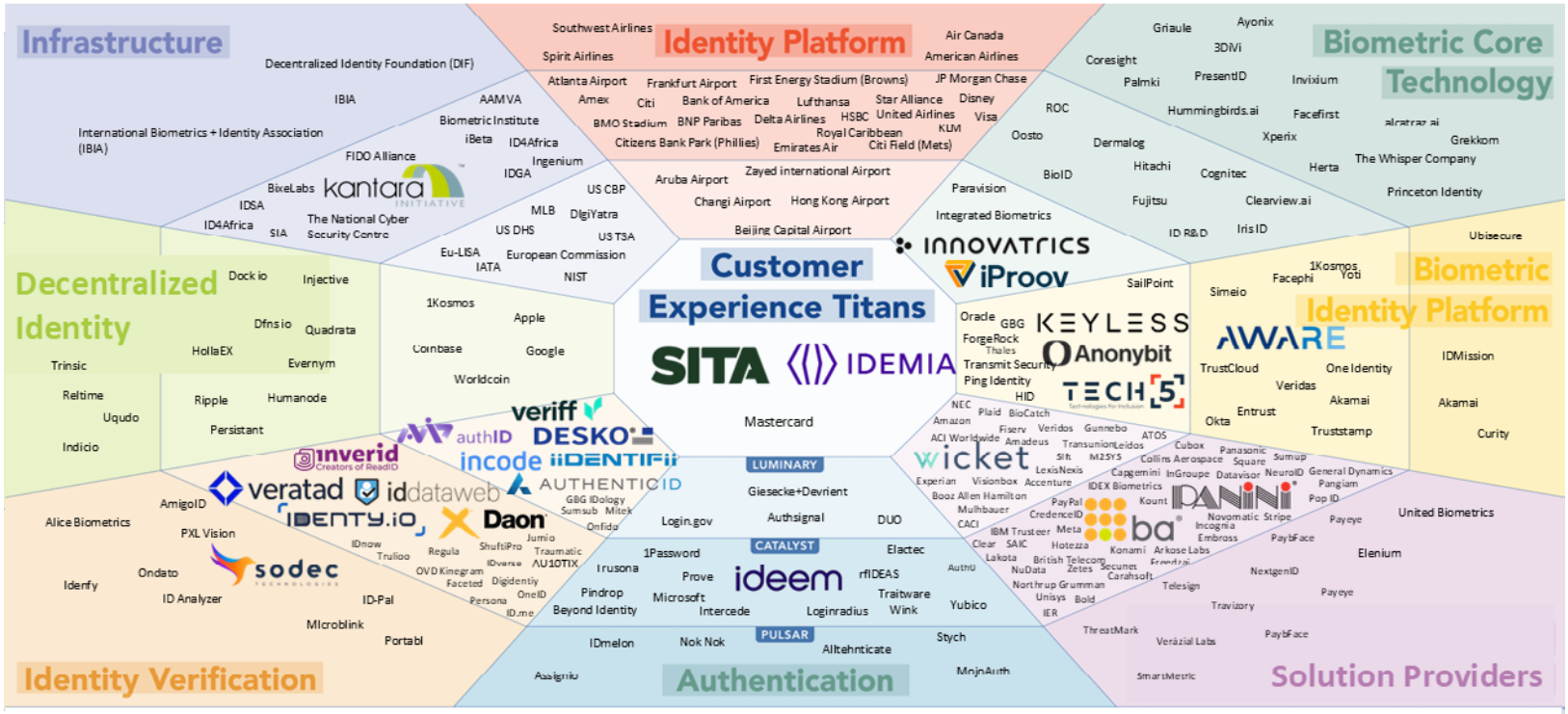
The center of the Prism is anchored by a special category—the Identity Titans. These companies, due to their size, global footprint, proven expertise, partner networks, and robust portfolios, have a definitive role in the biometric digital identity landscape. This role is that of a Refractor: it is through their initiatives that the industry is viewed.

As the market evolves through acquisition, development, regulation, and innovation, the Refractor position may grow or diminish. Luminaries in the Identity Platform Beam are best positioned to ascend to Refractor status.

Prism Ver. 1.0 © 2024 The Prism Project

The 2024 Flagship Biometric Digital Identity Ecosystem

2024 Flagship Biometric Digital Identity Prism



The Prism Beams and the classifications within represent important components of the emerging biometric digital identity landscape, and group vendors by the role they play therein. It is modality agnostic. Because of the broad nature of Prism Beams, many companies in the same areas are not direct competitors but represent the leading providers of their given solutions.

Prism Ver. 1.0 © 2024 The Prism Project

Evaluations & Profiles

In order to place vendors on the Biometric Digital Identity Prism, we assess the leading companies in each Prism Beam based on a proprietary evaluation scheme that includes six broad criteria.

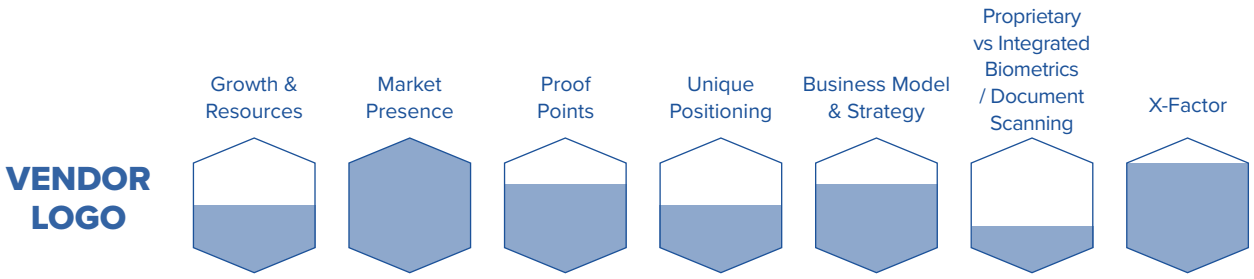
- **Growth & Resources** – Current revenue, year-on-year growth, financial stability, and resources available to sustain and support ongoing growth.
- **Market Presence** – Overall geographic footprint and market sector penetration, as well as specific geographic regions and markets where a level of dominance has been achieved.
- **Proof Points** – Profile and size of overall and market sector customer base and key customers. Also includes 3rd party testing results and certifications and speed of implementation.
- **Unique Positioning** – Unique Value Proposition (UVP) along with differentiable technology and market innovation generally and within market sector.
- **Business Model & Strategy** – Overall marketing and sales positioning, messaging, and strategy as well as channel scope and quality and range of partnerships, channels, thought leadership, use of digital, social media presence, and engagement generally and within market sector.
- **Proprietary Versus Integrated Biometrics and Document Authentication** – Depending on the market, solutions(s), specific beam, may be rated higher as proprietary or integrated technology.
- **X-Factor** – This is a unique beam and market sector specific metric.

For the Infrastructure Beam, because of the special critical market supporting nature of these organizations, we replace Proof Points with Commitment to Biometrics and we replace Proprietary Versus Integrated Biometrics and Document Authentication with Impact and Influence.

- **Commitment to Biometrics** – Evidence of long term financial and cultural investment in biometrics as a core identity technology, not only within a product portfolio, but conceptually at an industry level.
- **Impact and Influence** – Effectiveness of an organization's ability to guide standards, regulation, policy, and industry best practices through its own initiatives and thought leadership.

Prism Ver. 1.0 © 2024 The Prism Project

We visualize this assessment as a Prism Evaluation Chart: an easy-to read graphic representation of a vendor's current activity, resources, and abilities. The more color filling a Prism hexagon, the higher level of proficiency.



Important Note of Evaluations and Prism Placement:

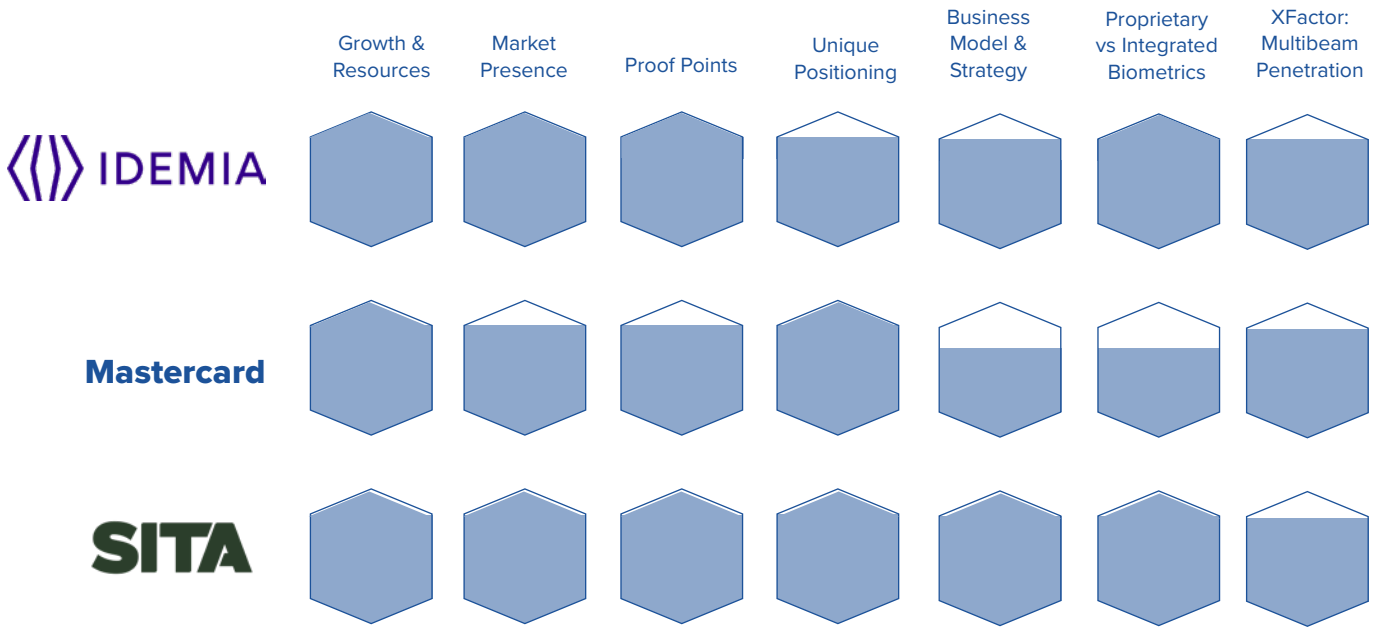
The vendor specific metrics in this report are based on publicly available data, survey data, interviews, and confidential briefings. It is presented in good faith as a representation of the biometric digital identity ecosystem according to the values stated previously in this report. If you see your company here and have questions about your evaluation or placement within the Prism, please contact: info@the-prism-project.com.

Prism Ver. 1.0 © 2024 The Prism Project

Identity Titans

These leading biometric digital identity players are critical to global acceptance and adoption. To date, they have made significant levels of investment in biometric tests, pilots, and deployments but they all understand the critical role biometrics will play as the digitally-driven global identity ecosystem evolves.

Evaluations

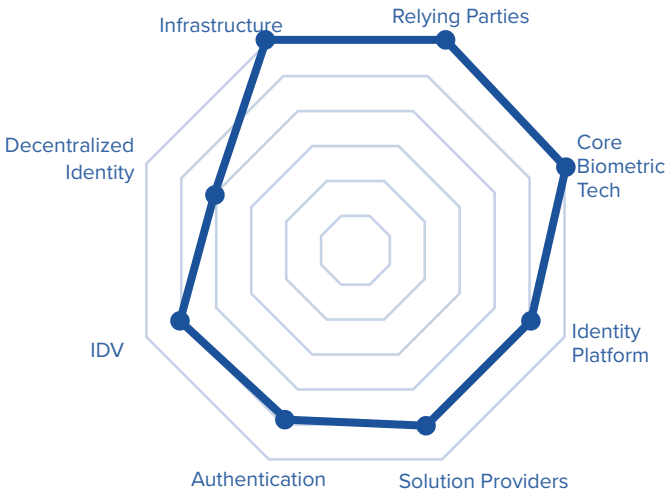


Prism Ver. 1.0 © 2024 The Prism Project

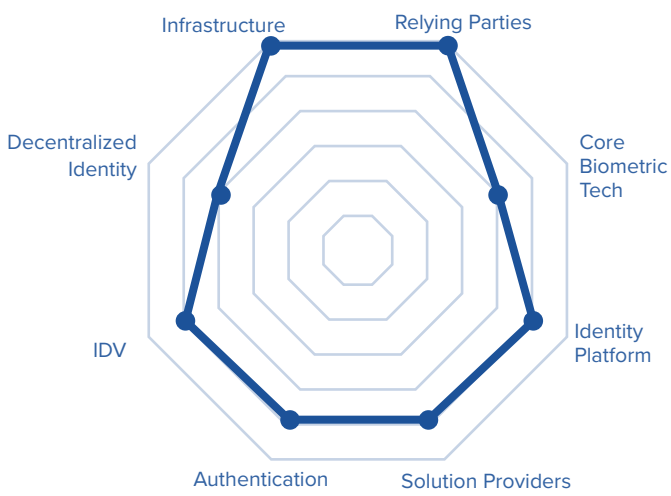
Refractor Beam Penetration

The Identity Titans are positioned in the center of the Prism because of their demonstrated ability to define the biometric digital identity landscape through their broad participation across the Prism Landscape. The following Refractor Charts display each Titan's leadership within every aspect of the biometric digital identity ecosystem.

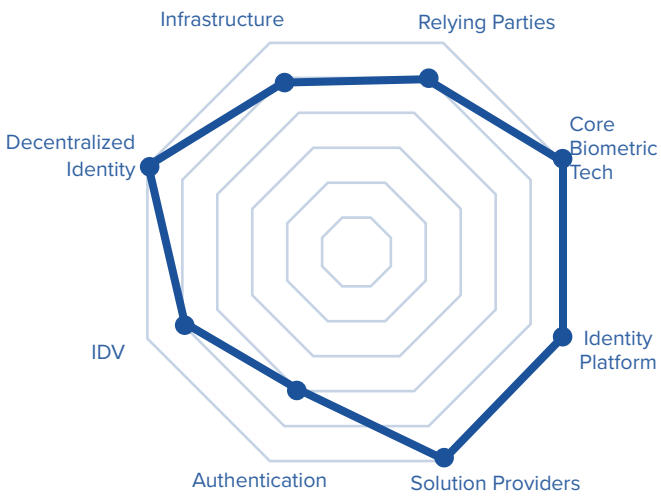
IDEMIA



Mastercard



SITA

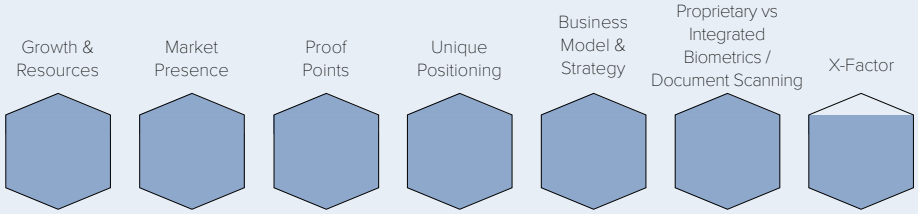


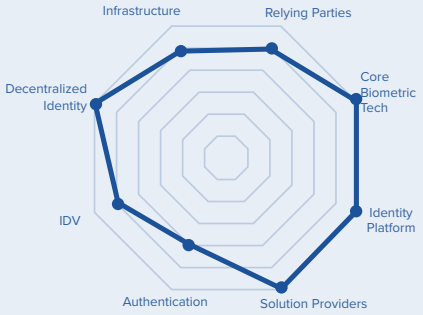
Prism Ver. 1.0 © 2024 The Prism Project

SITA

sita.aero

BEAM: **Identity Titan** / CLASSIFICATION: **Refractor**





Renowned for its leadership in the global travel industry, SITA is a 2024 Flagship Prism Refractor. Founded in 1949 as the Société Internationale de Télécommunications Aéronautique, the company was initially the product of 11 airlines seeking to improve air travel by providing network and communication services within the industry. In the 75 years since, SITA has evolved to not only improve the way we travel on a global scale, but to help define the world's perception of digital identity in practice. With a presence that encompasses 1000 airports, serving over 200 countries and territories and covering 90% of international travel destinations, the company has led the way in providing seamless guest journeys while collaborating with governments and bolstering national security through the innovative use of biometrics, verifiable credentials, and digital ID technologies. All of this in the name of a sustainable, safe, and easy future for those of us who value safe passage in our era of mass digitization.

An Industry Defining Refractor

As an Identity Titan in the 2024 Flagship Prism Report, SITA stands out thanks to its significant engagement in all areas of the biometric digital identity ecosystem. It shines particularly bright in the areas of core technology, distributed identity, a platform-based approach to orchestration, and targeted solutions. This position in the Prism ecosystem reflects its three-quarter century mission to revolutionize air travel, which itself has grown to encompass other experiences as well. With approximately 5,000 biometric touchpoints globally, SITA is a major contributor to facilitating the kind of comprehensively seamless guest journeys that are setting the groundwork for the next phase of converged physical-digital user experiences in all markets.

The Best Path is the Smart Path

When we talk about orchestration, SITA's SmartPath solution serves as an instructive role model. Leveraging facial recognition for biometric passenger identification at every passenger touchpoint, SmartPath is deployed in 43 airports, including Frankfurt. The German airport, operated by Fraport, serves over 90 airlines and has severe spatial limitations that prevent it from any significant physical expansion. So when passenger volumes began to surge, it implemented SmartPath, which eased throughput, improved operational efficiency, and kept security premium. Passenger processing times from check-in to boarding sped up by 30%. With biometrics at the core, high volumes of traffic can be facilitated without compromise.

Gateway to Better National Security

In addition to airlines and airports, SITA's partner network spans seaports and land borders. The company works with more than 70 governments, putting it in the ideal position to build on its rock-solid foundation in travel and hospitality to government applications. And that's exactly what it's done, leveraging eGates, Automated Border Control Kiosks, and the Digital Travel Ecosystem to provide a trust network for sharing Verifiable Credentials, like its game-changing Digital Travel Credential (DTC). Empowered by technical standards recently released by UN's International Civil Aviation Organization (ICAO), SITA's DTC has already transformed this island of Aruba's tourism industry for the better, enabling visitors to interact with the island's government from home and receive pre-approval for border control. Now the average border crossing only takes eight seconds and visitor data errors have been eliminated. With plans to expand DTC based on passenger demand, it's clear SITA's industry-shaping presence will continue to guide the way for practical biometric digital identity on a global scale.

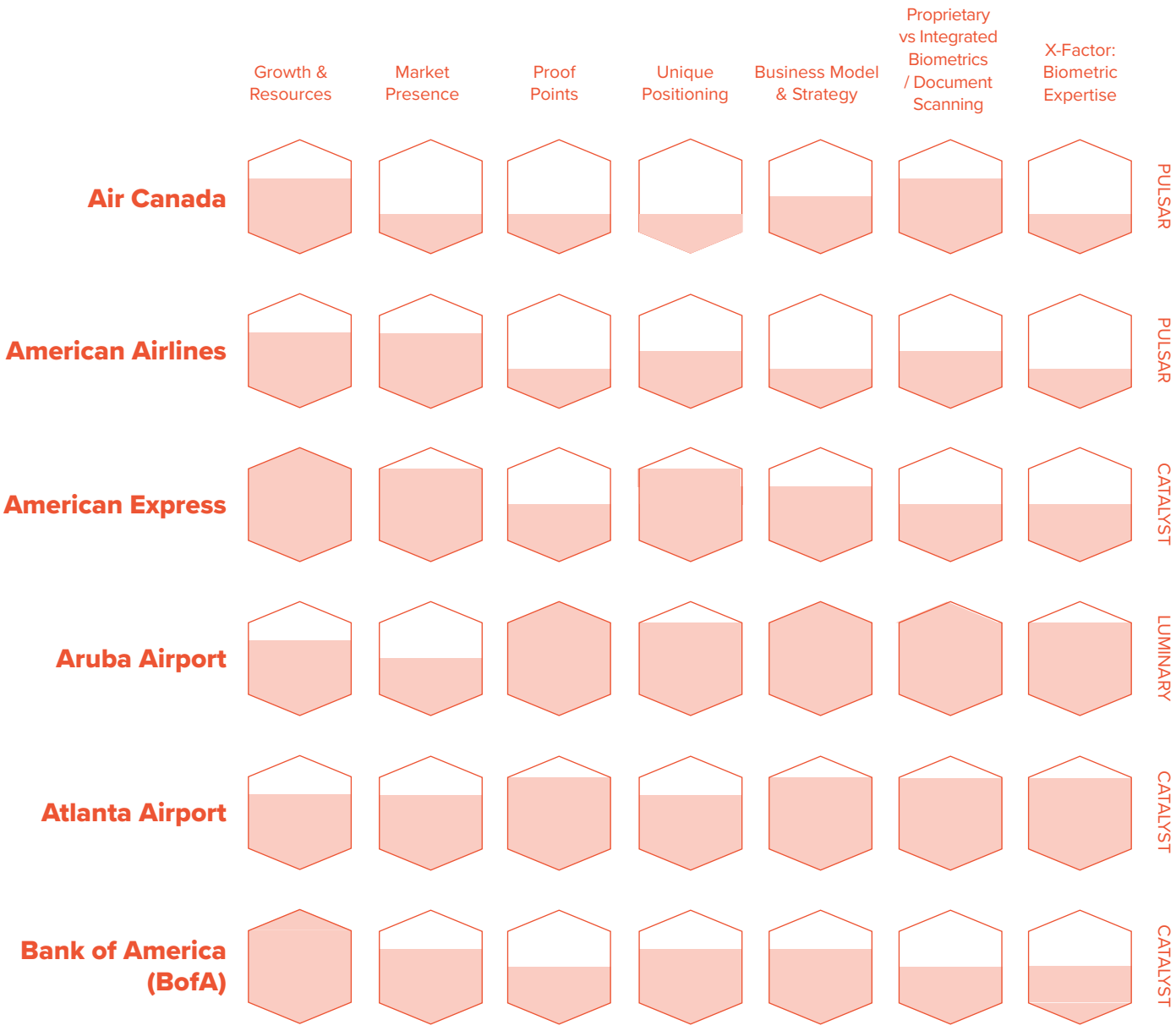
Contact SITA: Euro.iSales@sita.aero

Relying Parties

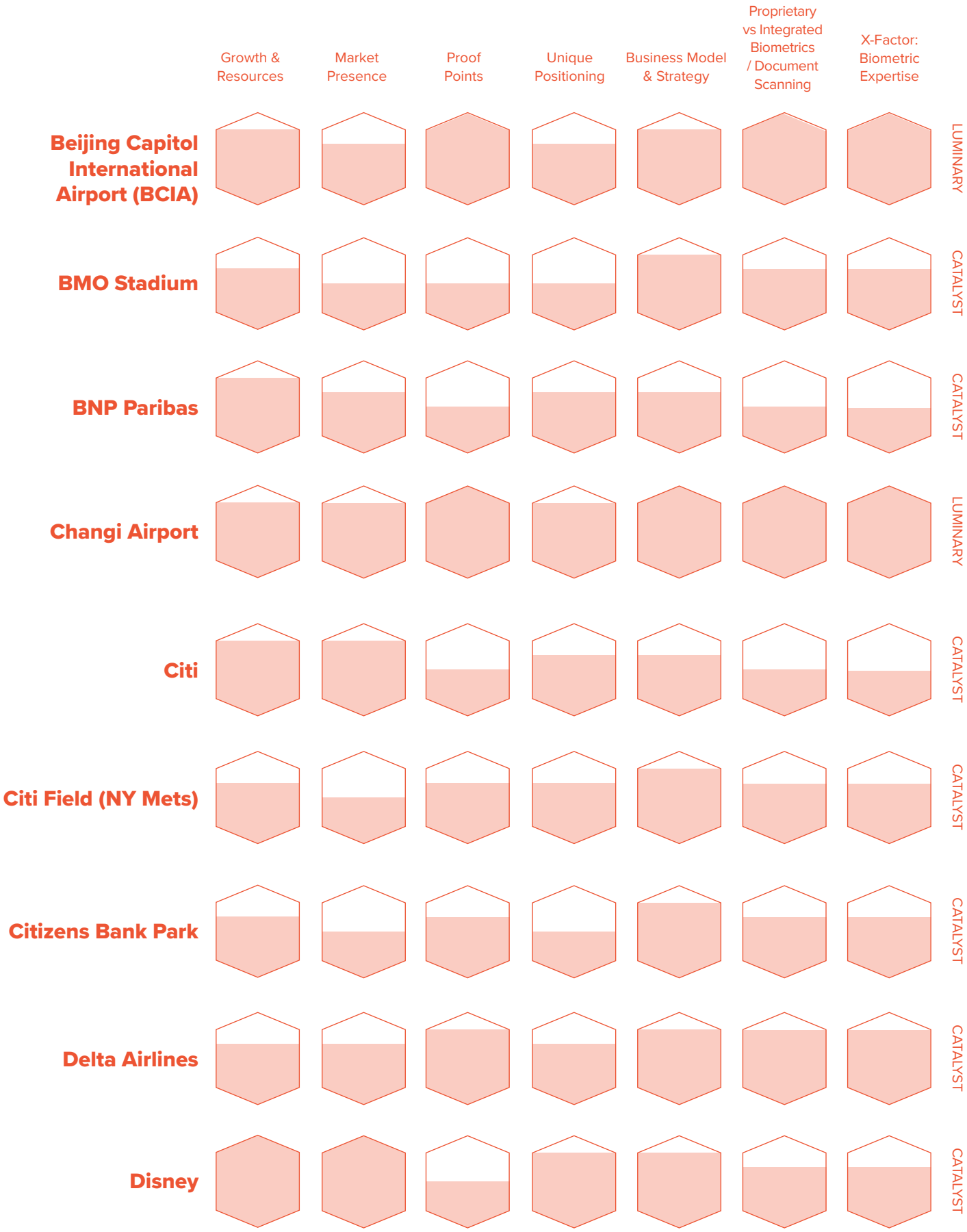
Organizations that drive end-user adoption by leveraging identity technology to improve and automate security, operations, and/or customer experience.

Prism XFactor: Biometric Expertise

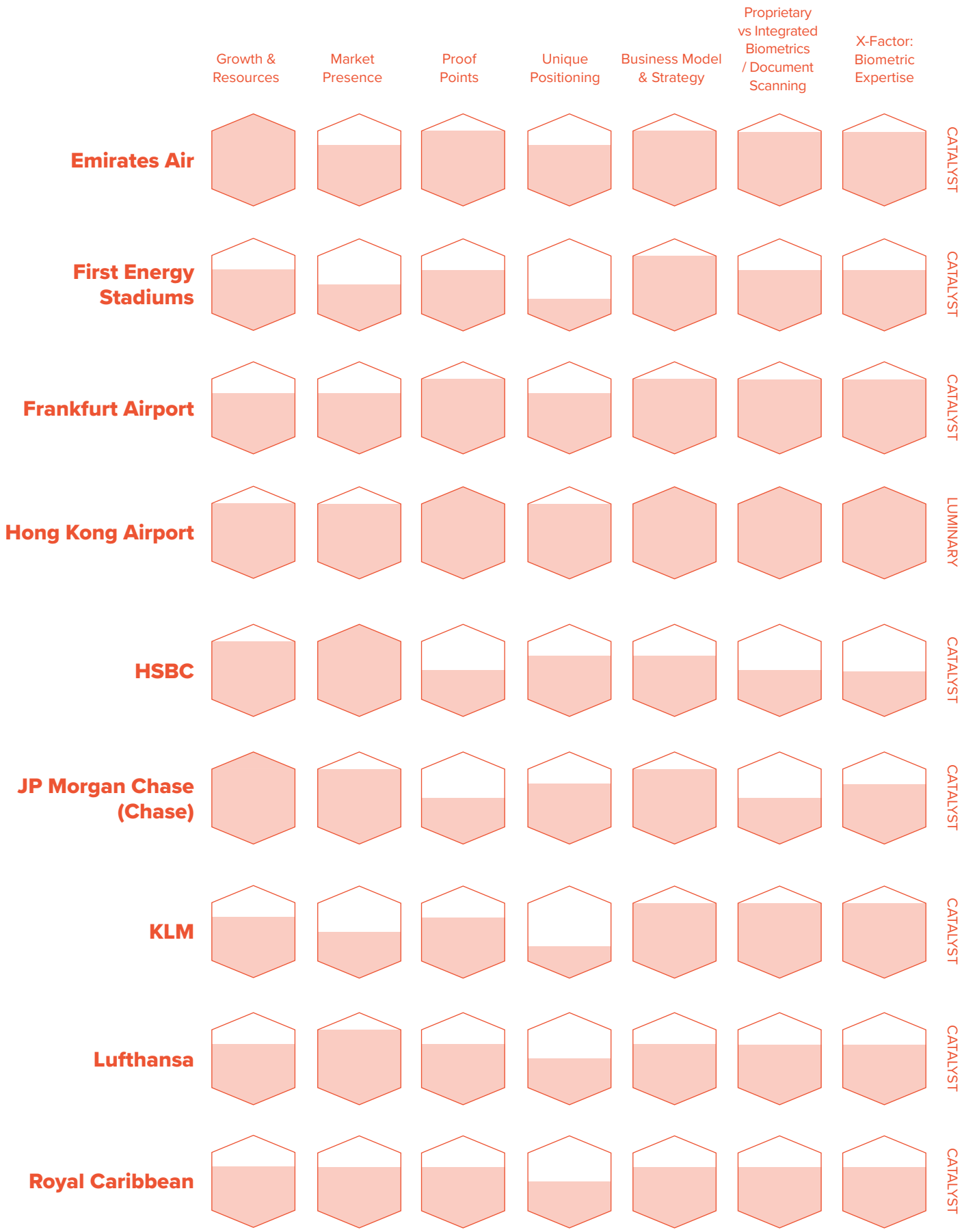
Evaluations



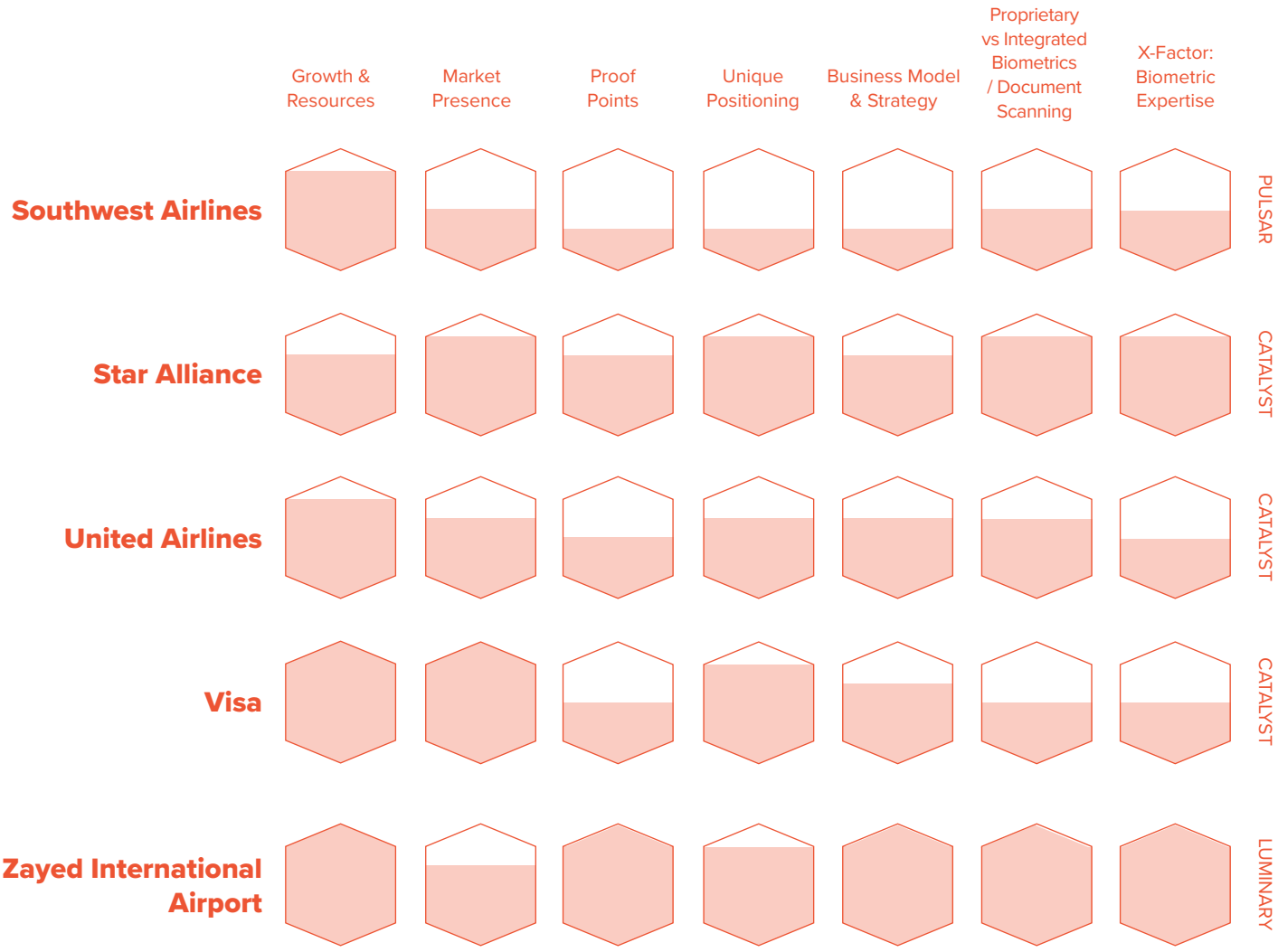
Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project



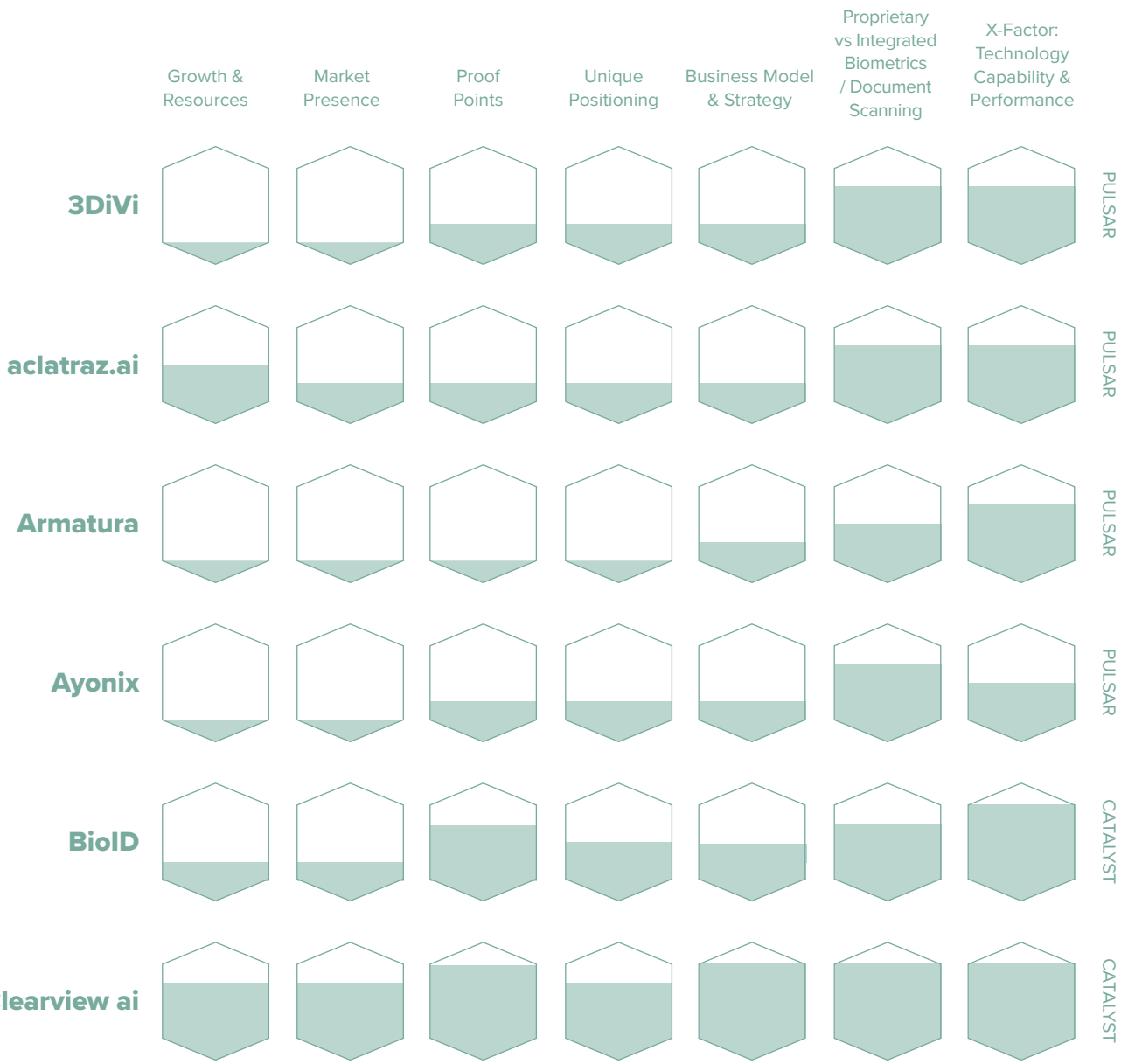
Prism Ver. 1.0 © 2024 The Prism Project

Biometric Core Technology

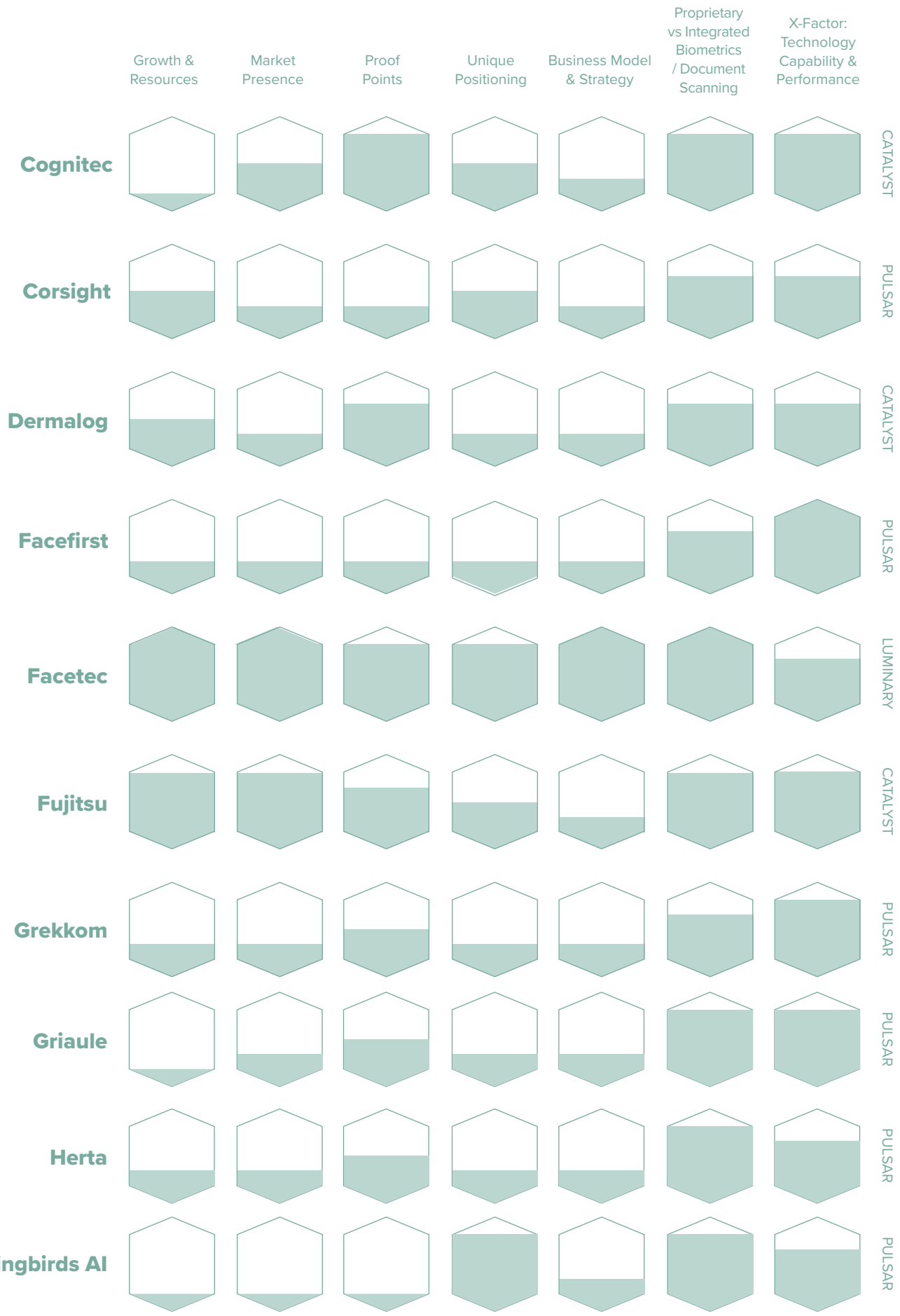
These vendors develop biometric core technology deployed across the Prism for verification, authentication, and to detect synthetic identities and deepfakes.

Prism XFactor: Technology Capability & Performance

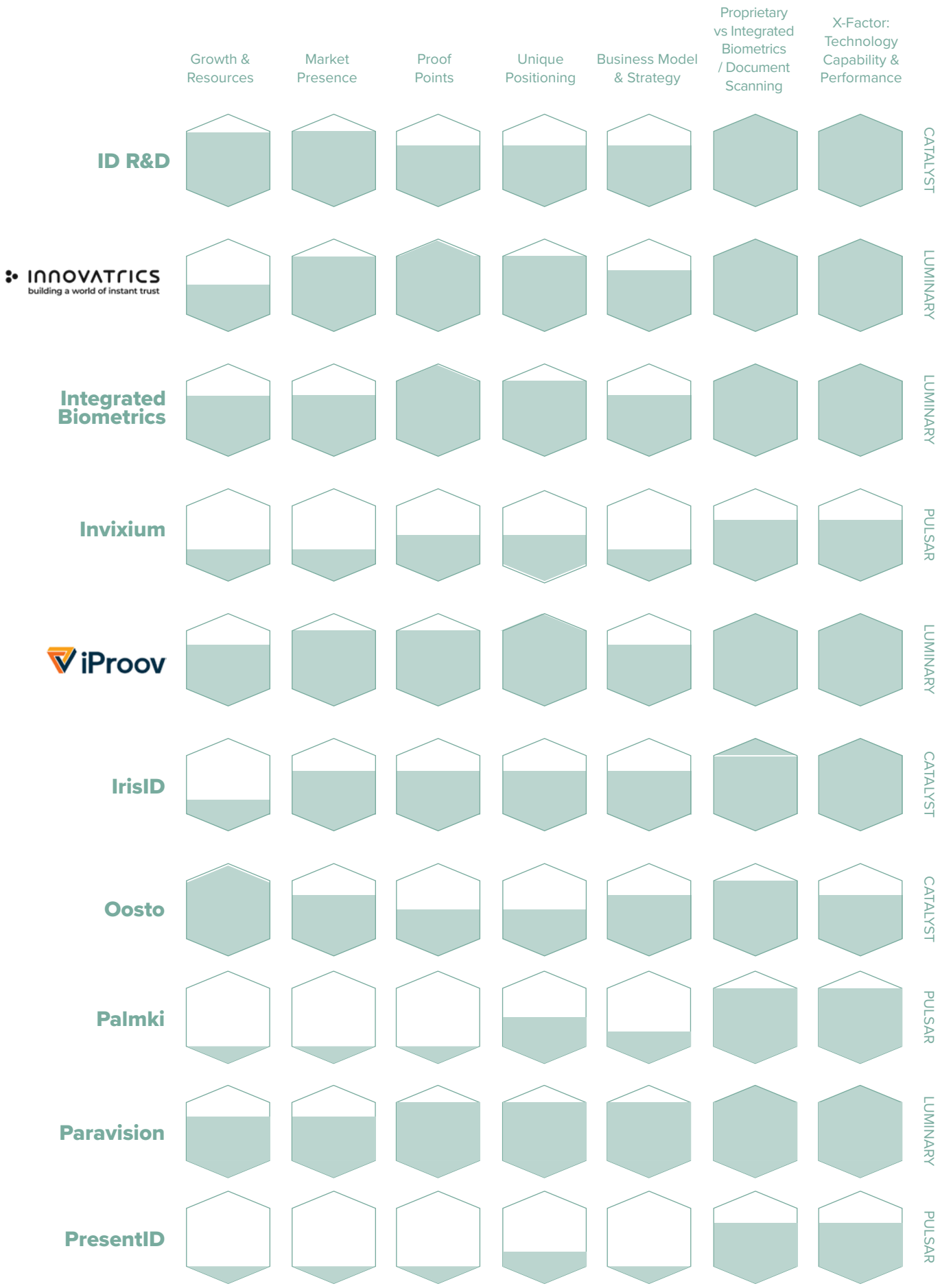
Evaluations



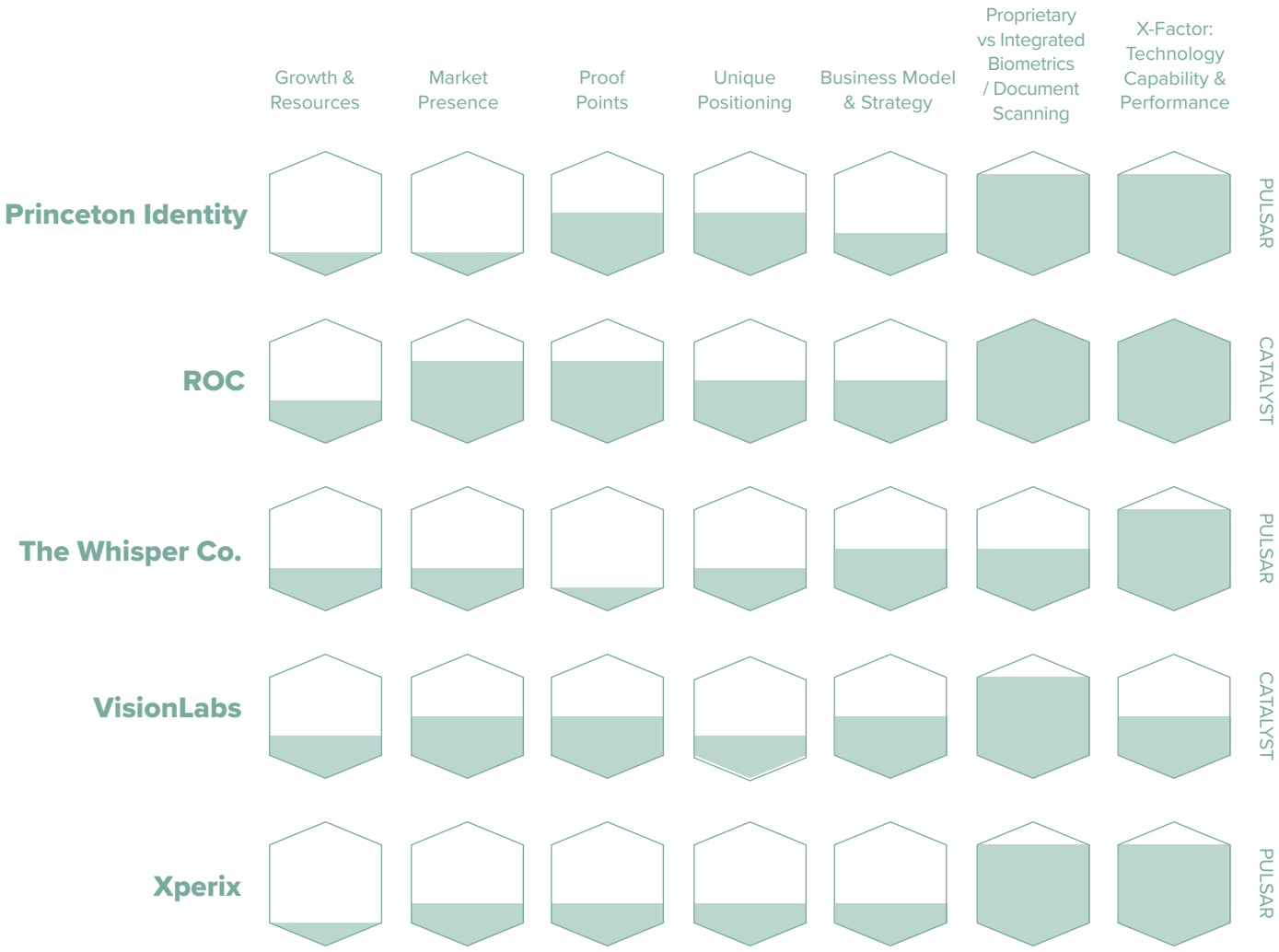
Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project



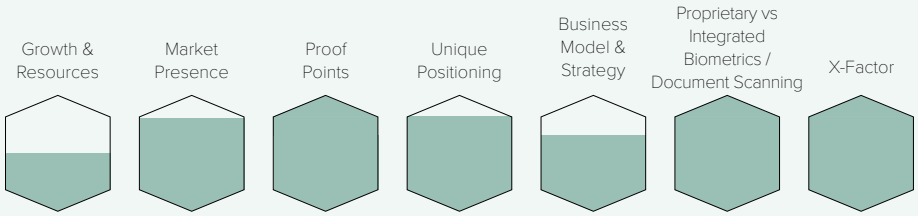
Prism Ver. 1.0 © 2024 The Prism Project

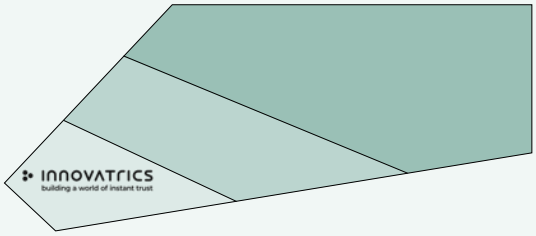
Innovatrics

innovatrics.com

INNOVATRICS
building a world of instant trust

BEAM: **Core Biometric Tech** / CLASSIFICATION: **Luminary**





Boasting a comprehensive suite of biometric technologies that span modalities, Biometric Core Technology Luminary Innovatrics serves over a billion users in 80 countries around the globe. Its flexible multimodal biometric technologies can be deployed on-premise, enabling compliance with the complex and intimidating regulatory landscape of our digitized era. The company is renowned for its fast and accurate face and fingerprint biometrics, which are developed in-house, and contribute to its Digital Onboarding Toolkit (DOT)—Innovatrics' full-stack technology for developing remote identity applications. Billed as a one-stop-shop for remote identity verification thanks to its face matching, facial liveness, ID document OCR, and NFC reading capabilities for ePassports, DOT has been deployed around the world, enhancing security and user experience in a range of use cases, from financial services, to telecoms, to government applications.

The versatility of Innovatrics' biometric technology is on full display in Southeast Asia, where DOT contributes to the eKYC services provided by ASLI RI, a biometric security provider that specializes in government services ranging from law enforcement to voter registration. In Thailand, Innovatrics' technology enables unsupervised identity verification for the ThaID mobile app. And when government and finance overlaps in Malaysia, DOT helps with onboarding and authentication for the country's top retirement savings fund. Taking a global perspective, international consumer finance provider Home Credit deployed DOT and Innovatrics' Trust Platform—which enables biometric de-duplication—to simplify onboarding through its native app. Now Home Credit can enroll more than 100,000 customers daily in four of the nine countries it serves. The process used to cost $20 per customer, now it costs just $0.05. It takes five minutes, and is untethered by geographic restrictions. That's the power of having biometrics at the core: material benefits for relying parties and intuitive inclusion for end users..

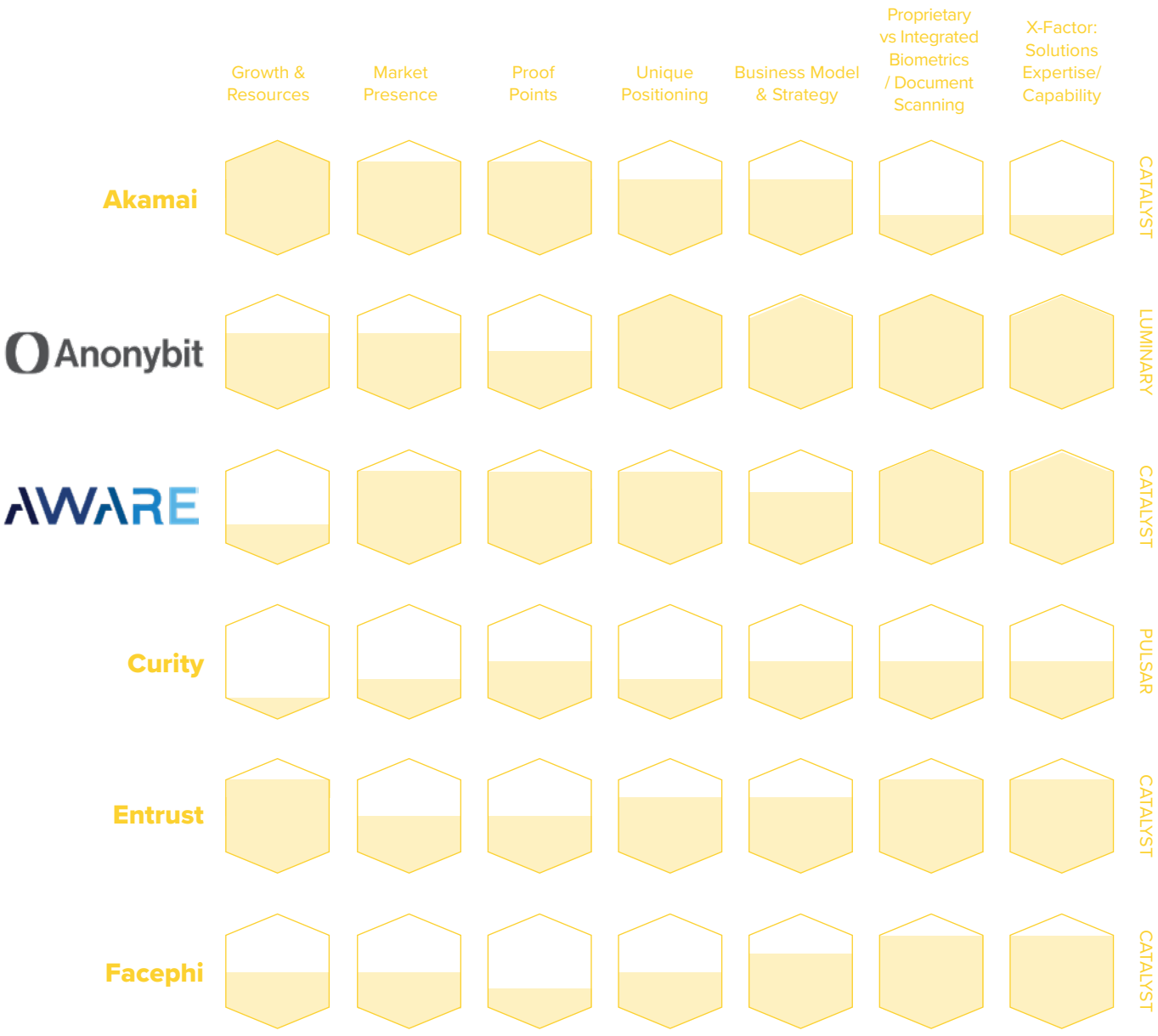
Contact Innovatrics: info@innovatrics.com

Identity Platforms

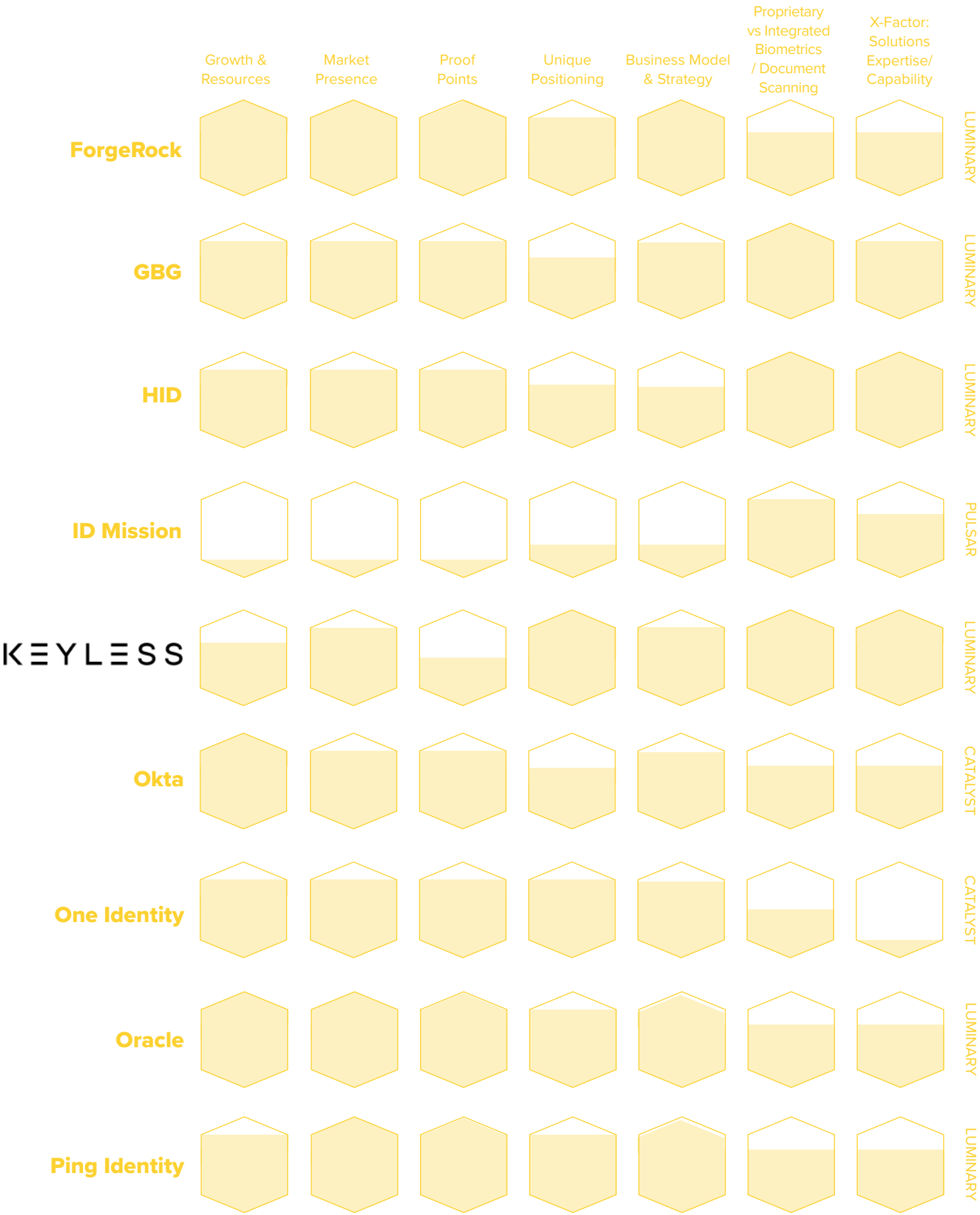
Identity platforms that enable end-to-end orchestration that may or may not be built on a foundation of biometrics.

Prism XFactor: Solutions Expertise/Capability

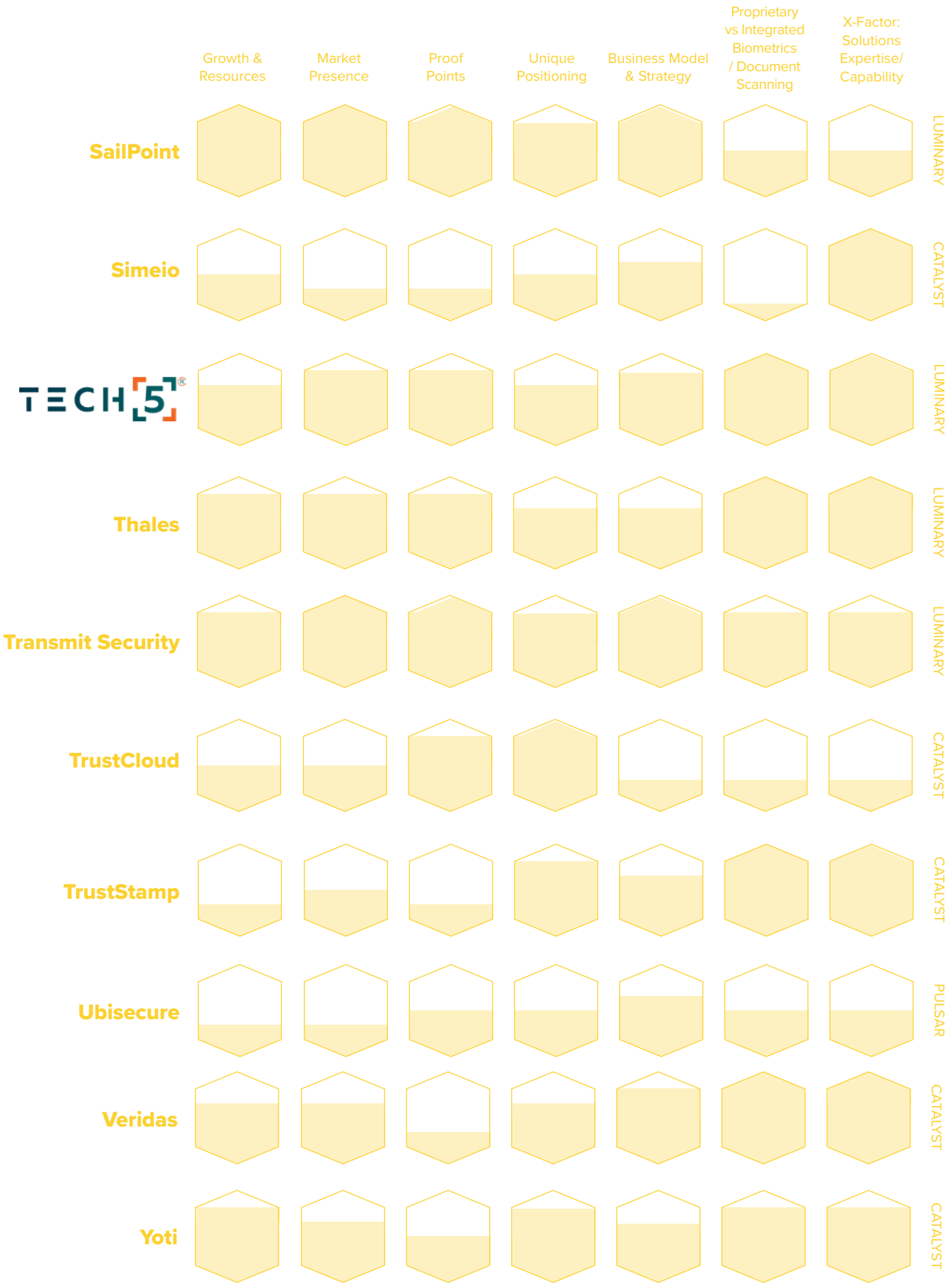
Evaluations



Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project

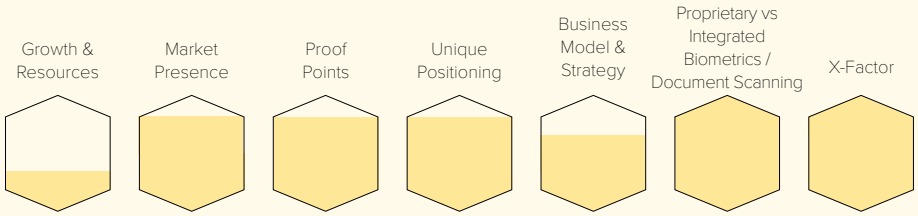


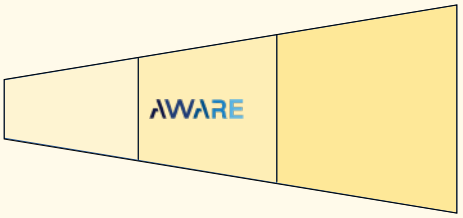
Prism Ver. 1.0 © 2024 The Prism Project

Aware

aware.com

BEAM: **Identity Platform** / CLASSIFICATION: **Catalyst**





Offering a range of proprietary biometric technologies that span every modality, Aware is an identity platform vendor operating on a global scale that puts biometrics at the core of financial services, government services, travel, hospitality, and enterprise applications. Founded in 1986, the company has its roots in government and law enforcement, playing an important role in the FBI's first large-scale fingerprint digitization effort over 30 years ago. In the interceding decades, Aware has evolved with the biometric digital identity space, earning a reputation of being ahead of the curve thanks to its oracular R&D efforts. Its broad product portfolio is versatile, modular, and boasts a track record of tamping down fraud, enabling compliance, improving operational efficiency, and enhancing customer experience.

Faster Finance Without the Fraud

In financial services, Aware has seen measurable success in reducing fraud, enabling compliance, and speeding up customer wait times while improving user experience. And it's not just during our current moment of accelerated digital transformation where we see evidence of its leadership. Aware has a long history of guiding its financial customers on their identity journeys, evolving along the way. When the 2008 financial crisis hit, and a Fortune 500 bank needed to meet new regulatory requirements, Aware's technology enabled that compliance. When a Brazilian bank needed to keep fraud down during a five-year period of 10x growth, Aware rose to the occasion. And when a Turkish retail bank was facing challenges brought on from the 2020 pandemic, Aware's biometric identity platform solutions helped improve its operations to make it a regional leader.

Arriving With Biometrics

Aware's broad portfolio makes it well suited for the competitive challenges of the travel and hospitality space, too. In an arena where stakeholders need to consider everything from customer loyalty, to national security, to passenger experience, a versatile platform approach to identity is required. From its Knomi SDK, to its Biometric Services Platform (BioSP), to AwareID—which enables biometric onboarding along with liveness-supported face and voice matching—Aware offers a full spectrum of solutions to tackle challenges while maintaining biometrics at the core of identity. The results speak for themselves: a leading air transport IT company deployed Aware's technology to allow guests to initiate the international border crossing process from home and saw its costs reduced by a factor of ten.

Building Biometric Governments

With such deep roots in the government sector, it is no surprise that Aware is well suited for the market. Aware's multimodal biometric components and BioSP platform are Commercial Off-The-Shelf (COTS) products, making them ideal for agencies that need to deal with the byzantine complexities of budgetary restrictions and funding approval processes. Aware's technology is proven reliable though extensive deployments in government use cases—these solutions are developed, tested, and ready to deploy. That's what makes it the biometric digital identity vendor chosen by numerous government agencies including UK Home Office, Australian Department of Defense, U.S. Department of Defense, and U.S. Customs and Border Protection. From how we manage money to how agencies protect our borders, Aware is ready to orchestrate the full range of identity lifecycle transactions on the terms demanded by its various customers.

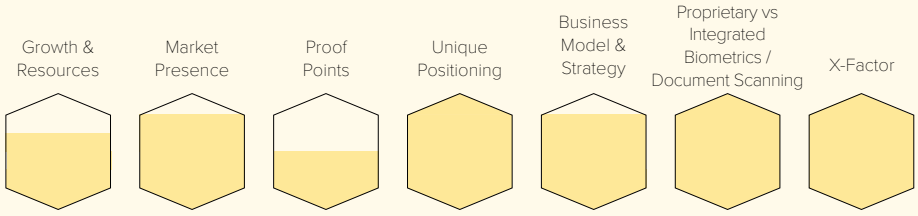
Contact Aware: sales@aware.com

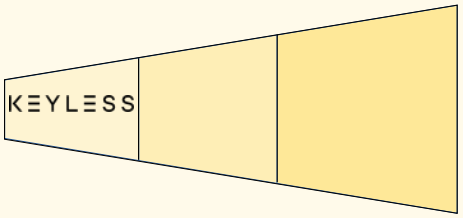
Keyless

keyless.io

KEYLESS

BEAM: **Identity Platform** / CLASSIFICATION: **Luminary**





Driven by a mission to create a safer, more private world, Keyless is a 2024 Flagship Prism Luminary. Tackling data privacy concerns head-on with its patented Zero-Knowledge Biometrics technology, this identity platform provider ensures compliance with stringent regulations like GDPR via an elegantly simple concept: it doesn't store biometric data on devices or in the cloud. That privacy-by-design aspect is made accessible through its seamless integration process, which allows its customers to easily upgrade their authentication from old and outmoded identity controls like SMS OTP, and to benefit from orchestration across the full user lifecycle, from onboarding through account recovery.

Uniquely Positioned With Innovative Technology

Offering a single-sign-on experience that puts user experience first, Keyless positions true user identity as the primary credential for all transactions. A selfie enrollment is all it takes for users to authenticate across multiple devices with ease. Keyless has integrated with risk platforms that enable step-up authentication when required. This approach ensures protection against account takeover fraud in authenticated sessions without treating every customer as if they are potentially a bad actor. Further solidifying its Luminary position in the Prism, the company enables fully automated account recovery secured by biometrics. This not only cuts down on help desk costs for its clients while making the process easy for end users, but it also closes one of the most vulnerable fraud gaps in digital security systems.

Biometrics at the Core of Banking

It was the cost of legacy authentication methods that drove a regional bank to turn to Keyless. Spending millions of dollars annually on customer support and SMS OTP second factor authentication, it needed to minimize its costs while shoring up its fraud protection. Of course, in the competitive financial services landscape where additional friction can lose customers, this had to be managed discretely. Replacing knowledge-based authenticators with facial recognition, the bank reduced its annual password and account management costs by millions. It bolstered its protection against account takeover fraud, improved user experience, and Keyless' platform significantly reduced customer service calls thanks to its automated account recovery. With biometrics at the core, getting back into your bank account only takes a single glance.

Enabling Healthy Identity Practices

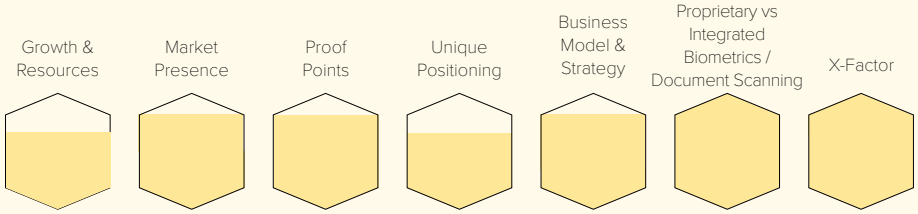
The healthcare sector is facing an identity crisis. Medical data is the most valuable type of user information on the black market, healthcare record transfer compliance regulations are unforgiving, and a medical emergency misidentification can be a matter of life and death. But digital transformation challenges in the sector have kept most identity leaders at bay.Keyless is an exception. A government-funded regional healthcare provider responsible for serving tens of thousands of patients and medical professionals across a sizeable number of European clinics and hospitals deployed Keyless Consumer Authentication to solve its significant digital transformation challenges. It immediately revolutionized its authentication process resulting in a 64% reduction in account takeover fraud. The implementation took only two months to deploy and serves as an example of how Keyless' privacy-forward biometric platform is making inroads for secure identity.

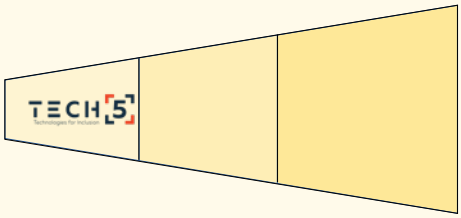
Contact Keyless: info.keyless.io

TECH5

tech5.ai

BEAM: **Identity Platform** / CLASSIFICATION: **Luminary**





With a formidable portfolio of high-performance biometric solutions, TECH5 is an Identity Platform Luminary in the 2024 Biometric Digital Identity Flagship Prism. With a leadership team spanning Switzerland and the United States, its focus on multimodal biometrics boosted by AI and machine learning has consistently placed its fingerprint, face, and iris recognition algorithms at the top of the National Institute of Standards and Technology (NIST)'s performance rankings. With 20 years of expertise and a track record of innovation, TECH5 is an example of how being on the cutting edge of R&D doesn't have to come at the expense of practical application.

A Reputation for Innovation

A known innovator, TECH5 places a strong focus on research and development, notably building solutions for contactless fingerprint capture; 1:N identification via face, fingerprint, and iris recognition; 1:1 biometric authentication; digital ID generation and issuance; and recently, biometric template protection for its multi-biometric matching system. Its proprietary, high-performance biometric solutions are only part of the story. TECH5 notably addresses the ESG challenges of digital transformation by striving to deliver inclusivity through biometrics. By introducing new methods of biometric portability, like its 2D Digital Storage for Biometrically Verifiable Digital ID, this Prism Luminary is stoking sustainability by ensuring users in developing countries can access their right to identification

Strong Identity Around the Globe

TECH5 has proven itself instrumental to large-scale identity projects around the world. From providing biometric voter registration for elections in Jamaica and Oman, to facilitating better border control with Finland's Digital Travel Credential (DTC)—the company is helping put biometrics at the core of modern life. TECH5 is enabling digital democracy, easing international travel, and building identity-first government services for our digital age, as can be seen in its work with the Mauritanian Ministry of Digital Transition, Innovation and Public Sector Modernization (MTNIMA). Participating in a pilot project between 2022 and 2023, the company helped put the Mauritanian government on track to be among the first countries in the world to adopt a national ID grounded in biometrically-bound foundational identity.

Consistent Commitment to Identity Excellence

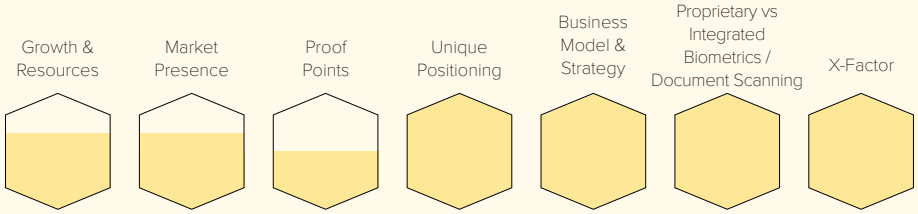
Large-scale identity projects aren't outliers for TECH5. They are increasingly becoming the sweet spot for this Prism Luminary. When a federal government in Africa wanted to provide services to a large unbanked population, TECH5 delivered. Supported with funding from World Bank, the UN, and its own treasury, the government worked with TECH5 to deploy the company's digital identity infrastructure solution. TECH5's platform was implemented in only three months, and the country can now to create and distribute digital identity documents to every citizen, providing the foundations needed for economic and social participation. It's another example of how TECH5's inclusive mode of innovation and collaboration can make life better for everyone.

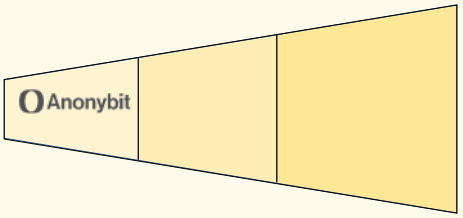
Contact TECH5: sales@tech5-sa.com

Anonybit

anonybit.io

BEAM: **Biometric ID Platform** / CLASSIFICATION: **Luminary**





Anonybit's one-of-a-kind biometric digital identity platform takes a unique approach to data storage, breaking up biometric templates into encrypted fragments and distributing them across a network. This approach naturally eliminates honeypot risks while protecting user privacy and enabling convenience without sacrificing security. Its flagship product, Anonybit Genie, unifies the user lifecycle, carrying strong identity assurance from onboarding to authentication and account recovery. Bolstered by Anonybit's decentralized biometric cloud and decentralized data vault, Genie supports all biometric modalities and clocks amazing speeds, preforming 1:1 matching in under 200 milliseconds and 10 million 1:N searches in a split second.

Its breadth of application demonstrates how the identity principles championed by Anonybit are central to life in the age of digital transformation. With Anonybit, hospitality chains of all sizes can streamline customer experience, enhance compliance posture in relation to GDPR, CPRA, and other, emerging regulations, while also bringing a secure and convenient element to guest flow. In the public sector, the company's decentralized approach to storage and matching ensures that the data breaches of the past—like the 2015 Office of Personnel Management (OPM) disaster—are impossible. And in the financial services sector, Anonybit is fighting in the fraud arms race. A Tier 1 Latin American bank is using its technology to prevent synthetic identities and account take over fraud, running 1:N matches on every account opening and 1:1 matches for every account recovery requests. Boasting zero processing failures to date, Anonybit is saving the banking group money through automation and defending it from modern identity threats. That's the power of biometrics at the core.

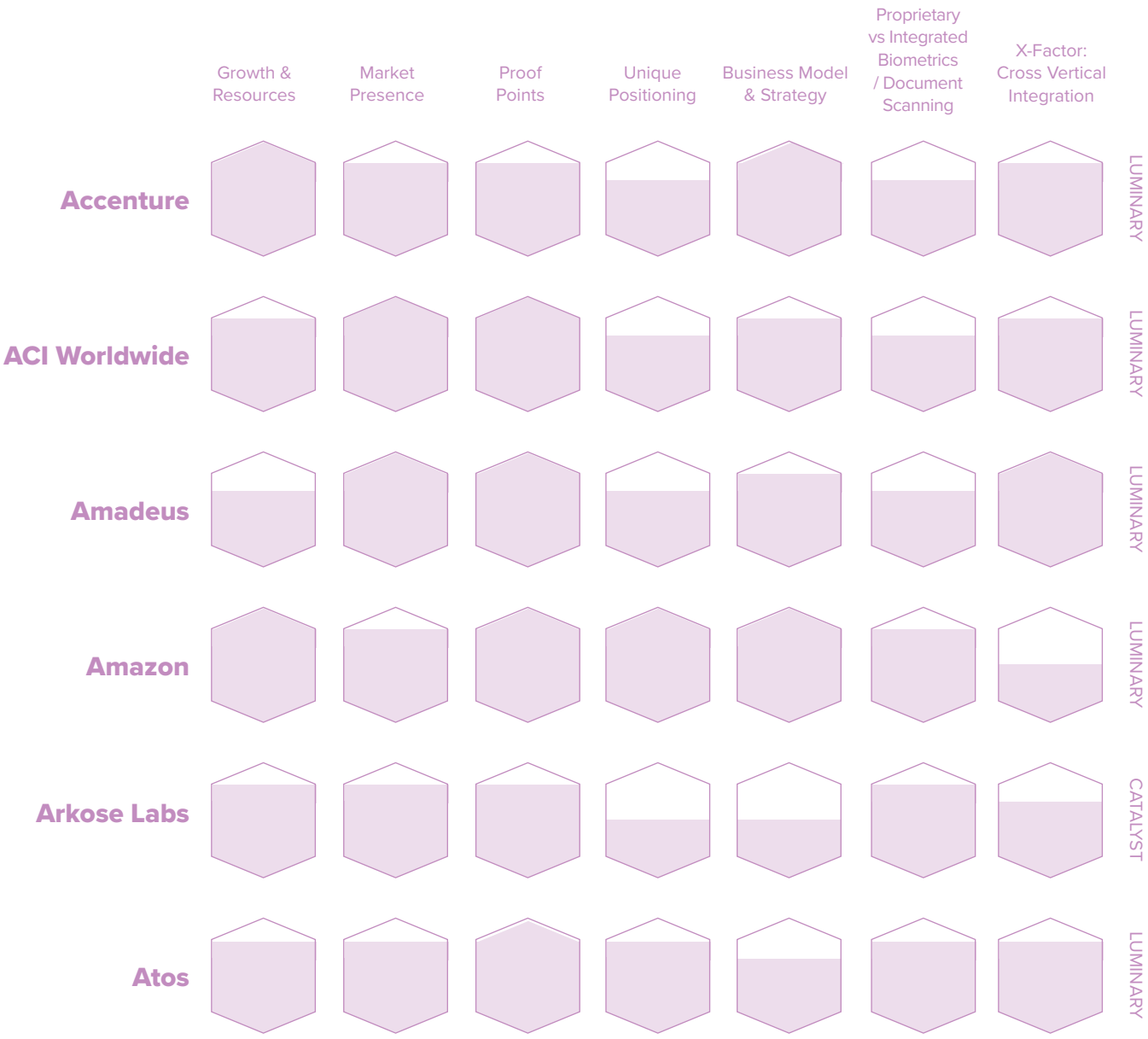
Contact Anonybit: info@anonybit.io

Solution Providers

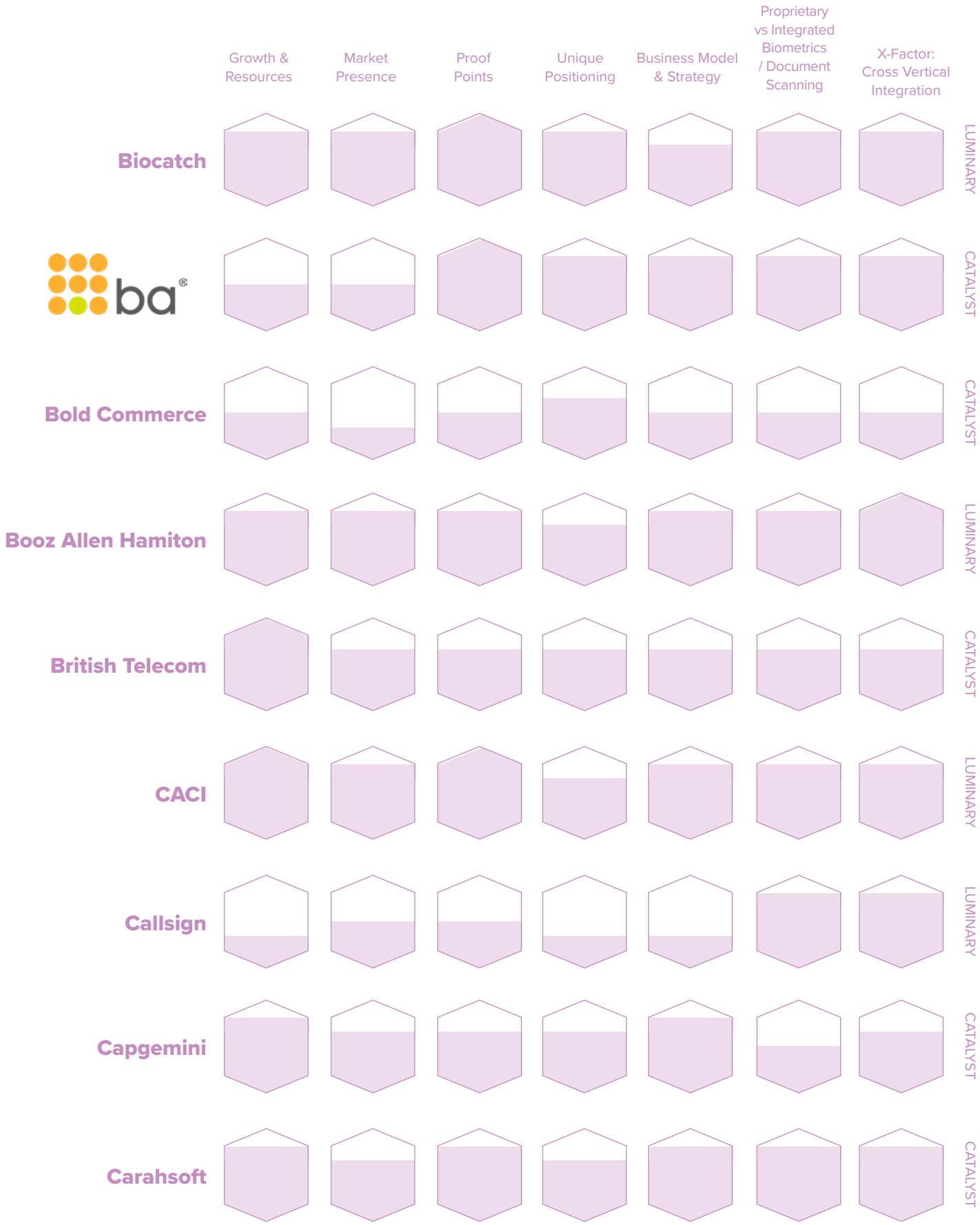
Purpose-built off-the-shelf and customized solutions designed to target specific verticals and/or specific identity-related enterprise challenges

Prism XFactor: Integrated Mobile Onboarding, Payments, Cross Vertical Integration

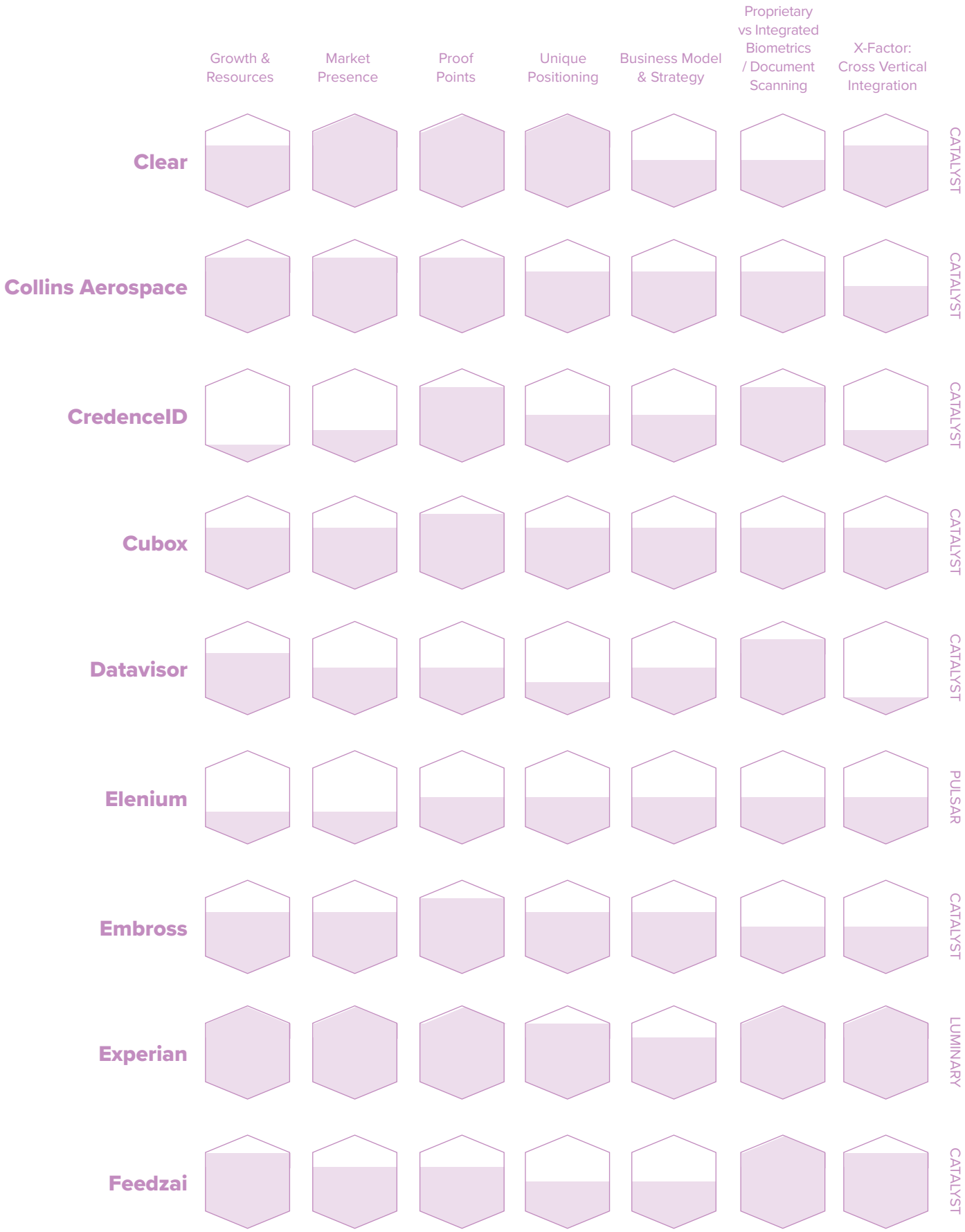
Evaluations



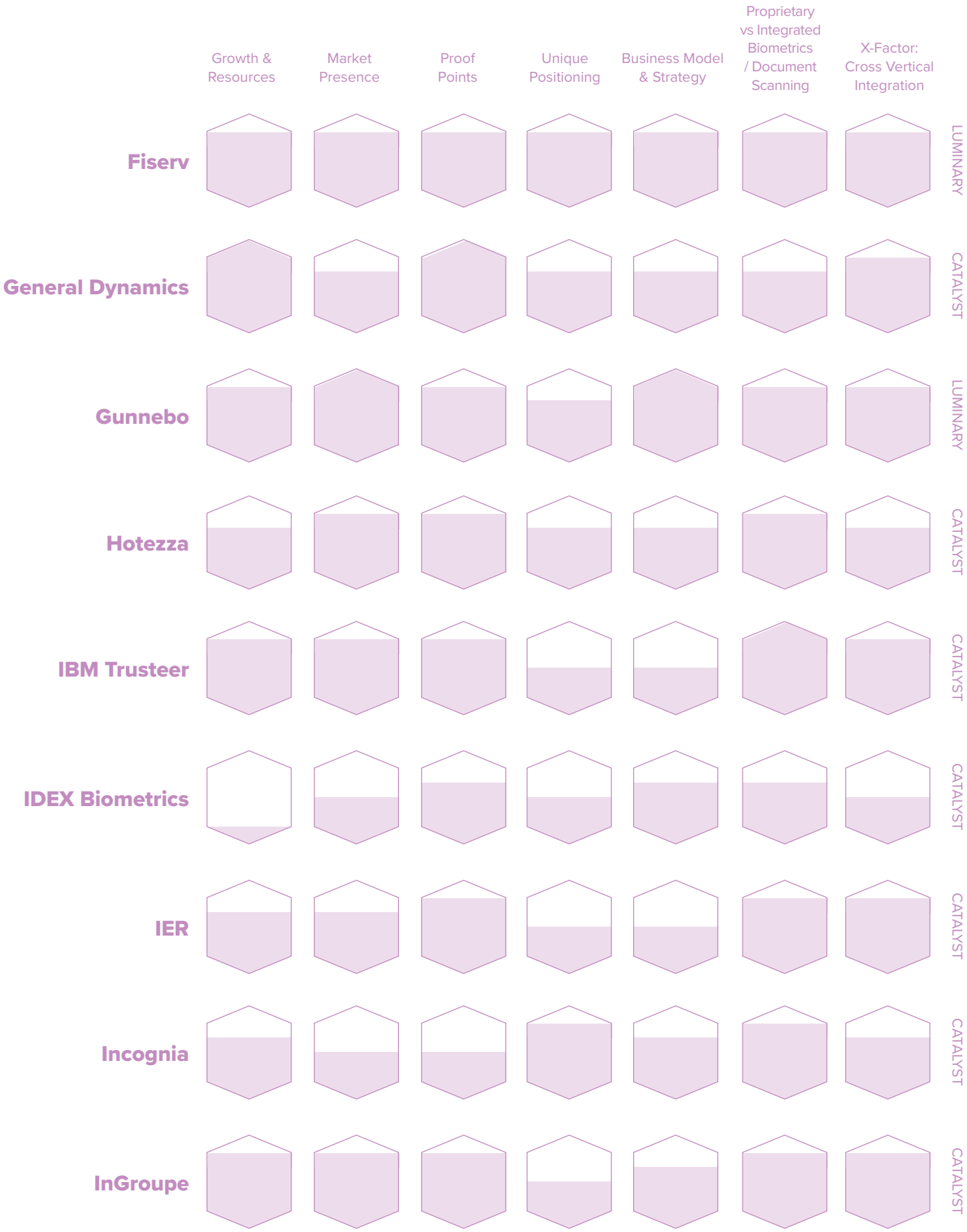
Prism Ver. 1.0 © 2024 The Prism Project



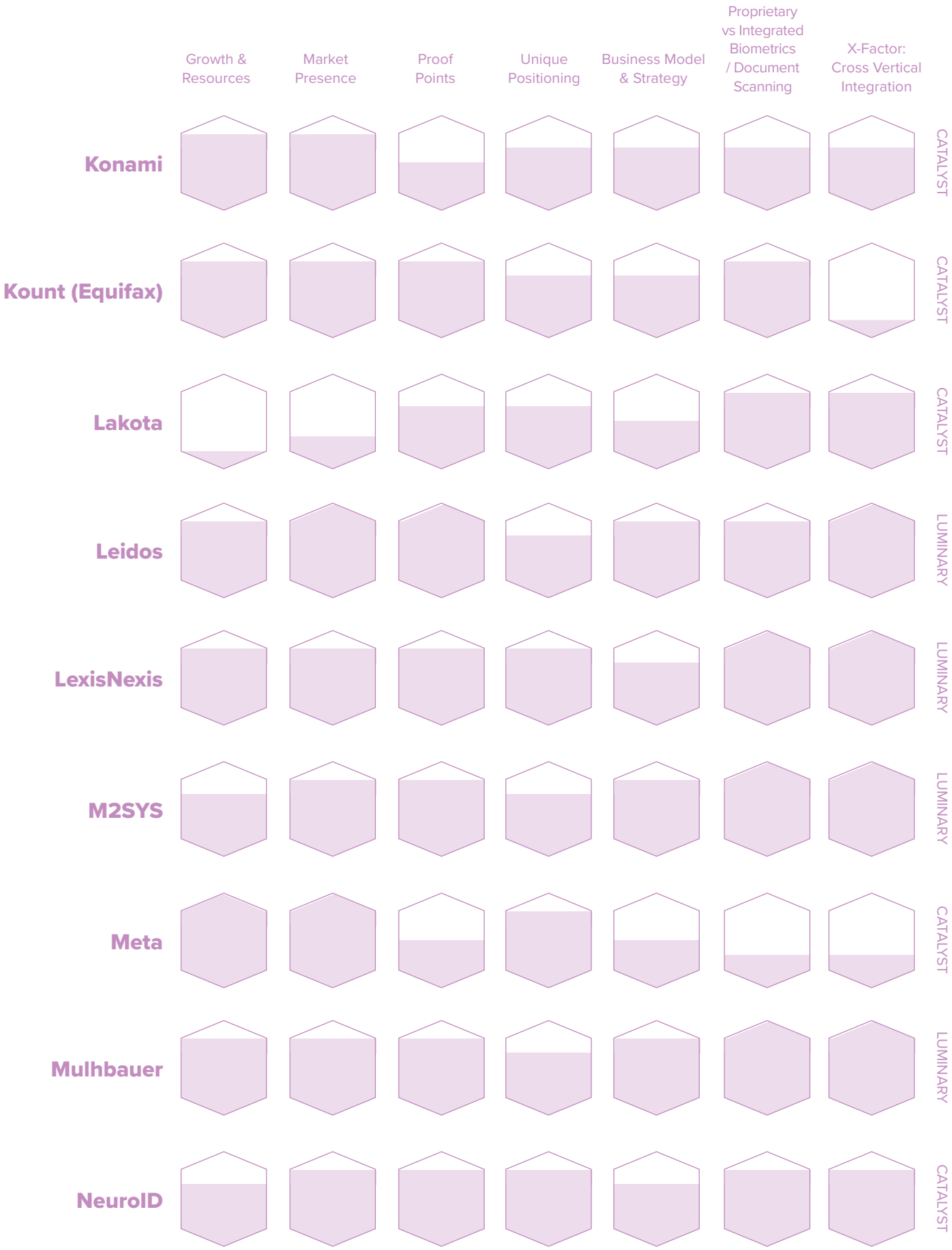
Prism Ver. 1.0 © 2024 The Prism Project



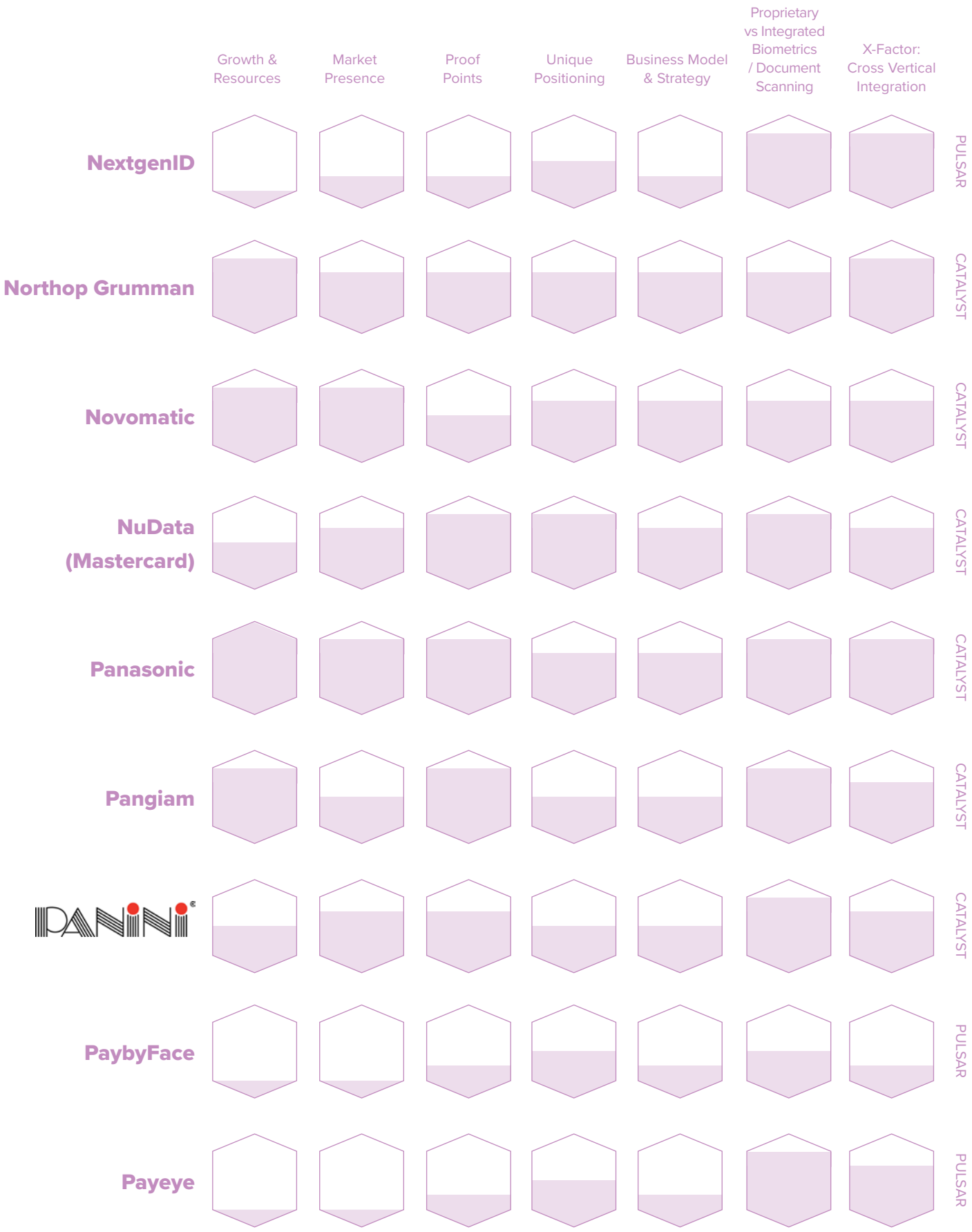
Prism Ver. 1.0 © 2024 The Prism Project



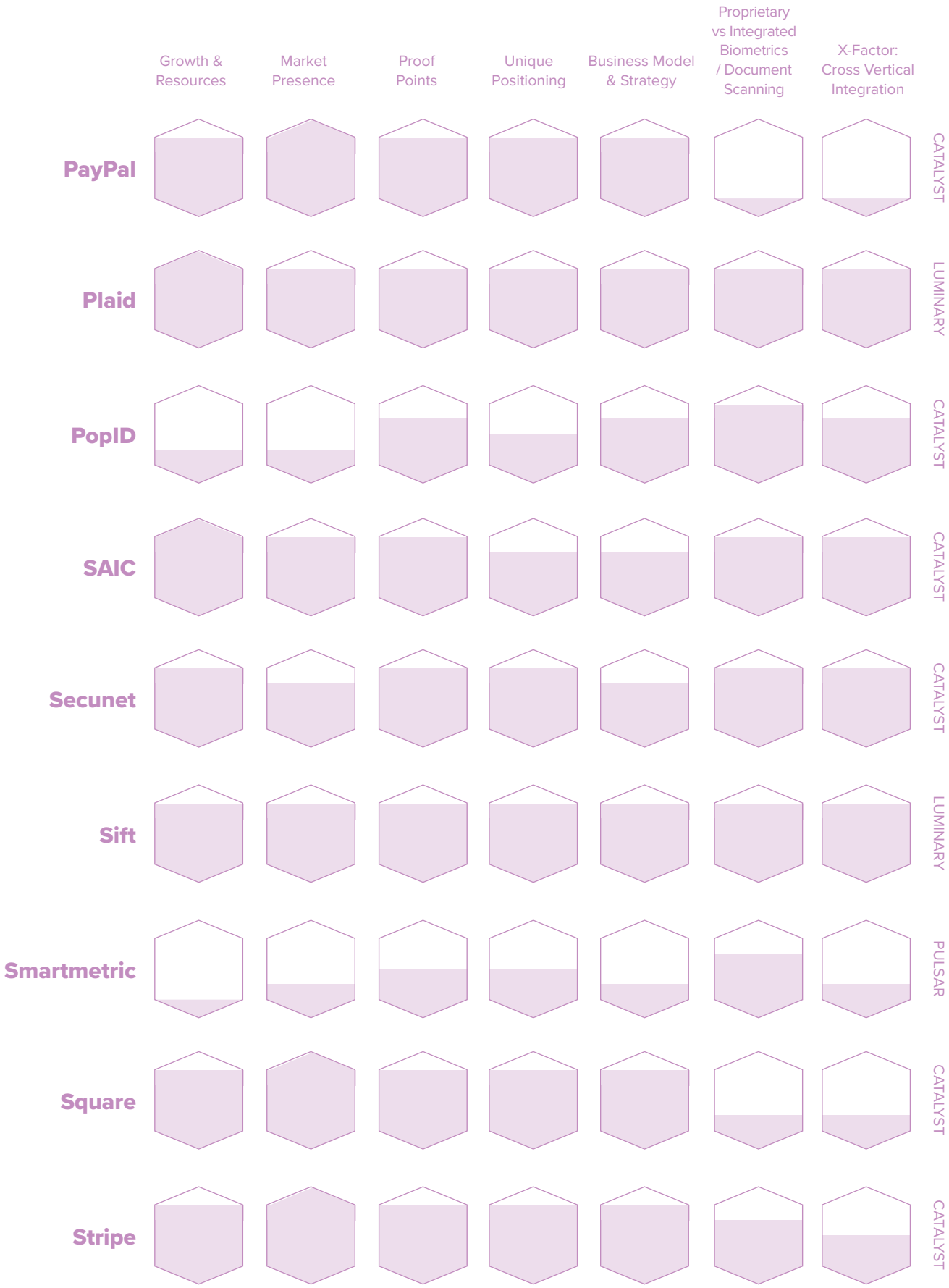
Prism Ver. 1.0 © 2024 The Prism Project



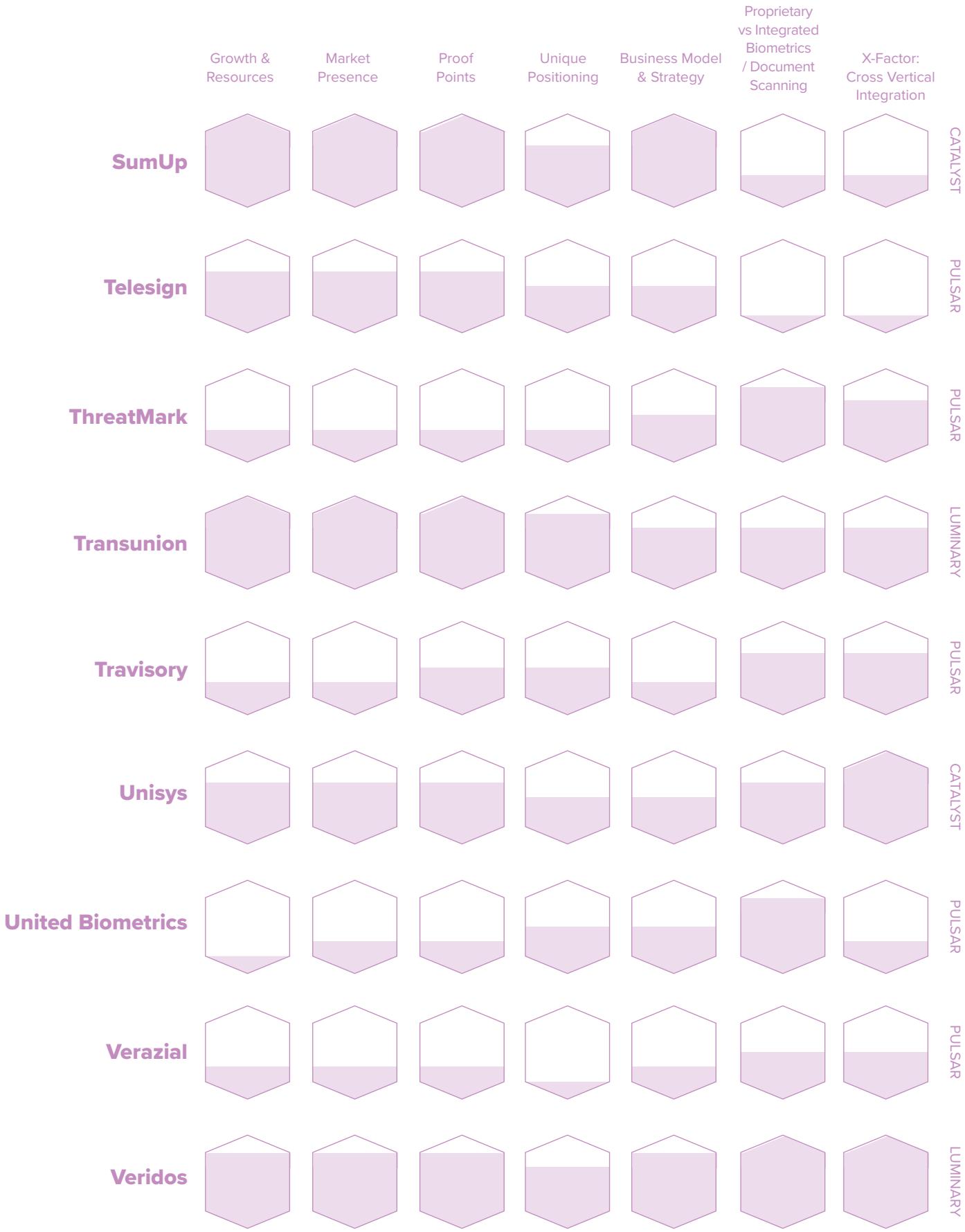
Prism Ver. 1.0 © 2024 The Prism Project



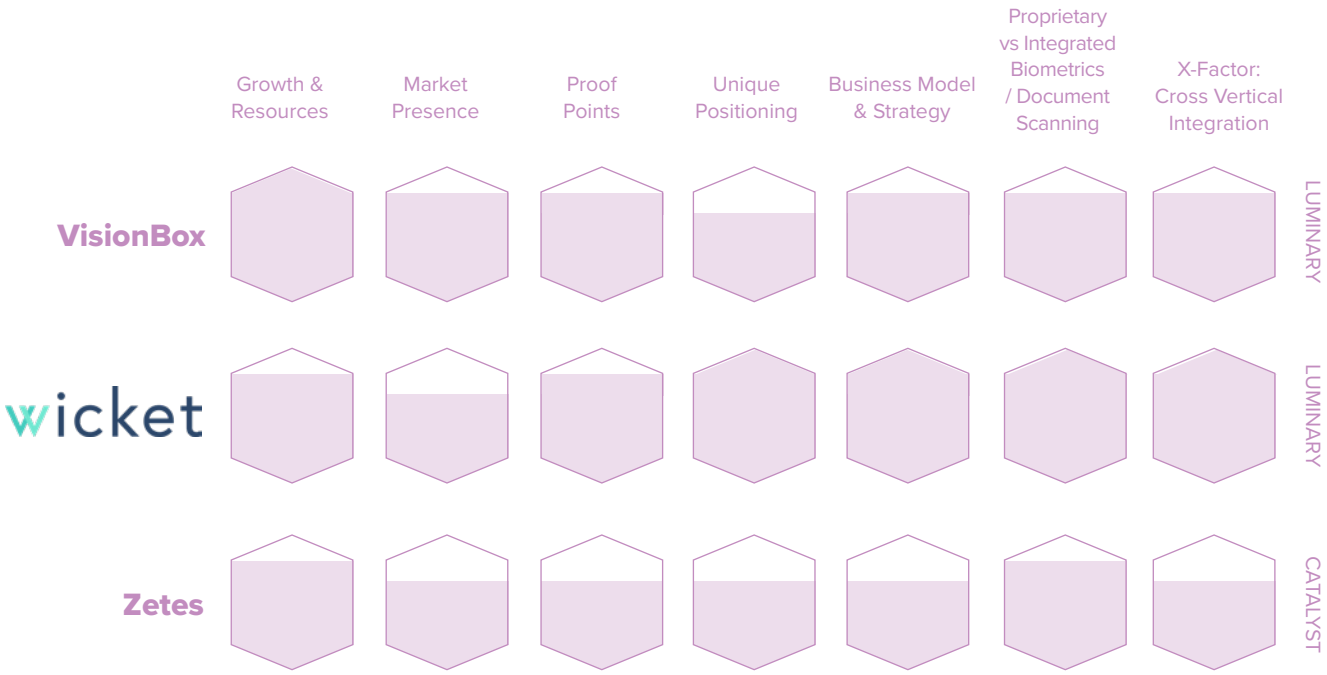
Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project

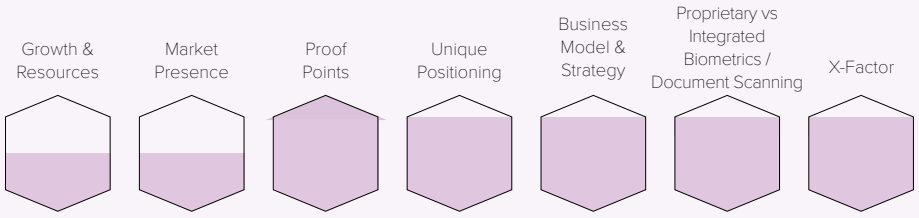


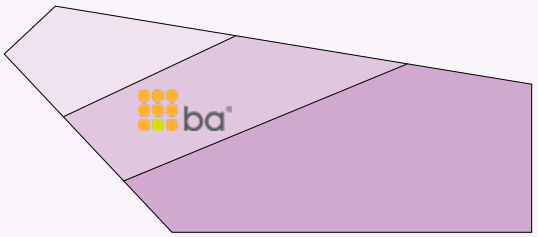
Prism Ver. 1.0 © 2024 The Prism Project

Biometria Aplicada

biometriaaplicada.com

BEAM: **Solution Providers** / CLASSIFICATION: **Catalyst**





Biometria Aplicada is a versatile Biometric Solutions Catalyst. Dedicated to solving difficult identity challenges through creative innovation, the Mexico-based company has risen to the occasion in our era of digital transformation, bridging the gap between legacy systems and the next generation of secure and convenient customer experience. It's ability to address longstanding, real world problems with intuitive and compliant biometric technologies has stood out particularly in the financial services space where the company is enabling financial inclusion.

In the realm of identity, the persistent challenges of Environment, Sustainability, and Governance (ESG) narrow down to inclusion and accessibility. Serving un-and-underbanked populations requires putting the needs of customers first while improving existing infrastructure, rather than replacing it. Biometria Aplicada facilitates this process through its EMi Plus and Identium Cloud solutions, which have vastly improved the onboarding and credit approval processes, in turn leading to better conversion rates and thus, greater inclusion.

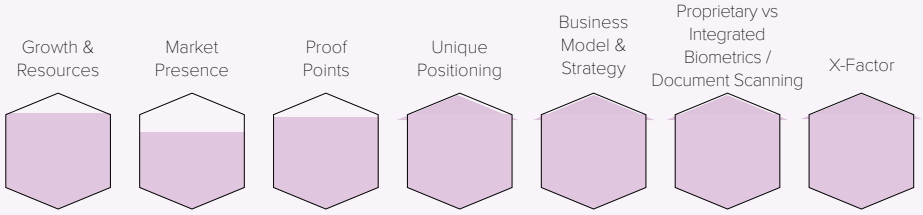
The company's pragmatic approach to deploying advanced technologies is further illustrated through its work with a National Pension Fund for State Workers based in Mexico City. After implementing identity document validation, fingerprint authentication, signature technologies, and video solutions—a process that took only one month—Biometria Aplicada helped the fund increase its service offerings while enabling safe and inclusive pensions. It is the hands-on innovation demonstrated here that shows the kind of forward-thinking practicality required for digital transformation to achieve its full promise.

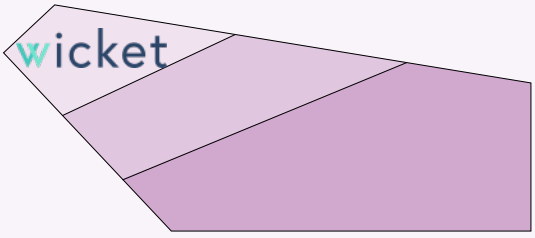
Contact Biometria Aplicada: ventas@biometriaaplicada.com

Wicket

wicketsoft.com

BEAM: **Solution Providers** / CLASSIFICATION: **Luminary**





To see how biometric digital identity is set to improve everyday life with privacy-forward secure convenience, simply look to the live entertainment space, where 2024 Flagship Prism Luminary Wicket is transforming the fan experience. The MA-based startup leverages facial recognition and mobile devices to enable trusted ticketing, seamless access, and frictionless payments while increasing automation and bolstering security for its client base, including 40 major stadiums and events venues. With customers across all major US sports leagues, the Australian Open, and several major trade conferences, Wicket is committed to collaboration, boasting a formidable partner network that includes industry defining names like Ticketmaster, Seat Geek, and Verizon. What it all adds up to is the perfect example of how making identity easy for the end user knits various transaction types together into one exemplary guest journey. And the best part m is: relying parties benefit from impressive ROI.

Anyone skeptical of how biometric digital identity can improve user experiences with intuitive and secure automation just needs to head to a Cleveland Browns game. The Browns adopted Wicket's Express Access solution to streamline facility entry, and in 2023 they expanded the deployment to further enhance the fan experience. Throughput improved significantly—so much that the team was able to reduce its number of entry lanes. The impact on cost was remarkable, with each Express Lane saving the team $8,000 per season. Once through the front gate, fans enrolled with Wicket are treated to automated concessions thanks to its Express Beer offering, which enables the purchase of drinks and snacks with a frictionless and fast face scan. And while the Browns saw a 171% return on investment, it was the fans who benefited most, saving thousands of hours normally spent waiting in line. With biometrics at the core, the wait is over—life, and gametime, can just be enjoyed.

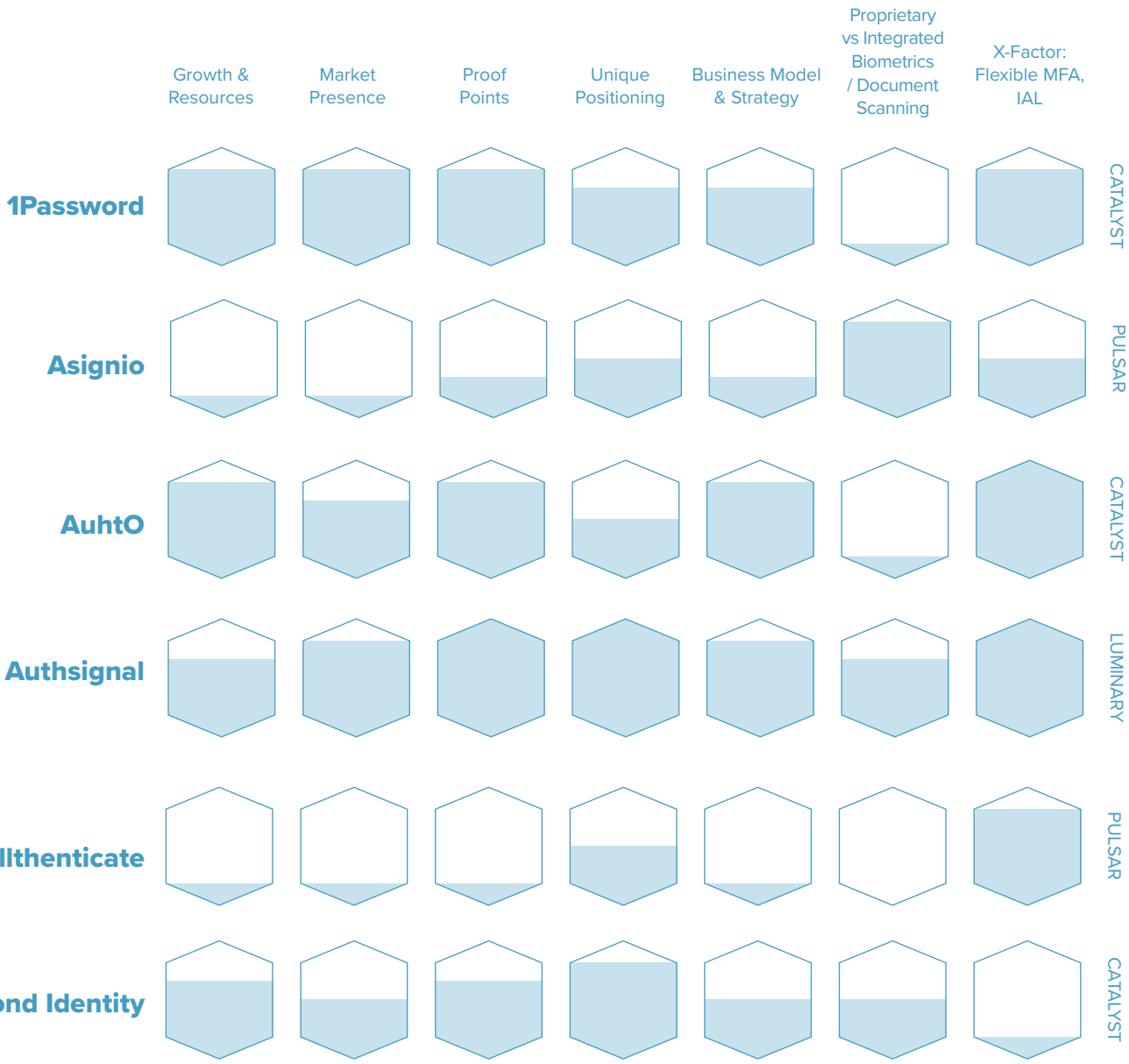
Contact Wicket: hello@wicketsoft.com

Authentication

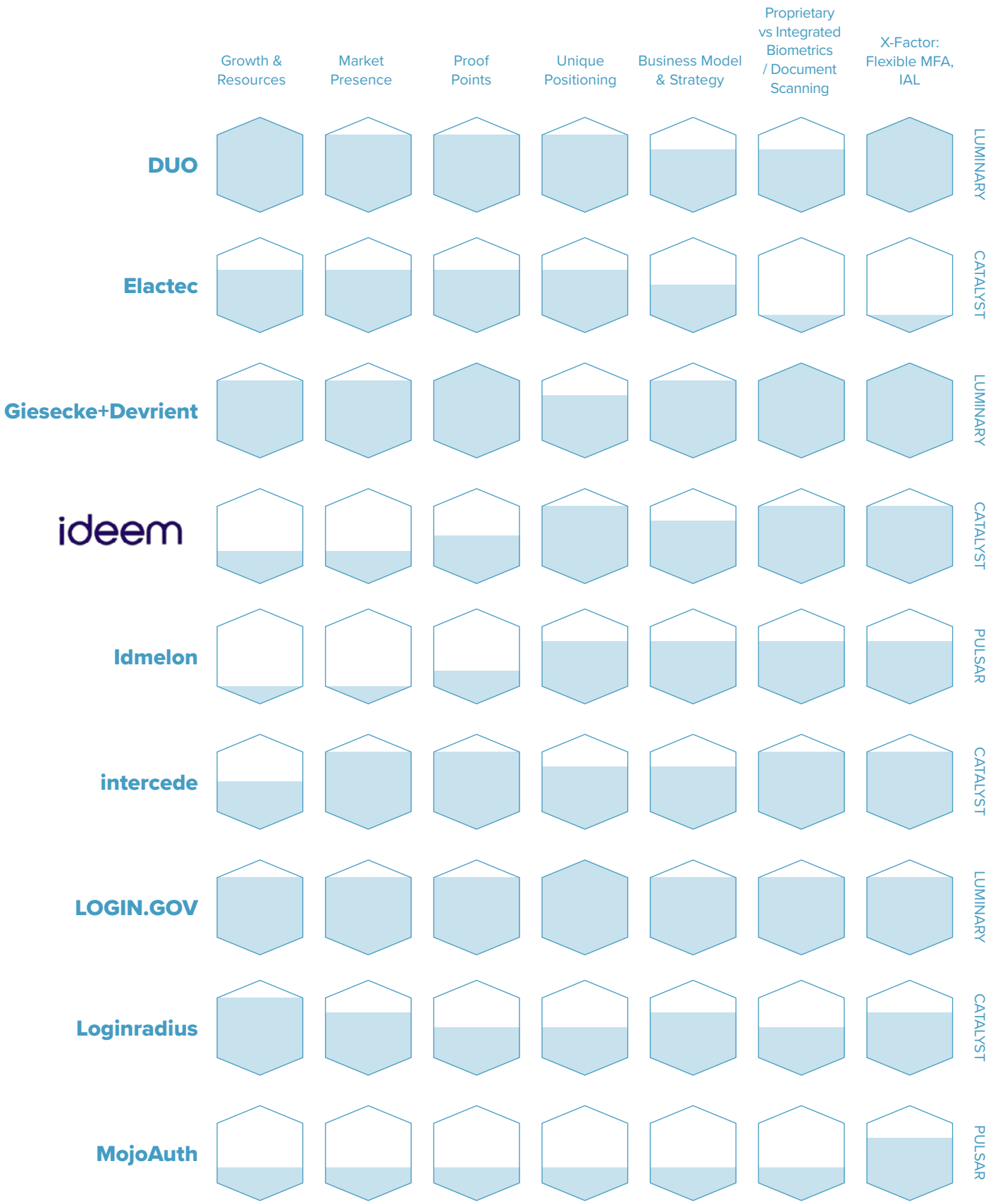
These vendors provide biometric and non-biometric security that links a digital identity to an individual for physical and logical access.

Prism XFactor: Flexible MFA (Multifactor Authentication), IAL (Identity Assurance Level)

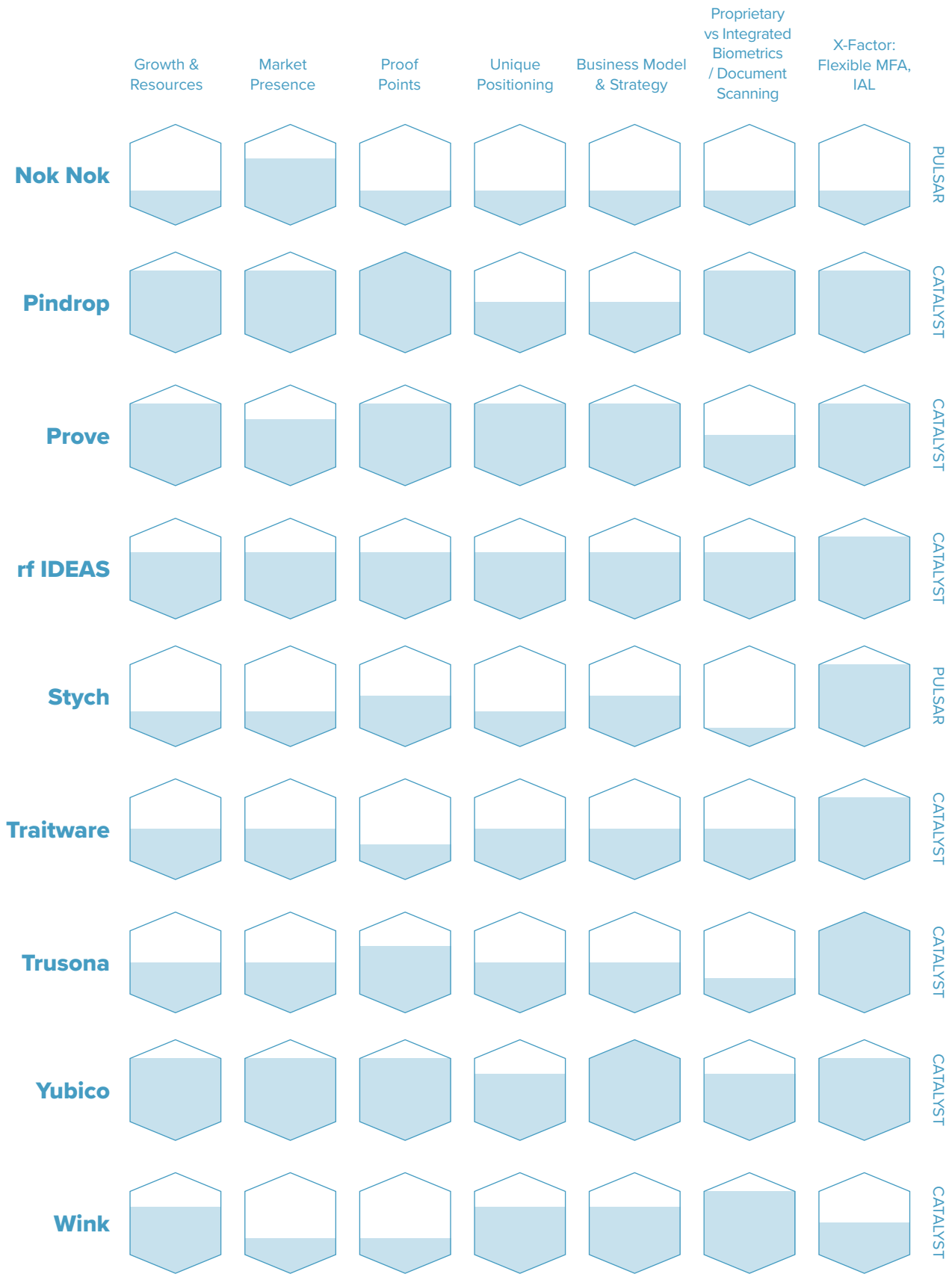
Evaluations



Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project

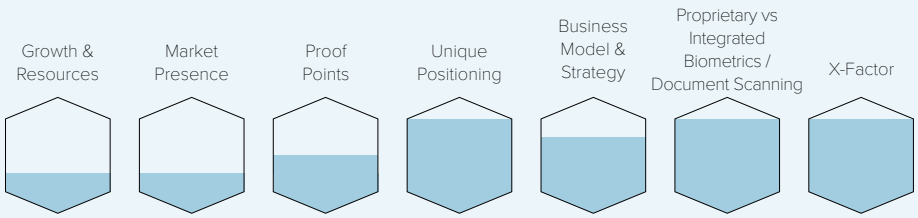


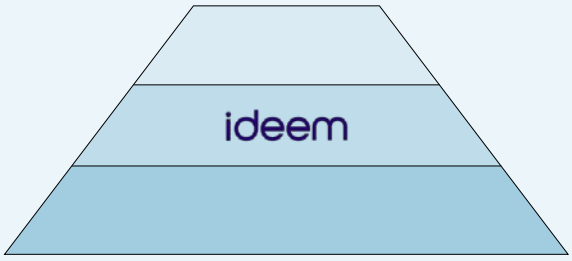
Prism Ver. 1.0 © 2024 The Prism Project

Ideem

useideem.com

BEAM: **Authentication** / CLASSIFICATION: **Catalyst**





Users need to buy-in to the incoming biometric digital identity paradigm, and that's especially true when it comes to the arena of authentication, where Prism Catalyst Ideem is making persistent two-factor authentication invisible. The customer experience in the era of digital transformation has little tolerance for added friction. A step-up authentication—particularly one-time passcodes (OTP) administered by token, app, or text message—is onerous and expensive. Ideem's ZeroTrust Secure Module (ZSM) software only solution allows for that second layer of authentication to persist, while completely eliminating the aspects that threaten user abandonment and a company's bottom line.

ZSM operates in the background of online sessions, leveraging persistent cryptographic device binding so that it doesn't need to be re-authenticated. Its advanced approach to device fingerprinting allows the second layer of user authentication to continue across interruptions that would otherwise terminate a session. Device restarts, cookie clearings, browser crashes, app deletions—users authenticated by ZSM don't need to suffer extra friction thanks to Ideem's NIST validated and FIDO2 compliant software.

Hardware agnostic and quantum safe, This Prism Catalyst's approach to next-gen device fingerprinting represents a paradigm shift in the "what you have" style security still widely deployed online. Paired with a biometrics-at-the-core level of foundational identity, this shift in 2FA perspective promises to be a powerful element in our digitized tomorrow.

Contact Ideem: useideem.com

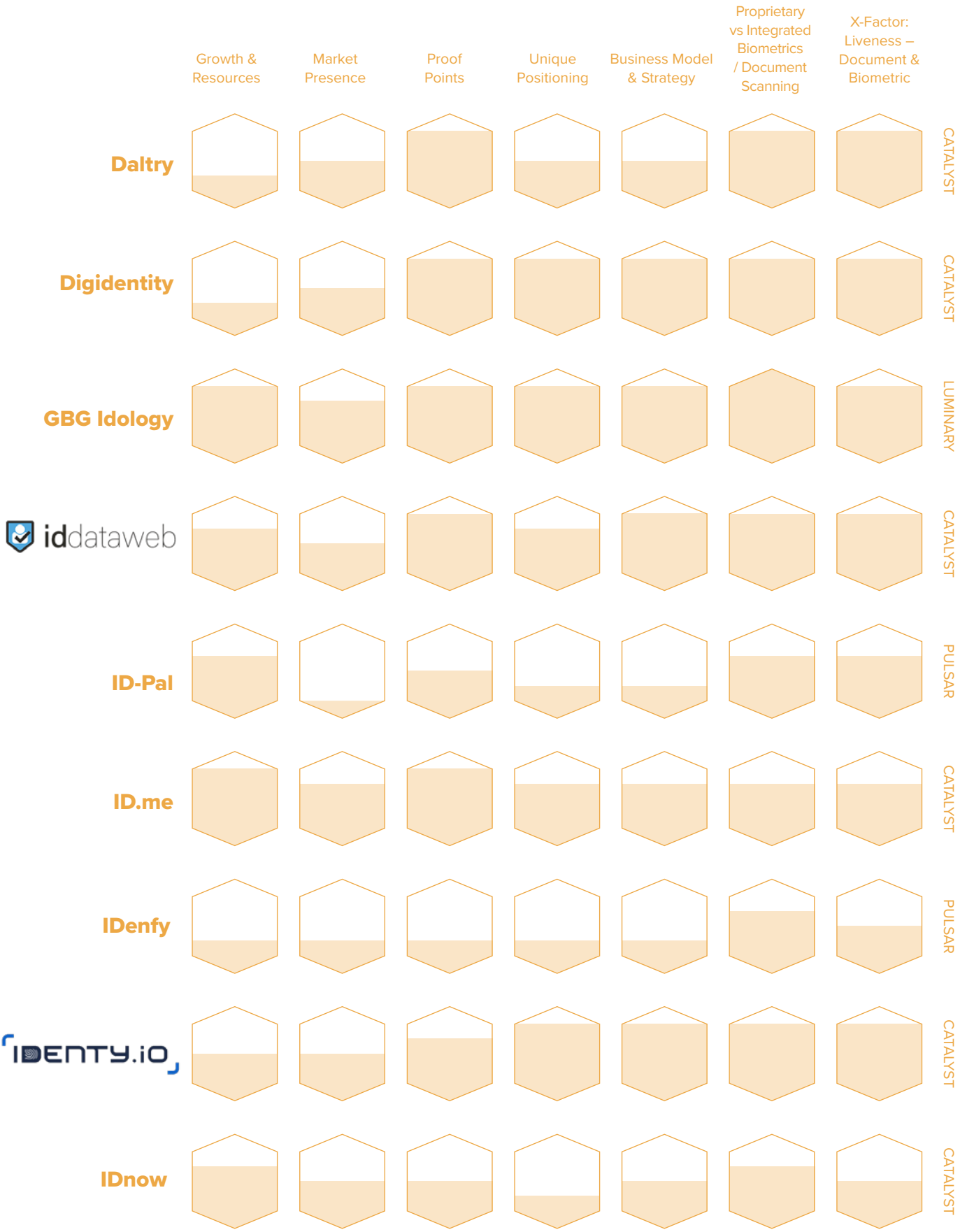
Identity Proofing and Verification

These vendors leverage biometrics, OCR, and NFC combined with various authoritative sources (SIM, device, geolocation, etc.) to enable onboarding and authentication for access to high-security and customer experience-enhancing applications.

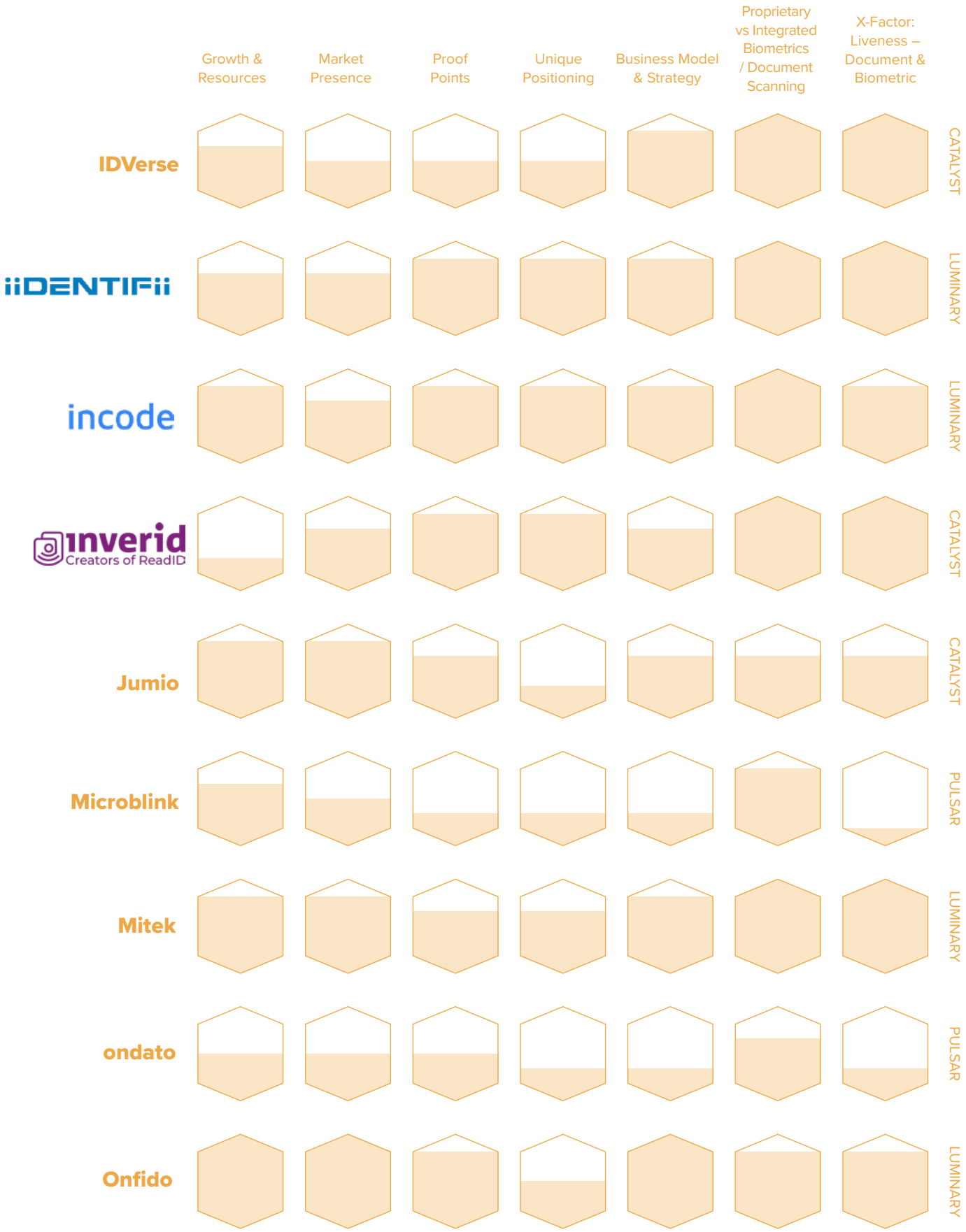
Prism XFactor: Document and Biometric Liveness

Evaluations

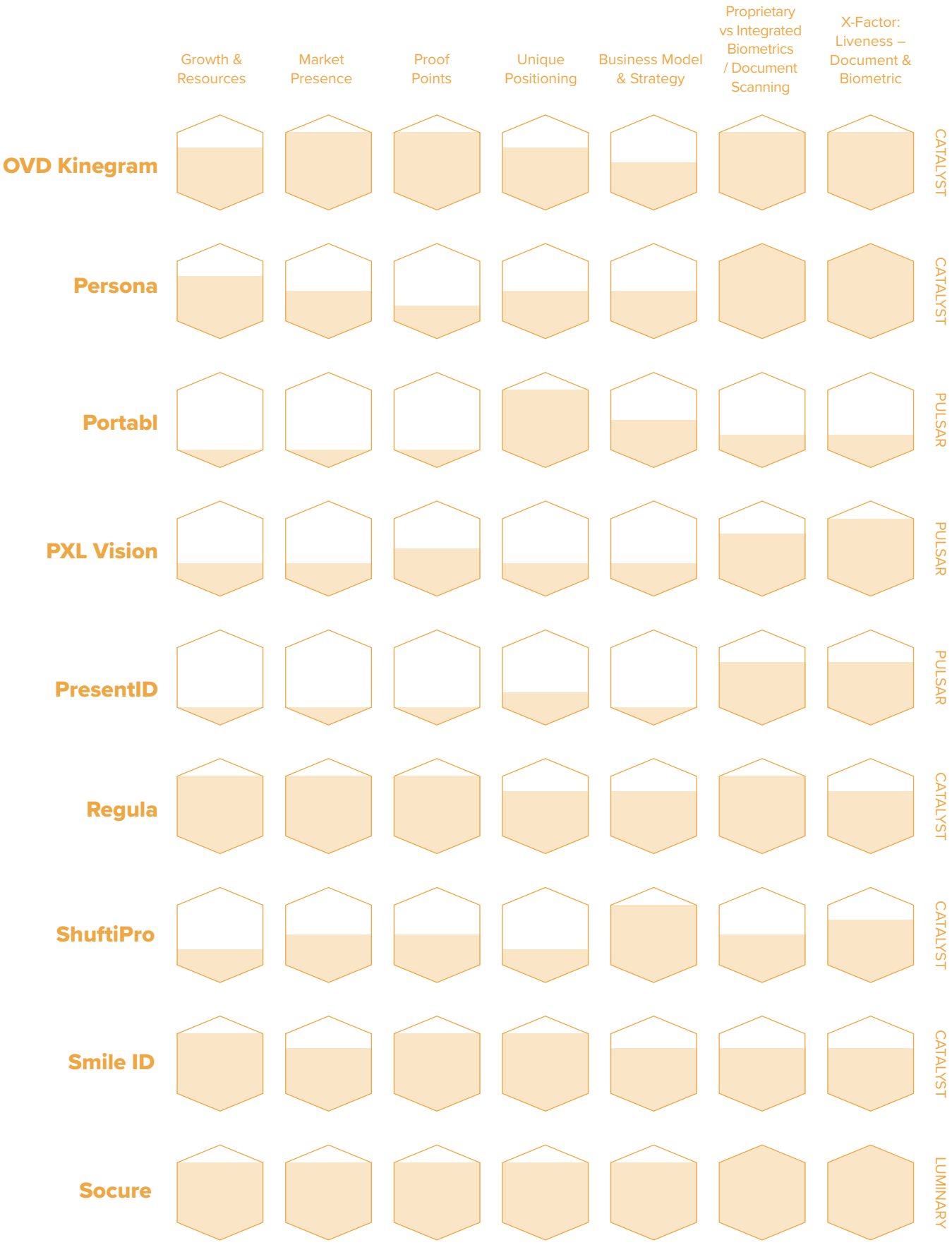
Prism Ver. 1.0 © 2024 The Prism Project



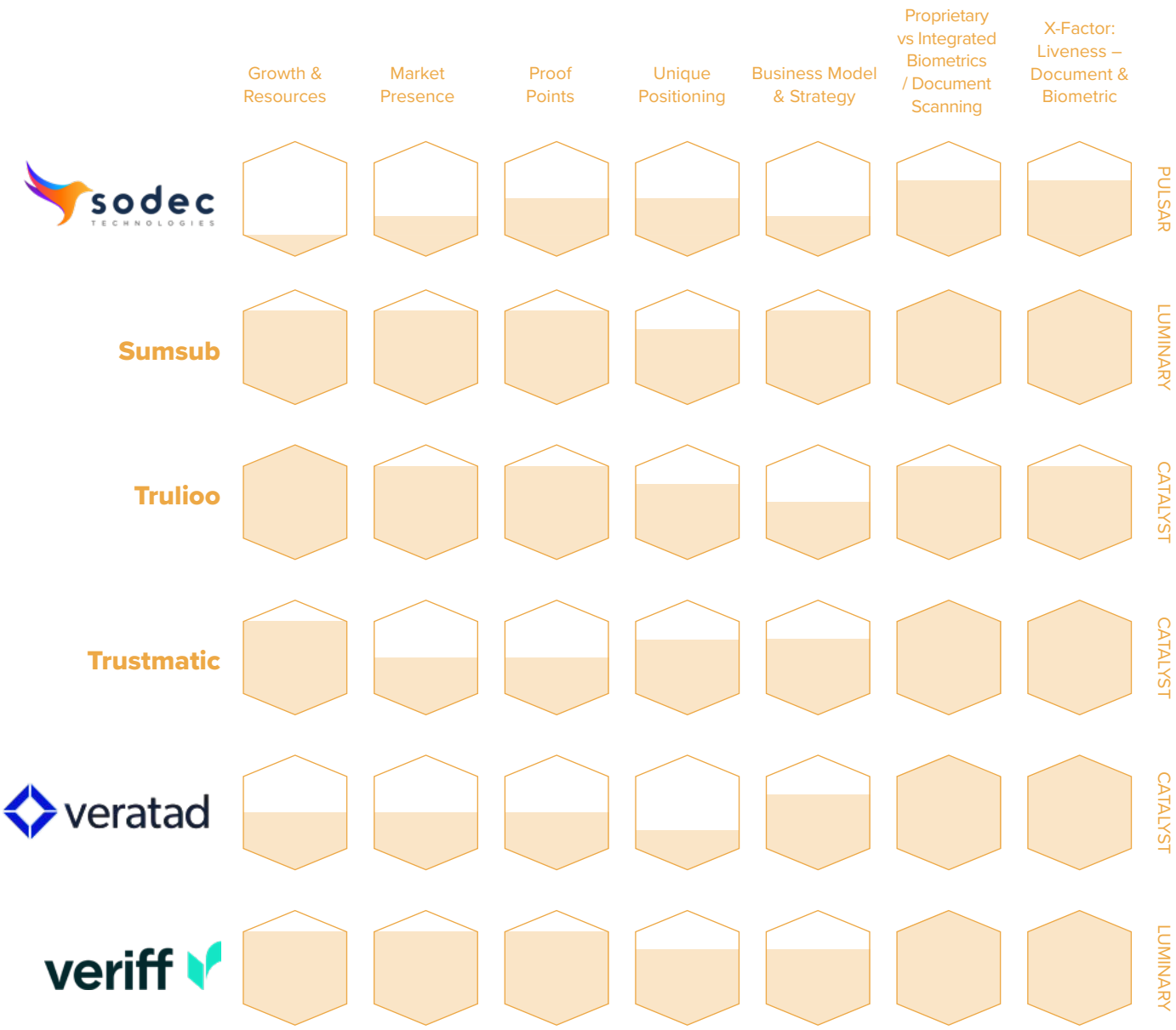
Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project
the-prism-project.com

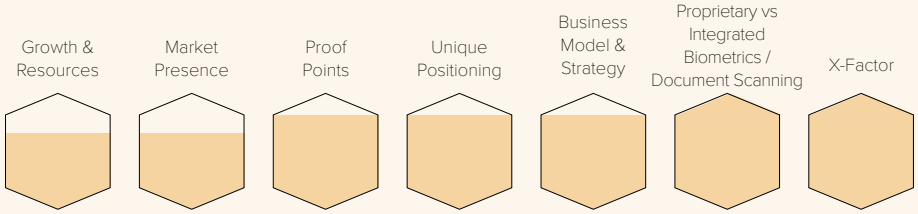


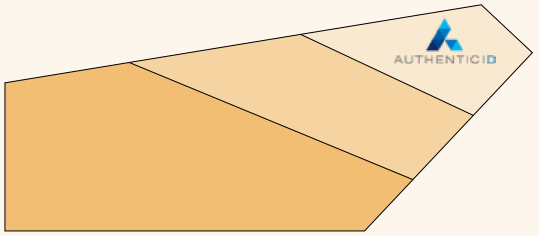
Prism Ver. 1.0 © 2024 The Prism Project

AuthenticID

authenticid.com

BEAM: **Identity Verification** / CLASSIFICATION: **Luminary**





Committed to combatting fraud and empowering users to confidently assert their identities in their own terms, AuthenticID shines bright as a 2024 Flagship Prism Luminary. Powerful identity proofing and verification technology underlies the company's fully customizable solution, which protects its customers from fraud, ensures compliance, and enhances operational efficiency. Supported by facial biometrics, liveness detection, and government ID matching, AuthenticID provides a friction-free onboarding experience for users while defending against the AI-powered cyberthreats that characterize this current era of widespread digital transformation.

Uniquely Positioned for Success

AutheneticID stands out in a sea of identity verification providers thanks to its strong track record of preventing fraud, as well as the inroads it has made in key marketplaces including financial services, telecom, government services, and workforce identity management. But its technology is where it shines brightest. Its AI tools limit biometric bias, and its computer vision technology allows for automated form-filling using biographic data. AuthenitcID's enterprise-scale solutions are hardware agnostic, can be implemented without system downtime, and achieve new heights of protection courtesy of its proprietary FraudShield service.

No Quarter for Known Fraudsters

The onboarding process is where fraud takes hold. Synthetic identity fraud is a $20-40 billion per year crisis, and it starts with the front door. Biometrics, liveness detection, and robust document scanning all play a role in preventing these problems, but recent innovations in AI are heating up the fraud arms race. AuthenticID's FraudShield offers an effective solution to bolster security during enrollment. When a user attempts to register for an account using AuthenticID, they upload a government issued credential and take a selfie. The software matches the user's face biometrics to the image on the ID in real-time, while also comparing the data to fraudulent document and bad actor watchlists. Those blacklists are updated instantly using unbiased AI decisioning. That means a fraudster only gets their first doomed attempt to create an account—once detected, they are blocked instantly and forever.

IDV You Can Count On

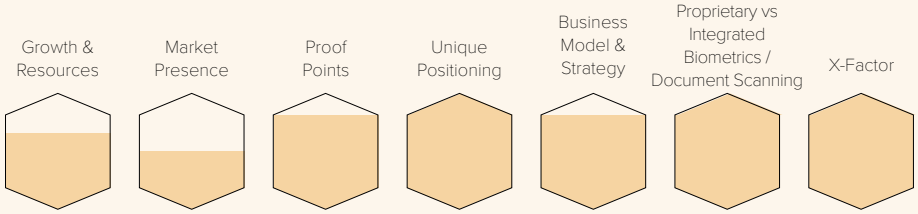
AuthenticID is widely deployed by banks and telecoms, for whom its technology is making a quantifiable difference. When deployed by a leading wireless provider, FraudShield was able to detect 46,291 fraudsters and add them to its blacklists. The client leveraged AuthenticID to halt 420,000 fraudulent transactions, saving an estimated $504 million in fraud losses. Meanwhile, when one of the 10 largest banks in North America was experiencing a high rate of app-based fraud caused by bad actors submitting legitimate stolen IDs that had been altered to have their own photo displayed, AuthenticID's technology enabled a remarkable reduction in fraud. Zero successful fraud attempts have been recorded by the bank since the implementation, and it saw its first-time pass rate for verifications jump from 61% to 98%. These tangible successes in crucial identity markets demonstrate how AuthenticID's token approach to identity proofing and verification is making our digitized world safer.

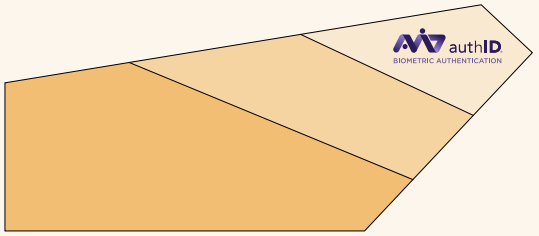
Contact AuthenticID: marketing@authenticid.com

authID

authid.ai

BEAM: **Identity Verification** / CLASSIFICATION: **Luminary**





With high-performance biometrics, a proven track record, and a clear mission to "eliminate fraud and deliver 100% zero trust identity protection," 2024 Prism Luminary authID is safeguarding the era of digitization. Anchoring user identity with liveness-supported face biometrics during the onboarding process, authID puts integrity at the foundation of every transaction between its customers and their end users. Guided by a leadership team of identity experts informed by intelligent customer feedback, few IDV players can compare to authID in terms of its consistent adaptation in the face of a rapidly evolving industry. Thanks to its unique positioning, multi-layered deepfake detection, and laser focus on user experience, authID has quickly become a guiding star in the Identity Proofing and Verification Prism Beam.

Organic Compliance for Today's Strict Regulations

Compliance is one of the major challenges facing industries in the current era of digitization. As new regulations emerge, and rules shift regarding the collection, storage, and transit of biometric data, identity verification becomes a high-risk proposition that can cost millions in fines and lawsuits if done improperly. This presents relying parties with a conundrum: store biometrics and take on compliance risk or delete biometrics after enrollment and face the threat of account takeover fraud. authID eliminates this trade-off. Using an innovative public key generation solution, the company keeps biometrics at the core of transactions without having to store the data, protecting privacy, enabling compliance, and keeping fraud at bay. From a customer perspective, they don't have to lift a finger—compliance is just a natural part of using authID's cutting edge face biometrics technology.

Fast, Frictionless, Friendly

In addition to its innovative approach to compliance, authID's biometric IDV is fine-tuned for performance and customer experience. With an intuitive, self-guided interface for image capture and a one-in-a-billion false match rate, the company's solution is accurate, reliable, and user friendly. And it's fast—able to process images and render onboarding decisions at breakneck speeds of 700 milliseconds. From a user perspective, it's fast, easy, and reliable, allowing for frictionless transactions and peace of mind. Operationally, authID's technology is easy to implement, too. Available in no code and low code configurations, and supported with accessible developer resources, authID's Luminary-level biometric products are ready to improve security, convenience, and built-in compliance in any market where identity is in play.

Verifying Professionals and Ditching Passwords

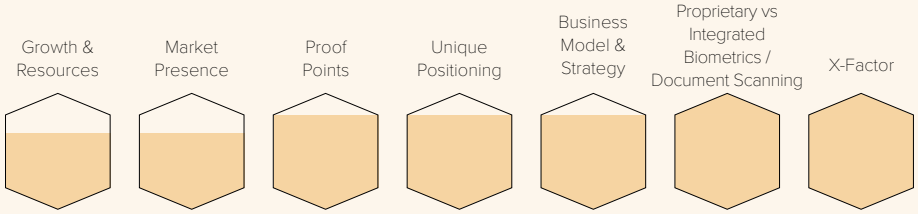
While the fine details of every industry make digital transformation a unique challenge, the core principles of identity remain the same across the board. authID exemplifies this paradigm through a wide breadth of application areas, where it's seen impressive success. When the American Board of Radiologists launched an online exam platform, it turned to authID to verify its members' identities through remote channels. When ABM, a Fortune 500 company specializing in facility solutions, needed to nix usernames and passwords for the more than 100,000 frontline workers it manages, it turned to authID to successfully deploy intuitive biometric authentication across shared devices. And when Beem, a financial services company focused on inclusion for the underbanked, required a solution to defend against fraud without interfering with its millions of monthly transactions, it found success with authID. When digitization gets complicated, authID proves that truly secure identity can feel simple.

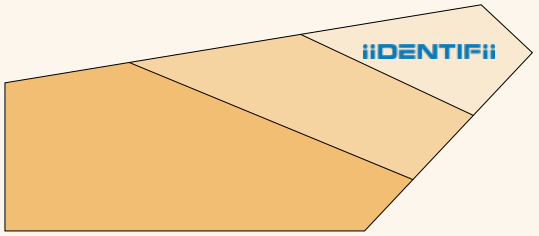
Contact authID: +1 (516) 778-5639

iiDENTIFii

iidentifii.com

BEAM: **Identity Verification** / CLASSIFICATION: **Luminary**





Founded in 2018 and headquartered in South Africa, iiDENTIFii is the perfect example of what is required at the foundational level of enterprise-grade biometric digital identity in order to realize a secure, convenient, and accessible future. Its identity proofing and verification technology is grounded in a government system of record, enabling the full spectrum of transactions outlined in the Prism Identity Hierarchy. From cutting down fraud, to speeding up customer onboarding, to enabling regulatory compliance for multiple tier 1 banks, iiDENTIFii is addressing digital transformation pain points using intuitive software based on facial recognition, finger recognition, document reading and forensic technology.

Identity's Fourth Dimension

In addition to being quick to deploy and anchored by a government system of record, iiDENTIFii's biometrics are bolstered by its 3D and 4D LivenessTM technology. As the name implies, 4D Liveness™ incorporates a temporal element into its face biometric verification process, helping bolster it against modern fraud threats like synthetic identities and deepfakes. Available in no-code or low-code configurations, iiDENTIFii's IDV technology is ideal for the region it serves, where boutique smartphones with specialized hardware are rare, but the need for strong and safe identity is high.

Setting the Identity Standard

iiDENTIFii's relationship with Standard Bank is crucial to understanding what makes this Prism Luminary stand out. Standard Bank is the largest bank on the African continent. With 161 years of history, it operates in 20 sub-Saharan countries serving 19 million clients through 12,000 points of presence, including branches. When Standard Bank faced rising levels of fraud, it turned to iiDENTIFii, which deployed its solution in a matter of months. This enabled the financial institution to decrease customer onboarding and verification times to seconds while complying with FICA, KYC, RICA, AML, GDPR and POPIA regulations. The deployment was so successful that Standard Bank went on to offer iiDENTIFii's technology through its OneHub platform, further spreading the company's identity-safe paradigm.

A Solution for South Africa's Digital Transformation

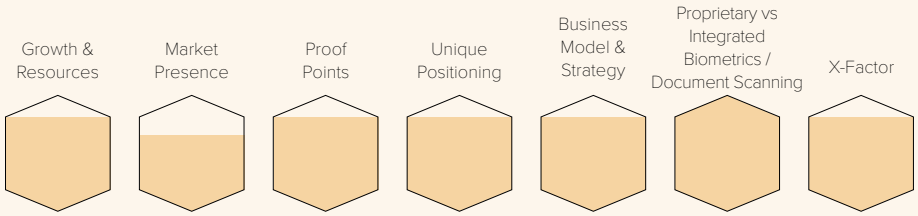
The South African government has embraced digital transformation and is facing the full range of critical challenges that come along with it. iiDENTIFii helps address these challenges by ensuring citizens and public employees benefit from secure access, fraud protection, and the identity assurance of an IDV solution with biometrics at the core. These benefits are crucial for security and convenience, but most importantly: iiDENTIFii ensures they are continuous. Thanks to built-in sophisticated redundancies that enable offline identity verification when networks go down or connectivity is out of reach, citizens can participate in government processes with the convenience they expect from a digitized future whether they're in a major city, a rural area, or a digital desert. Between this thoughtful implementation that prioritizes accessibility, trust, security, and its commitment to innovation and a strong foundation of identity, iiDENTIFii is a biometric digital identity role model not just on its home continent, but for the industry at large.

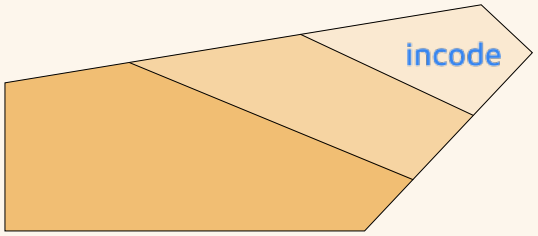
Contact iiDENTIFii: tel:+27 21 286 9104 | email: info@iidentifii.com

Incode

incode.com

BEAM: **Identity Verification** / CLASSIFICATION: **Luminary**





Verifying over 100 million users globally on an annual basis, incode shines bright as a 2024 Flagship Prism Luminary. Protecting customers against fraud across a range of markets—from financial services to hospitality to social media—the company is on a mission to power a world of trust. It manages this with its AI-driven technology, all developed in-house, which orchestrates the full identity lifecycle from onboarding forward. What's more: incode stands out in the Identity Proofing and Verification beam thanks to its integration of government systems of record, which facilitate the foundational levels of identity assurance required for all of today's modern identity transaction demands, ranging from the high risk to the pseudonymous.

Orchestrated Innovation

incode's platform approach to identity verification makes it shine. The company was able to deftly navigate the turbulent market during the COVID pandemic, largely thanks to its culture of innovation. It fully owns an entire suite of identity verification technologies and KYB products, centered around its own AI-supported face biometrics. Fully customizable and vendor agnostic, incode's technology offers confident identity defense on the edge. Ensuring real human identity at the front door during onboarding, it continues to defend against fraud with step-up verification during authenticated sessions. In an era defined by synthetic identity fraud and account takeover attacks, this is a powerful approach. Constantly adapting to the accelerating fraud landscape, incode is coalescing the fragmented customer identity journey into an orchestrated experience.

Intelligent Identity

The premium experience offered by incode extends beyond end users. This Prism Luminary's approach to artificial intelligence offers a window into the future of identity management, which is just as intuitive on the backend as it is for customers. With its AI Suite, incode has integrated generative AI into its orchestration workflows. This allows administrators to directly query the platform and receive real time identity and risk level insights. In an industry where admin-facing dashboards and controls are often neglected, incode's AI Suite isn't just a useful tool for enhancing integrations, it's another example of how the company is endeavoring to power a world of trust through thoughtful research, development, and innovation.

Financial Finesse

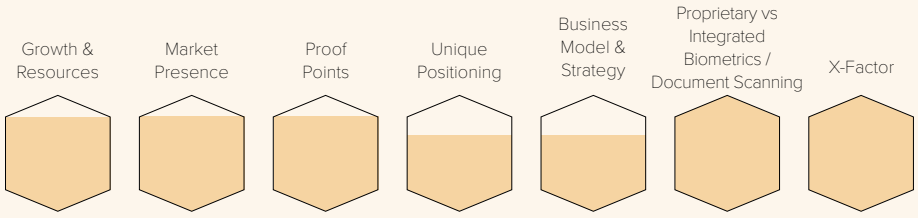
Simply look to the financial services sector to see how incode is putting these technologies to work. The largest neobank in the United States chose to implement incode for its IDV needs, based on the Luminary's consistent ability to positively verify rightful user and reject impostors. The result was a 15% increase in successful verifications and a 38% reduction in fraud for the neobank, equating to millions in additional revenue and cost savings. Meanwhile in Latin America, Rappi—the largest on-demand delivery service in the region—implemented Incode Verify and its system of record integrations in Mexico and saw over 98% reduction in fraud. Examples like these show how incode's innovative solutions, grounded in true foundational identity, are having a measurable impact on fighting fraud in the real world.

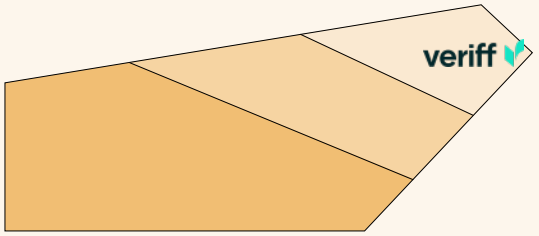
Contact Incode: +1 (650) 446-3444

Veriff

veriff.com

BEAM: **Identity Verification** / CLASSIFICATION: **Luminary**





Established in 2015, Estonian identity verification provider Veriff serves customers the world over, both directly and through an extensive and sophisticated network of leading identity platforms, aggregators, and resellers. Its rapidly scalable solutions address the identity challenges inherent to digital transformation by verifying trusted identities with intuitive biometrics and document scanning. The core trust established through its quick and accurate onboarding process is carried forward through the entire user lifecycle—authenticating every subsequent transaction and allowing for automated account recovery. Its mission to prevent fraud, enable compliance, and enhance user experience makes Veriff an identity leader in financial services, but its breadth of application can't be ignored. This Prism Luminary serves customers in established and emerging markets for biometric digital identity including transportation, gaming, social media, the gig economy, dating services, video games, and ride-sharing.

A Versatile IDV Unicorn

The identity verification space is saturated thanks to a COVID-driven rogue wave of activity in the early 2020s which saw vendors flood the market to serve a rapidly accelerated need for remote enrollment. Veriff stands out as a star in the Identity Proofing and Verification Prism Beam thanks to its robust and versatile technology, which is bolstered by liveness detection and supports 48 different languages. Just as remarkable is the company's growth and resources. In 2022, after receiving $100 million in series C funding from Tiger Global, Veriff ascended to unicorn status, earning a $1.5 billion valuation. This achievement put it in league with Estonia's other tech industry crown jewels such as Skype and Wise.

AI Powered Identity Verification

Powered by machine learning models, Veriff's fully automated identity verification technology enables compliance for essential KYC and AML regulations. Boasting coverage for over 12,000 documents from more than 230 countries and territories, the platform can verify users in six seconds. Authentication is even faster with Veriff—users simply snap a selfie and are approved as trusted users in one second. This is all supported by the aforementioned liveness detection, which ensures the person enrolled is who they claim to be and that every subsequent transaction is being performed by a rightful user, not a fraudster using deepfakes and spoofs. Given the prominence of synthetic identities and account takeover fraud, particularly within the markets Veriff serves, this approach blocks bad actors at the front door and keeps its users' accounts safe for the duration of the customer experience.

Enhancing Experiences in Regulated Arenas

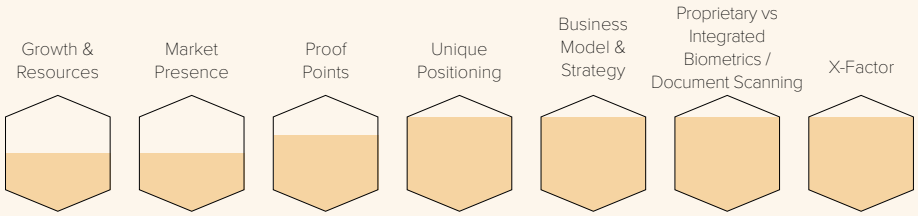
Veriff's platform serves companies from SMBs to large enterprises for a range of applications, shining particularly bright in mobility and marketplaces applications. Joyride, a company that manages thousands of electric lightweight vehicles in over 250 markets, works with Veriff to ensure all its customers are real people, that they are old enough to operate a vehicle, and that have the proper licenses. That same full-spectrum approach to solving identity challenges is also reflected in Veriff's work with Japan Tobacco International (JTI). By automating JTI Philippines's identity verification process with biometric technology, Veriff was able to improve its customer's conversion rates by 223% while also ensuring users under 18 can't access the company's highly regulated products and age restricted online events. This market versatility and tangible impact is a testament to Veriff's capabilities and offers a glimpse of the future it envisions—a world where "one reusable identity" rules them all, simplifying the experience of our digital lives.

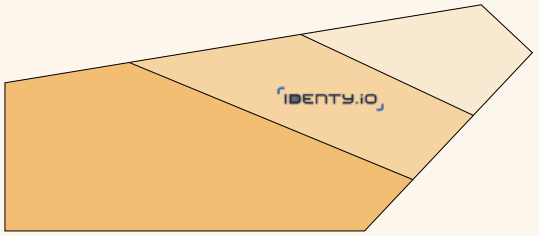
Contact Veriff: sales@veriff.com

Identy

identy.io

BEAM: **Identity Verification** / CLASSIFICATION: **Catalyst**





Specializing in mobile touchless biometrics, IDENTY is mission-driven to replace the flimsy user verification methods of the past with privacy-forward, guaranteed digital identity. Supported by liveness detection and protected with triple-level encryption, its solutions portfolio sports multimodal biometric face and fingerprint technology. Remarkably, both biometric modalities are software-based, available through multi-platform SDKs. That puts IDENTY in the rarified category of Identity Proofing and Verification vendors that can enable touchless 10-fingerprint biometrics via iOS and Android smartphones—even including older devices with low end cameras.

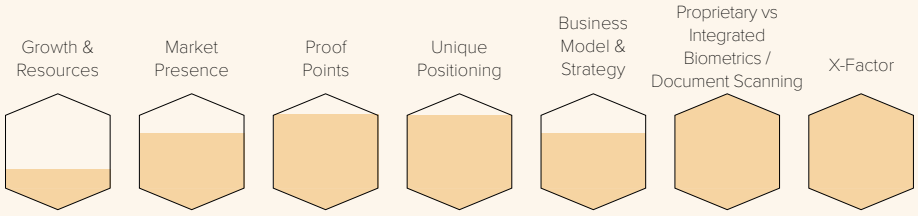
IDENTY serves diverse industries, including financial services, telecom, and travel, while specifically targeting government and enterprise organizations to deliver trusted identity that can be carried forward through the entire user lifecycle. And what's more: it's inclusive. As digital transformation takes hold around the globe and across all industries, that level of accessible innovation is crucial. It has long been a tenet of the Prism Project that biometric digital identity cannot be exclusively the purview of boutique smartphone users for reasons of ethics, sustainability, and security. IDENTY—thanks to its global presence and emphasis on self-sovereign concepts of identity that empower users, enable compliance, and protect businesses—is an example of the kind of R&D and technological application required for everyone to finally replace the knowledge-based authenticators and physical tokens that anchor us to approximate forms of identity assurance tethering us to the past.

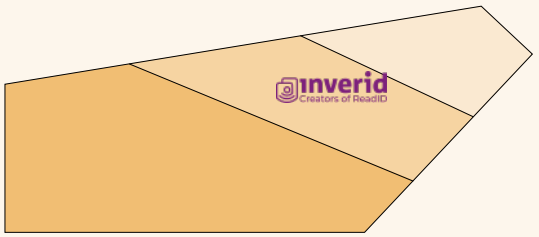
Contact Identy: contact@identy.io

Inverid

inverid.com

BEAM: **Identity Verification** / CLASSIFICATION: **Catalyst**





Safe and easy—that's the mantra of 2024 Prism Catalyst Inverid, which is on a mission of security and convenience. Serving use cases in government services, finance, travel, hospitality and more, Inverid's NFC-first solution, ReadID, enables the remote verification of electronic Machine Readable Documents (eMRTD) for identity verification. The most impressive part: it does this by using standard smartphone NFC reading capabilities. ReadID accesses the electronic data in eMRTDs to verify the document's authenticity and retrieve the document data including the embedded high-resolution photo of the eMRTD holder. That foundational ID data can be compared to the real human credential holder via 1:1 facial verification and liveness detection, providing the basis for the full-spectrum of transactions described by the Prism Identity Hierarchy.

Regulatory compliance is the most prominent use case for identity verification, and in financial services, Inverid enables eKYC and AML, as well as reverification. Most notably, ReadID's NFC capabilities allow for reliable first-time verification rates by virtue of not relying on optical OCR technology—a differentiator that helped it significantly improve conversion rates for ASB Bank. In the government sector, ReadID played an important part in the post-Brexit EU Settlement Scheme, easing the immigration process for EEA nationals living in the UK. And in a travel context, Inverid was able to demonstrate how self-service traveler data collection enabled by biometric remote verification can mitigate operational slowdown and ease bottlenecks for the incoming European Commission Entry Exit System (EES). By focusing on getting IDV right through novel innovation, Inverid is doing its part in building a user friendly and identity-safe tomorrow.

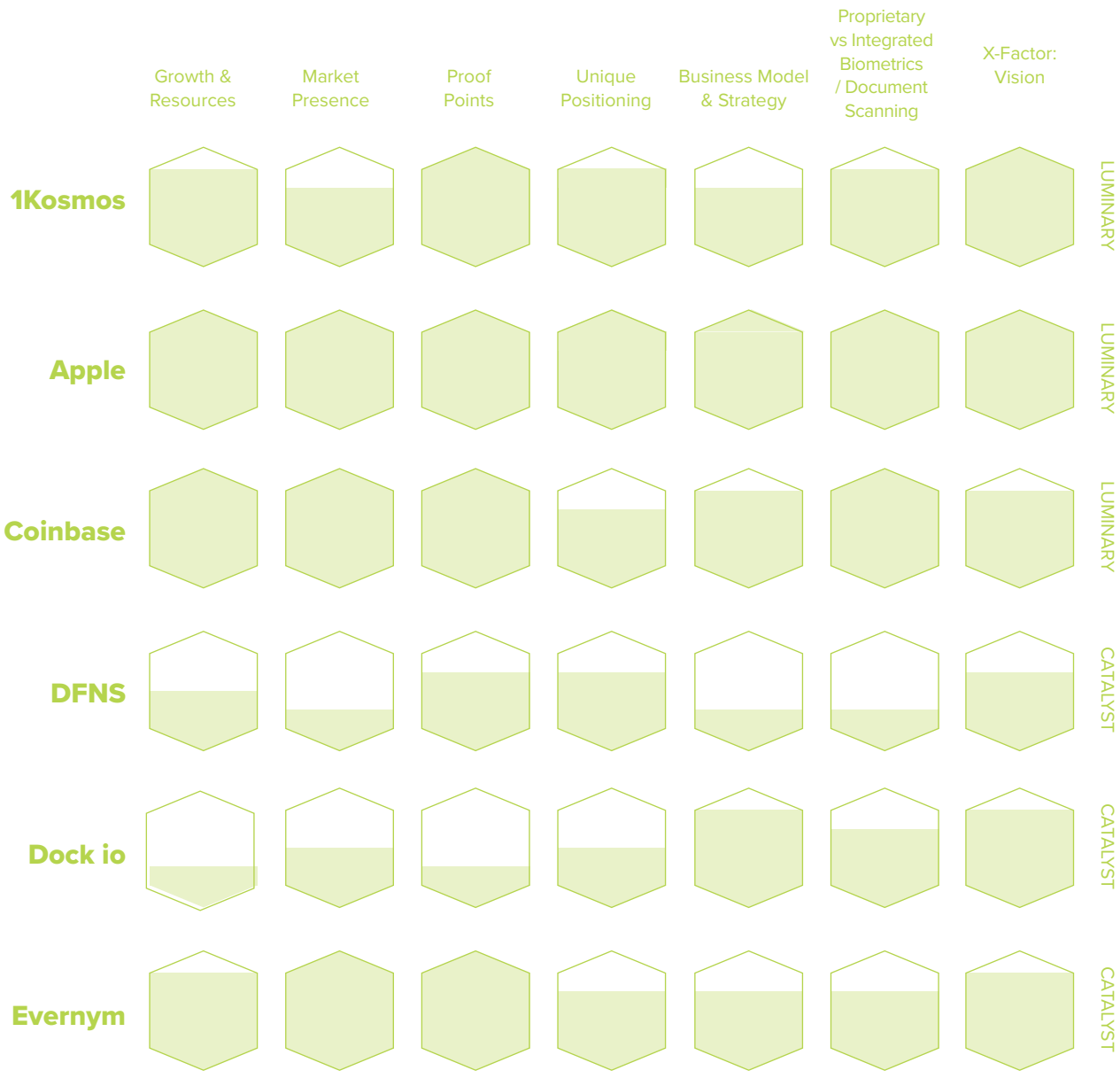
Contact Inverid: sales@inverid.com

Decentralized Identity

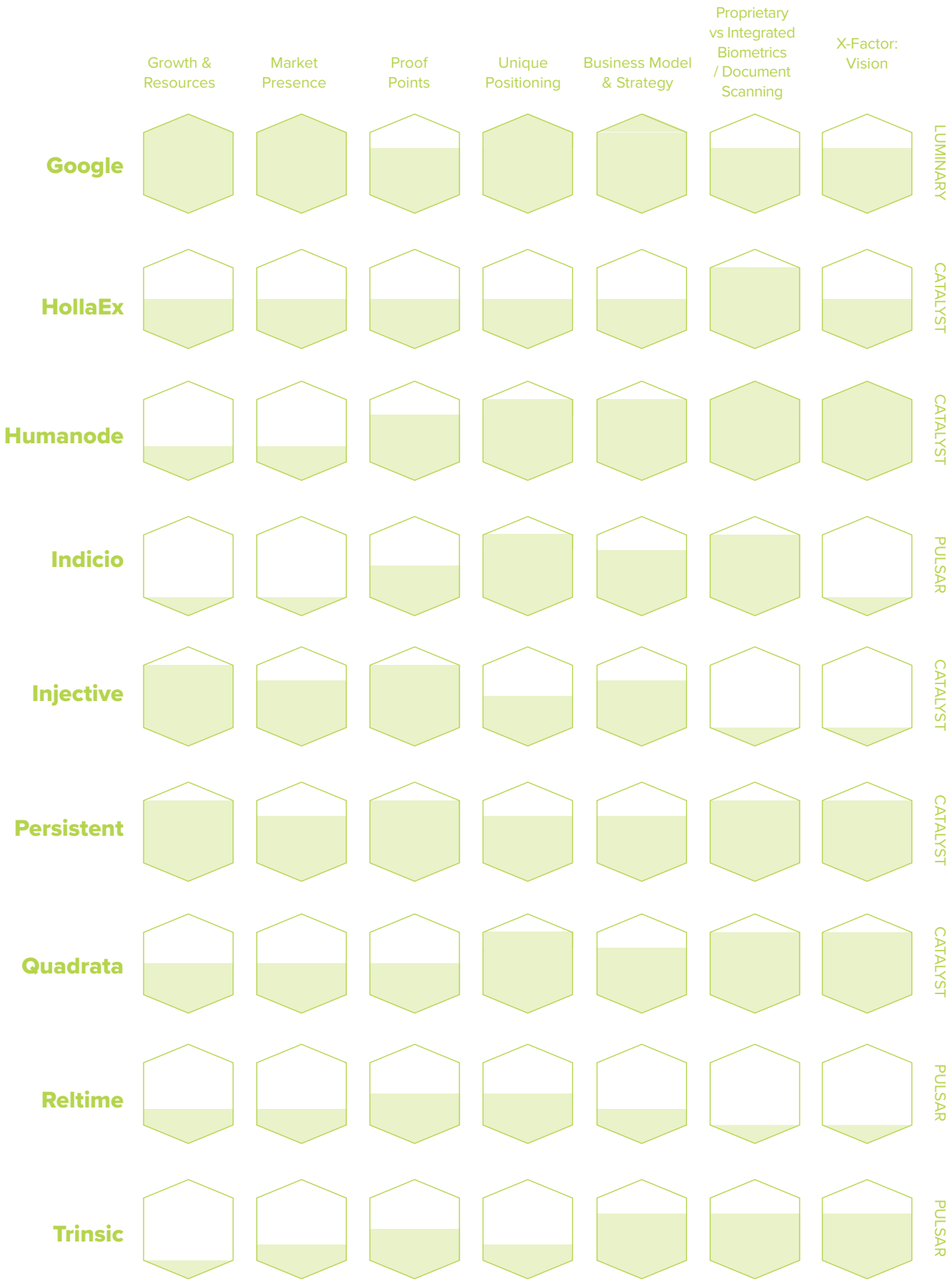
These vendors offer distributed identity technologies and solutions leveraging some combination of blockchain, VCs (Verifiable Credentials), DIDs (Decentralized Identifiers), and other decentralized approaches.

Prism XFactor: Biometric Digital Identity Vision

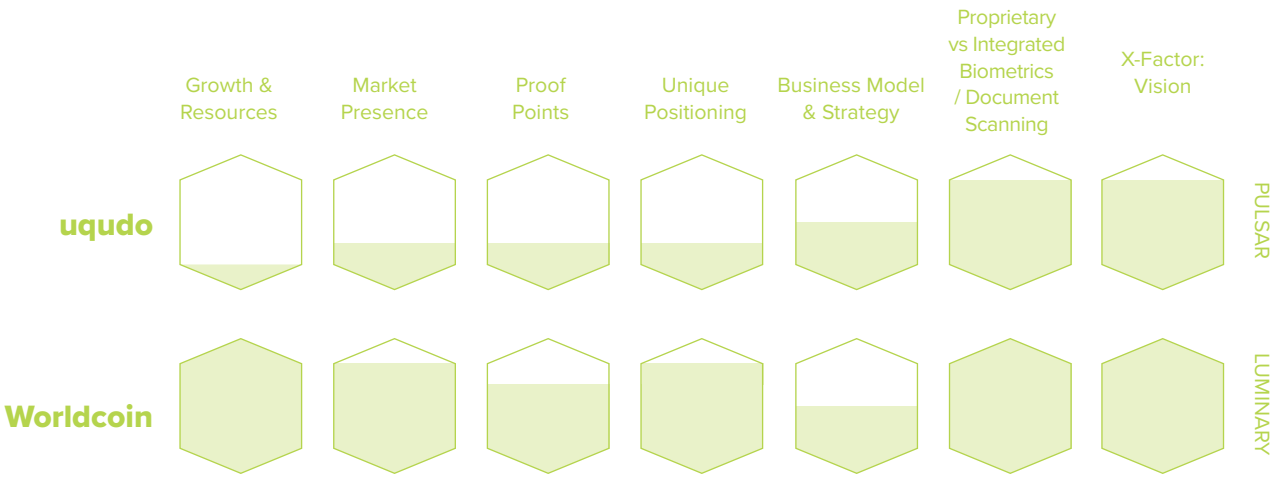
Evaluations



Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project

Infrastructure

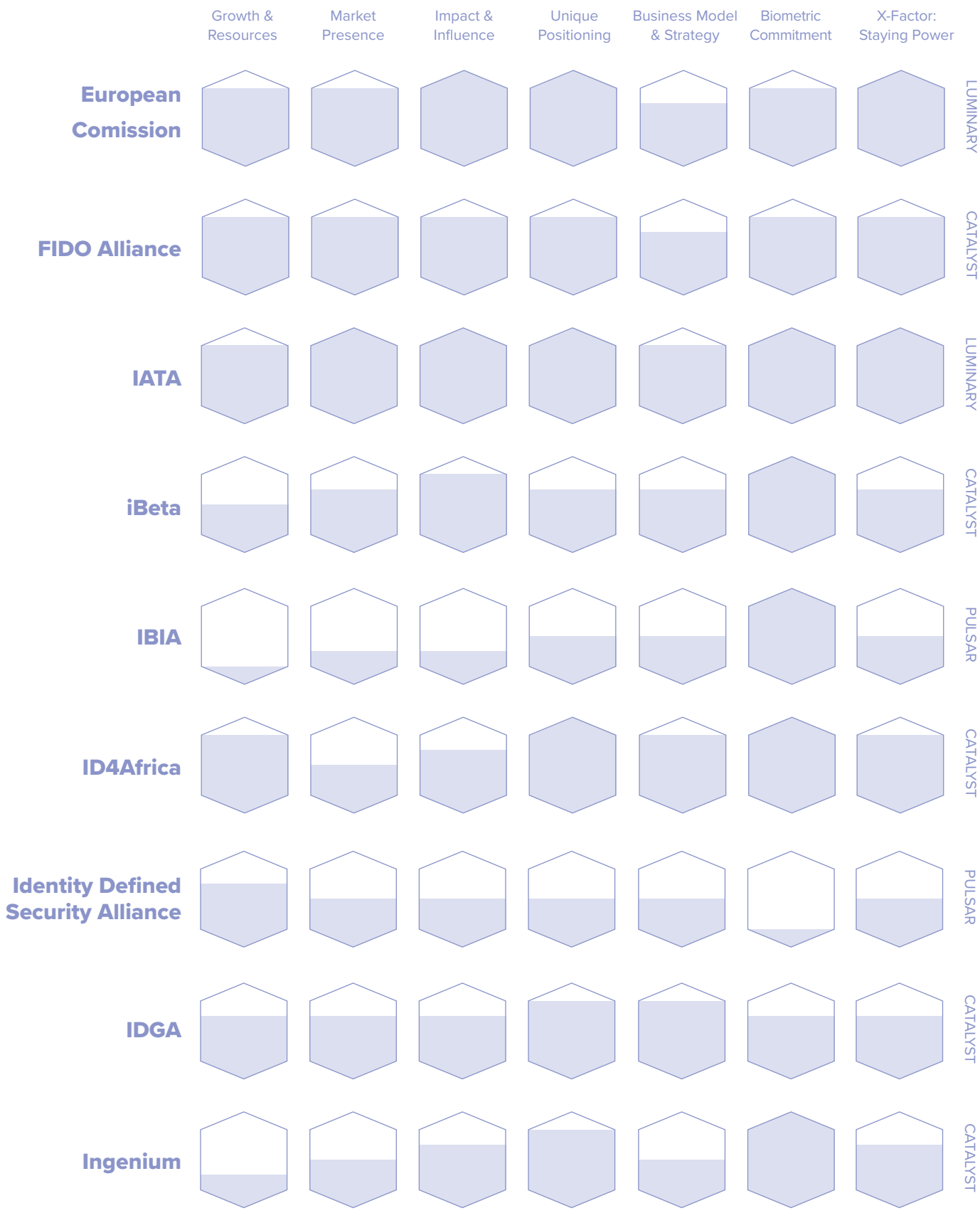
These vendors provide and/or deploy behavioral biometrics along with other signals intelligence in the background of financial sessions to identify and prevent fraud.

Prism XFactor: Biometric Digital Identity Vision

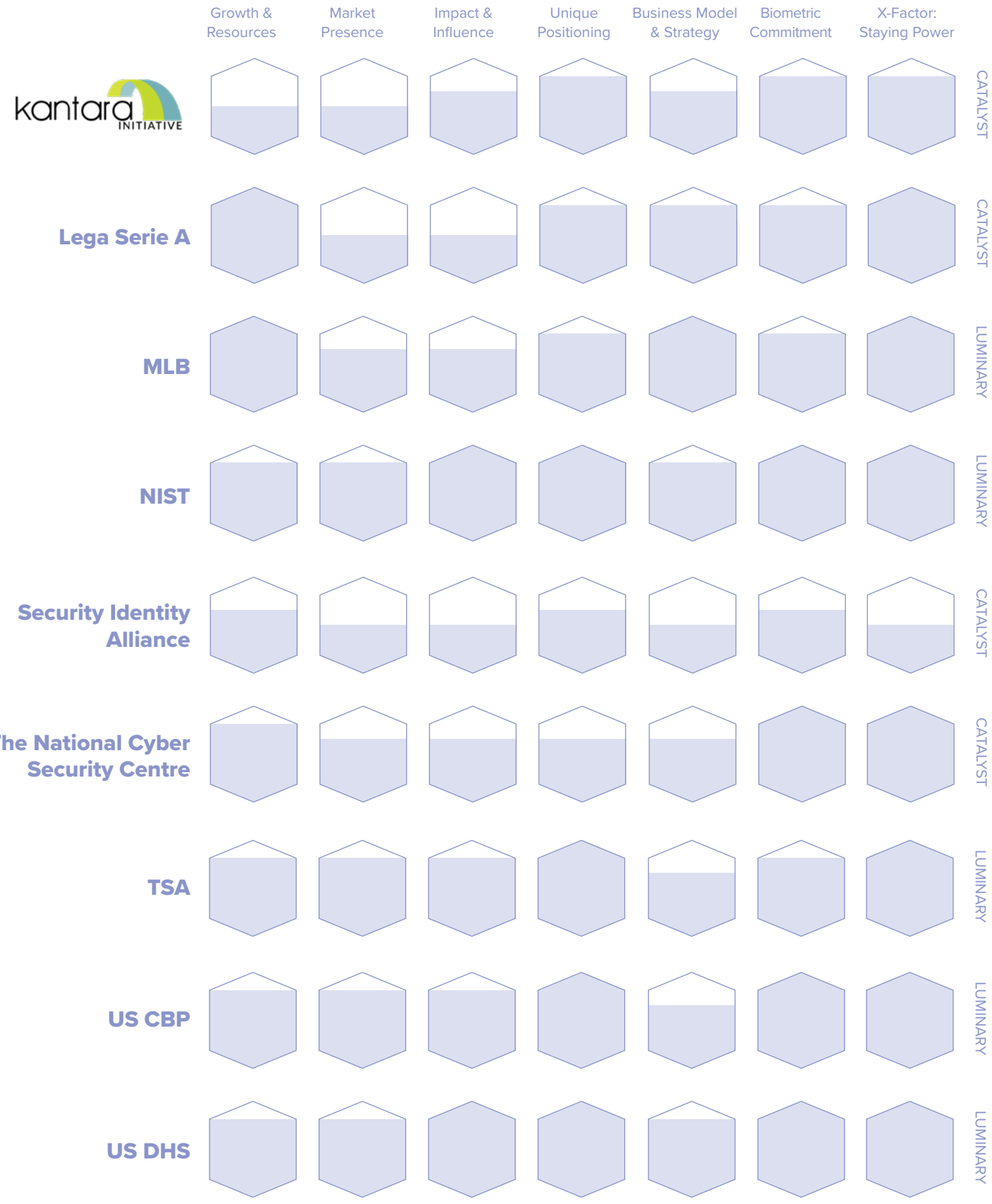
Evaluation Note:
The Infrastructure Prism Beam contains the unique criteria "Impact & Influence" and "Biometric Commitment."

Evaluations

Prism Ver. 1.0 © 2024 The Prism Project



Prism Ver. 1.0 © 2024 The Prism Project

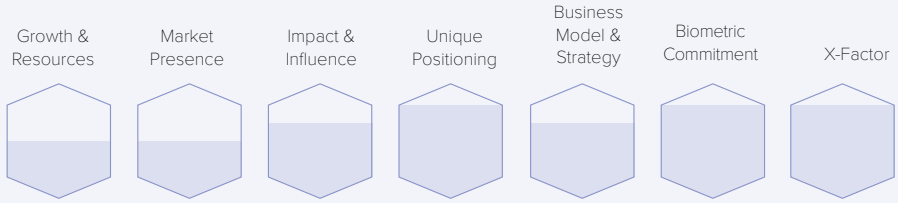


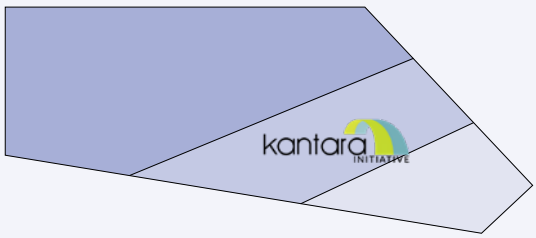
Prism Ver. 1.0 © 2024 The Prism Project

Kantara Initiative

kantarainitiative.org

BEAM: **Infrastructure** / CLASSIFICATION: **Catalyst**





Founded in 2009, the Kantara Initiative is a collaborative hub for identity technology thought leadership dedicated to improving the trustworthy use of identity and personal data. The high-stakes nature of identity in the era of digital transformation requires Infrastructure Catalysts like Kantara, which—in addition to its work groups, discussion groups, events, and reports—is the only organization in the world able to assess identity solutions and services against NIST's 800-63 guidance for identity privacy and technology. With dozens of organization members backed up by a host of notable individual contributor members, the Kantara Initiative is providing the framework that will support a future characterized by the responsible capture, sharing, storage, and verification of identity data.

Working Together

Kantara's work groups engage every major identity challenge identified by The Prism Project in the government services space. From 'Privacy Enhancing Mobile Credentials' and 'Diversity, Equity, Inclusion & Accessibility,' to 'Deepfake Threats to Identity Verification & Proofing,' Kantara Work Groups provide the identity industry's most prominent figures with the opportunity to collaborate on the groundwork for an identity-safe future that's fully inclusive, compliant, and consensual. Whether it's identifying the changes that need to happen in our rapidly digitizing society so that everyone can participate, or researching how identity proofing and verification systems—which are essential to securing digital government services—can distinguish between real users and AI generated deepfakes, Kantara's Work Groups are actively guiding the industry through engaged discussion between relying parties, government agencies, and identity leaders..

Identity Accountability

The Infrastructure beam of the 2024 Biometric Digital Identity Flagship Prism is responsible for maintaining the integrity of an overall identity ecosystem that is susceptible to a range of political and economic threats. Biometric digital identity technology, especially when deployed in government services, must be held to the highest levels of scrutiny, not only to protect the personal data of citizens but to ensure the equal access to essential services by all citizens. Anything less is a failure of public private partnerships. When sub-par technologies are deployed, or when vendors fail to maintain a commitment to privacy, security, and inclusion, they put citizens and nations at high risk. Organizations like the Kantara Initiative provide the essential guidance required to secure identity while enabling the benefits of digital civics.

Organization Members:

1KOSMOS, Airside an Entrust Company, incode, beruku knowledge, GakuNin, CLEAR, facetec, THALES Building a future we can all trust, IDmachines, Proof, IDPrivateid, WEAVE, INTERNET2, SLANDALA, Socure, ID.me, Patient Centric Solutions, UNITED STATES POSTAL SERVICE, YuTru, CALVERT CONSULTING, experian, IDEMIA, IDENTOS, HINDLE CONSULTING, GSA, Zygma

Contact Kantara Initiative: hello@kantarainitiative.org

The Prismatic Future of Identity

Widespread digitization has opened the door to a secure and convenient future powered by biometric digital identity. Through the adoption of technologies grounded in the foundational level of the Prism Identity Hierarchy, relying parties in all industries stand to significantly benefit from the biometric digital identity solutions explored in this report while also providing a solid anchor of trust for other markets.

The future of biometric digital identity demands:

- AI-powered anti-fraud solutions that can compete in the ongoing cybersecurity arms race.
- Easy and accessible onboarding that can bind human biometric identity to a system of record, rejecting synthetic identities and complying with shifting regulations.
- Strong authentication that carries the trust from that foundational identity forward through every transaction including account recovery.
- A convenient end user experience meeting the evolving demands of citizens that doesn't compromise security.

Enterprise stakeholders have a multitude of biometric digital identity options to choose from. Those highlighted in this report are ready to deploy and have an eye toward the orchestration and proficiency required to make the Prism Identity Hierarchy a reality. By choosing biometrics with AI-enhanced liveness detection and full lifecycle orchestration, government services stakeholders are laying the groundwork for an identity safe future everyone can enjoy.

Prism Ver. 1.0 © 2024 The Prism Project

The Prism Project

Showing Identity in a New Light

The Prism Project arose organically out of a collaborative survey-based research project launched by Acuity Market Intelligence and FindBiometrics in late 2022. The initial proof-of-concept Prism graphic was developed and debuted in the winter of 2023. It instantly became the most shared asset in our history, receiving over 50,000 impressions within weeks. By September 2023, we developed that proof-of-concept into a robust Prism Report, which served as the foundation for The Prism Project. The intent of the Project is to use the Prism as the lens through which we continue to analyze and evaluate the rapidly evolving biometric digital identity industry as we help influencers and decision makers understand, innovate, and implement digital identity technologies.

Reports and Collaborations

The Prism Project will publish, promote, and distribute new reports in 2025, focusing on key applications of biometric digital identity, such as:

- Deepfakes and synthetic identities
- Compliance and privacy
- Customer experience and fraud

Visit www.the-prism-project.com/prism-reports for more information.

Prism Project Brain Trust

The Prism Project is the brainchild of Maxine Most, Principal, Acuity Market Intelligence and Peter Counter, Author, Technology Writer, and former Editor and Chief, FindBiometrics. This innovative new framework for understanding and evaluating the rapidly evolving biometric digital identity marketplace is the only market model that is truly biometric-centric based on the foundational conviction that in the age of digital transformation the only true, reliable link between humans and their digital data is biometrics.

Prism Ver. 1.0 © 2024 The Prism Project

Ongoing Collaboration and Sponsorship Opportunities.

The Prism Project is conducting on-going research and continuing to explore how biometric digital identity is being used today, where the roadblocks to adoption lay, what obstacles must be overcome to successfully deploy these technology solutions, and where they are being used and by whom. We welcome collaborators and are open to discussing how your organization might benefit from and/or leverage the opportunities The Prism Project presents. To reach out, visit www.the-prism-project.com or email us at info@the-prism-project.com.

Prism Ver. 1.0 © 2024 The Prism Project

About the Author

Maxine Most

Internationally recognized biometrics and digital identity thought leader celebrated for provocative market insights, accurate market predictions and forecasts, and unbiased, pragmatic market intelligence.

Strategic innovator, market visionary, and forecasting guru Maxine Most is the founding Principal of Acuity Market Intelligence (www.acuity-mi.com), a strategic research and analysis consultancy recognized as the definitive authority on global biometrics market development. Throughout her decades long career, Maxine has evangelized emerging technology on five continents. Since 2001, she has applied her unique ability to bring clarity to the unpredictable and volatile world of emerging technology to the rapidly evolving biometric and digital identity marketplace.

As an executive strategist, Maxine has earned a stellar reputation for innovative thought leadership by consistently providing unique, unvarnished, and reliable market insight while accurately anticipating biometric and digital identity market trends. Under her leadership, Acuity has provided strategic guidance to Global 1000s, established technology market leaders, start-ups, and a range of organizations in between. Most leverages her deep understanding of technology evolution, emerging market development, and the process through which industry leaders are created to provide candid strategic analysis, highly targeted implementation plans, and quantifiable, measurable results.

Ms. Most is the author of numerous biometric and digital identity research reports including Face Verification & Liveness for Remote Digital Onboarding," "The Global Automated Border Control Industry Report: Airport eGates & Kiosks," "The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy," "The Global National eID Industry Report," "The Global ePassport and eVisa Industry Report," and "The Future of Biometrics," as well as a contributor to several books including "Digital Identity Management" edited by digital identity thought leader David G. Birch.

Ms. Most regularly offers insight and analysis in on and off-line publications, is quoted often in industry, business, and consumer press, is an active contributor to the Kantara Initiative, and presents

Prism Ver. 1.0 © 2024 The Prism Project

regularly at industry events on the evolution and development of biometrics and digital identity markets. She is a graduate of the University of California, San Diego with a multi-disciplinary degree in Mathematics and Computer Science and minors in Visual Arts and Economics.

Prism Ver. 1.0 © 2024 The Prism Project

Let The Prism Project be Your Guiding Light!

The Prism Project (www.the-prism-project.com)
The Prism Project is the brainchild of Maxine Most, Principal, Acuity Market Intelligence and Peter Counter, Author, Technology Writer, and former Editor and Chief, FindBiometrics. This innovative new framework for understanding and evaluating the rapidly evolving biometric digital identity marketplace is **the only market model that is truly biometric-centric** based on the foundational conviction that in the age of digital transformation the only true, reliable link between humans and their digital data is biometrics.

Maxine Most
Principal, Acuity Market Intelligence
cmaxmost@acuity-mi.com
Founder, The Prism Project
cmaxmost@the-prism-project

About Acuity Market Intelligence:

With decade of practical expertise in the unpredictable and volatile world of emerging technology, Acuity Market Intelligence consistently delivers consistently original, thought-provoking, and reliable insight and analysis. Proud, self-proclaimed technology business development and marketing geeks, Acuity is globally renowned for its uniquely customized business and marketing strategies and for creating and deploying innovative programs that integrate digital and traditional channels and platforms.

Visit acuitymi.com and let us help your organization thrive.

Prism Ver. 1.0 © 2024 The Prism Project