FindBiometrics and **Acuity Market Intelligence** Present:

THE BIOMETRIC DIGITAL IDENTITY PRISM REPORT

NOVEMBER 2023

A new paradigm for the emerging digital identity ecosystem.

FindBiometrics.com
acuitymi.com

FINDBIOMETRICS
GLOBAL IDENTITY MANAGEMENT

ACUITY
MARKET INTELLIGENCE

Table of Contents

Introduction

Biometric digital identity is no longer a novelty. As the mounting fraud crisis around the globe accelerates, users the world over are seeking to take control of their privacy, and public and private organizations are looking for security. Biometric digital identity has emerged as the only true solution to the problem of moving people across digital and physical spaces safely, securely, and intuitively.

Advances in biometric digital identity have evolved in parallel with Web3, artificial intelligence, mobile infrastructure, and data regulations. In the winter of 2023, FindBiometrics and Acuity Market Intelligence reframed the landscape. This innovative model reveals how technology vendors play integral role in the converged physical digital identity ecosystem. We are proud to introduce the Biometric Digital Identity Prism.

This report is the first entry in an ongoing research program from FindBiometrics and Acuity Market Intelligence aimed at providing education and strategic guidance for influencers and decision makers seeking to understand, innovate, and implement digital identity technologies, with a specific focus on the financial services, healthcare, government, and travel & hospitality sectors.

In this report you will find:

- Evolutionary trends driving the biometric digital identity market.
- Strategic guidance for vendors seeking to capitalize on opportunities in the biometric identity space.
- Key differentiators to help plan a digital identity roadmap for your organization.
- The advanced Biometric Digital Identity Prism landscape reference model.
- Assessments and profiles for vendors included on the Biometric Digital Identity Prism.

As industry advocates and evangelists of human identity, the authors of this report hope to level-up constructive and collaborative discussions among identity industry players and the relying parties with stakes in the growth of this industry. As that

conversation continues, industry development will accelerate, and these stakeholders will benefit manyfold. As the landscape evolves, we intend to update this report.

The Biometric Digital Identity Prism Report is made possible through the participation of industry leaders. If you would like to be included in an upcoming version of the Biometric Digital Identity Prism, please contact editor@findbiometrics.com and get involved with our research efforts.

Sincerely,

Report Authors

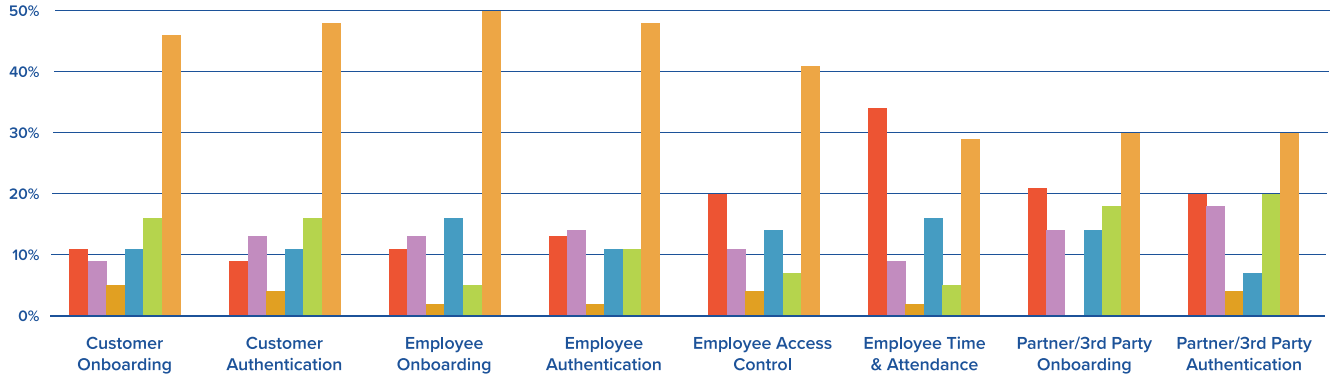
Evolutionary Trend Forecast

The Biometric Digital Identity Prism evolved from research on the relationship between digitization trends and their intersection with biometric digital identity.

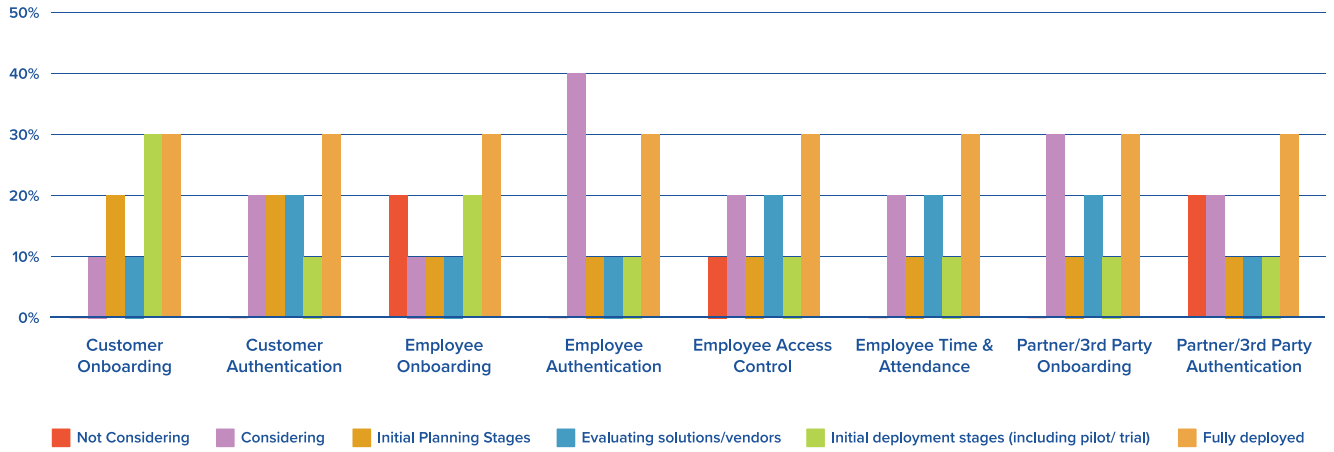
Digital Transformation and Core Identity Markets

MIT Press says organizations that prioritize digital transformation synchronize people, processes, data and technology "to identify and deliver innovative customer solutions — and redefine strategy." In our initial surveys we asked respondents to place identity-related processes on a scale between “Not Considering” to “Fully Deployed.”

VENDORS: Where would you place the following processes on your customers' digitization roadmaps?



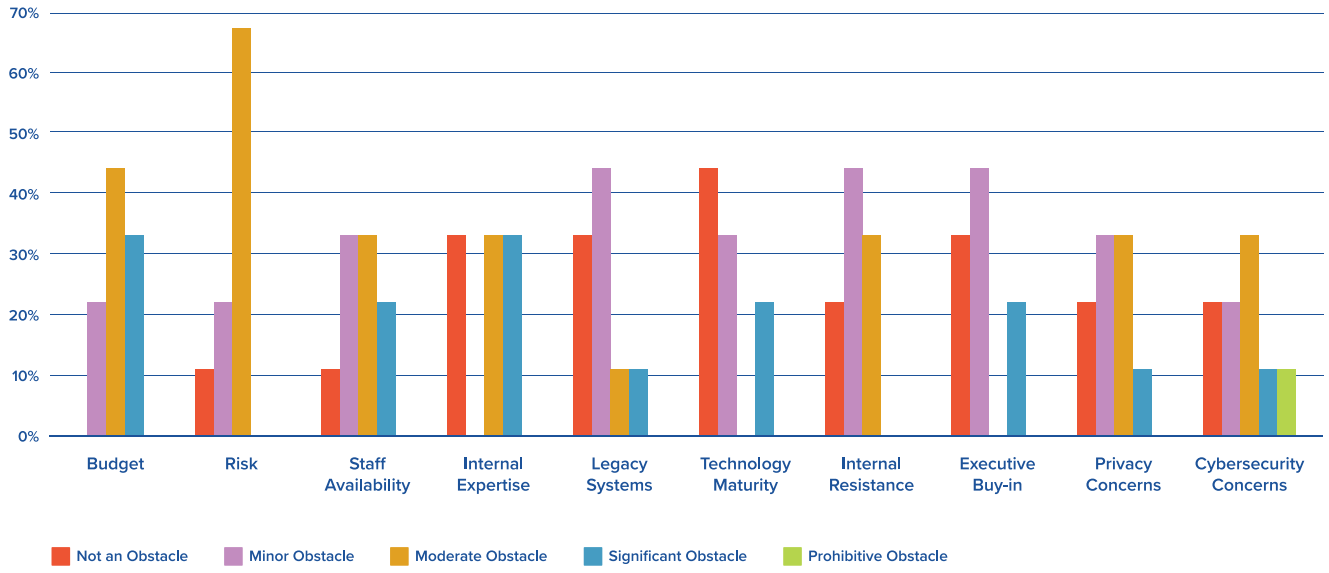
END USERS: Where would you place the following processes on your digitization roadmap?



The overall picture was clear: onboarding and authentication processes were the most advanced, with a preference for customer-facing applications, followed by employee applications, and even some appetite for partner and 3rd party applications.

Less of a priority is employee access and time & attendance. This is further reflected in how respondents characterized adoption obstacles traditionally associated with these two identity applications. Legacy systems no longer appear to be a significant obstacle for end users.

END USERS: How severe are the following obstacles to your digital transformation roadmap?



Converged Access Prioritizes Digital

The apparent de-prioritization of identity access and time & attendance systems comes after years of the identity industry focusing on the convergence between logical and physical access systems. The central idea is simple: the human being accessing a physical space is the same human being accessing digital spaces, and therefore should be able to use a single reusable identity for both applications. In effect this is the promise of biometric digital ID: one strong identity for every transaction.

As digital transformation has expanded the perimeter of all kinds of organizations—from banks, to DMVs, to healthcare facilities, to airports—and remote work has redefined the modern concept of a shared workplace, we are seeing the tasks normally handled by specialized hardware (which depends on a single physical touchpoint) offloaded onto the more versatile digital channel,

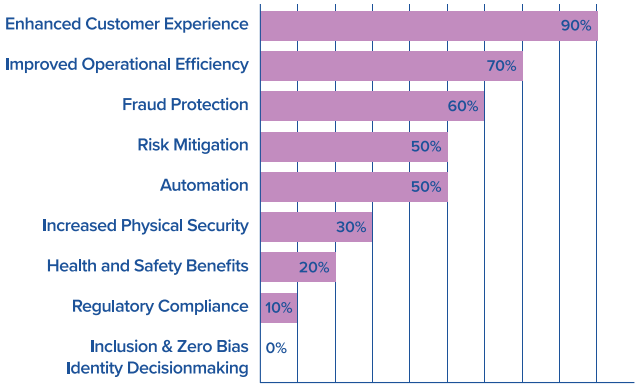
supported by mobile-based digital ID solutions.

Physical time clocks and access control systems are diminishing into specific niche markets that demand physical presence for a set schedule or the highest levels of physical security. When everything a user does within a work system is bound to a biometric digital identity they carry with them, time & attendance and access management don't go away, but fold into the overall process of verification and continuous authentication.

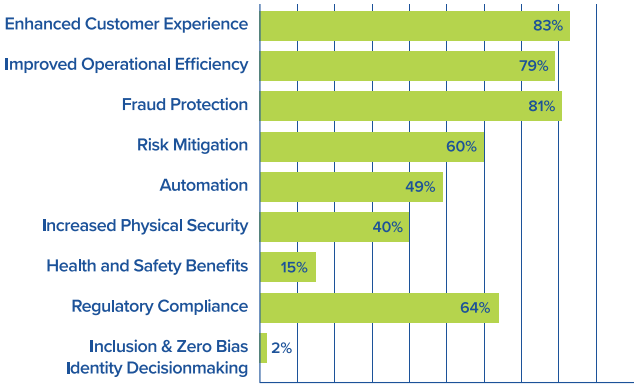
Identity's Role in Digitization

This unification of processes under biometric digital identity management—wherein a single biometric digital ID can provide access, transaction approval, and proof of presence—is in line with vendor and end user expectations of what biometric digital identity technologies ought to be used for.

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



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



Our survey showed that enhancing customer service, reducing fraud, and creating operational efficiency were the three most pressing motivators for adoption. With those in mind, let's take a birds-eye-view of the markets most ready for biometric digital ID adoption.

Leading Identity Markets

Biometric digital ID enables the highest level of convenient user experience, streamlines operations, and secures the most vulnerable vectors for fraud. As such, the most crucial markets for biometric digital ID are high risk environments trading in sensitive identity data that traditionally implement high-friction security measures at the cost of user experience.

The four markets identified in our research as the focus area for the Biometric Digital Identity Prism are financial services, healthcare, government, and travel & hospitality.

Financial Services

Over the past ten years, the financial services sector has been at the forefront of biometric adoption. The highly competitive banking and payments players prioritized convenience and user experience, while Know Your Customer and Anti-Money Laundering regulations incentivized the widespread adoption of identity verification technologies for customer onboarding.

As of this writing, two of the most notable uses of biometric digital identity in financial services are in international money transfer and the account recovery function for cryptocurrency wallets. These use cases require the strongest levels of identity assurance only enabled by leading matching and liveness technology supporting a trust chain anchored with biometric digital ID.

Relying Parties:

- Banks
- Credit Unions
- Insurance Providers
- Payments Networks
- Retailers (Including eCommerce)

Key Use Cases:

- Payments
- Account Opening
- Account Access
- Cash Withdrawal/Deposit
- Pension & Benefits Management
- Money Transfer
- Credit Check
- Insurance Claims
- Membership and Loyalty Program

Healthcare

The healthcare sector has long been touted as the next major market for biometric digital ID. The demand is massive thanks to the high stakes at play when it comes to patient identity data. Patient healthcare data is the most valuable in dark web marketplaces, and compromised patient ID is contributing factors to the ongoing opioid crisis. Furthermore, accurate patient ID ensures proper treatment, binding a person's medical history to their strong identity.

Regulatory factors are further stoking demand. In the United States, HIPAA requires timely transfer and secure handling of

Relying Parties:

- Hospitals
- Pharmacies
- Clinics
- Dentists
- Optometrists
- Mental Health Professionals
- Physiotherapists
- Insurance Providers

Key Use Cases:

- ePrescriptions
- Electronic Health Records

patient medical data, with severe fines for relying parties that fail to comply. Cost and implementation obstacles are most cited by industry professionals as to why adoption has been slow in this sector. As biometric digital identity matures further, these obstacles will diminish.

- Patient ID
- Visitor Management
- Insurance Claims
- Telehealth
- Consumer Health Tech

Government

Because the government sector plays a foundational role in establishing and validating citizen identities, it is a participant in the biometric digital identity landscape in addition to being a major market for vendors. Recent developments in remote digital onboarding, which leverage biometric identity technologies, have launched the government sector into the forefront of biometric digital identity innovation. Taking advantage of mobile biometrics, liveness detection, document validation, and trusted government records, digitized citizen identity has the potential to serve as the core identity form factor for users as they transact across all physical and digital spaces.

The government sector is defined largely by public perception and (somewhat obviously) politics. This is an area in which educating decision makers about the promise and reality of biometric digital identity is key to widescale adoption and use. Interoperability will also be key, as government-issued digital IDs will need to be recognized and useable across jurisdictions.

Relying Parties:

- Federal, State, and Municipal Governments
- Key Use Cases:
- Civil ID
- Elections
- Passports and Visas
- Border Control
- Immigration
- Military
- Law Enforcement
- Internal Administration

Travel & Hospitality

The shift from specialized hardware-based identity solutions to the biometric digital identity of the future is most apparent in the travel sector, where a decade-long paradigm shift is underway. The airline industry is aggressively pursuing “seamless” or “frictionless” passenger experiences, all of which depend on biometrics-enabled self-check-in, expedited security, border control, and automated boarding. These applications are also being seen in the cruise line industry and, more generally, in public transit.

As an extension of the seamless travel paradigm, the hospitality industry is also looking to biometric digital ID for many of the same experience enhancing reasons. Entertainment venues offer high throughput environments similar to airports, but where a premium is placed on convenience. Hotels and resorts, meanwhile are finding opportunities in remote check-in, mobile keys, and enhanced loyalty programs.

Relying Parties:

- Airlines
- Airports
- Cruise Lines
- Sea Ports
- Train Lines
- Bus Lines
- Hotels/Resorts
- Entertainment Venues
- Private Clubs

Key Use Cases:

- Booking
- Border Control
- Access Control
- Retail Food and Drink Purchases (including age check)
- Membership Management

Prism Identity Paradigm

The Biometric Digital Identity Prism is a living research project that is constantly adapting to developments in the ever-shifting market landscape. As vendors merge, acquire or develop new capabilities, grow, innovate, and deploy their technology, they move through the Prism. Companies may travel between beams and enter new classifications. New evaluation criteria will emerge, and new beams will be born.

But the Prism does have a foundation. Core concepts inform a philosophy of identity underlying our framework, motivating all of the dynamic elements at play.

Forget the Password; Bring Carbon-Based Life Forms into the Digital World

Passwords—be they **security keys, one-time passcodes, or authenticator apps**—are secret strings of data that can be used by anyone who knows them, guesses them, cracks them, or buys them. They can be forgotten. They can be reset. They can be phished. The integrity of a password-based system depends entirely on its secretive nature. They simply prove a user has an authenticated device. And while sometimes it might feel like our phones are extensions of our bodies, a device is not your identity.

By contrast, biometrics represent **the actual carbon-based lifeform at the end of a transaction**. Your fingerprint, iris, voice, and face are all unique parts of you that are used for identification online and offline, and are public by virtue of their plainly visible nature. When you phone a parent, you know them by the sound of their voice, not by the secret code you ask them for at the beginning of every call. Likewise, you know your coworkers by their faces, not a secret handshake.

Biometrics are not analogous to passwords. They aspire to something more organic: bringing the unique, irreplicable aspects of your physical identity into the digitized world so that only you can access your accounts, credentials, finances, healthcare, and government services, as if the institution you interact with knows you like family. Yes, password-replacement has long been the flagship mainstream use case for biometrics, but a shared application is not grounds to equate two fundamentally different ideas: knowable secret data and unique public physical traits. Biometrics are only similar to passwords in their shared

goal of enabling or restricting access to digital or physical assets. That's where the similarity ends.

The evolution of digital identity will continue to be stunted so long as this fundamental mischaracterization of the relationship between biometrics and passwords persists. **Biometrics are not the next evolutionary step up from knowledge-based authentication—they represent an entirely new foundation for identity in the digital age**. Passwords and their knowledge-based offspring are a class of 20th century technologies irrelevant to our 21st century digital ecosystem. As this global interconnected web of relationships and services continually expands and matures, we need to recognize them as the historical artefact they are and embrace a biometric-centric view of identity. Only then can we bridge the identity gap between carbon-based lifeform and the digital world.

As long as this false dichotomy of passwords and biometrics persists, we are fated to build our biometric digital identity systems around archaic measurements and concepts from a bygone era. We need to move on, and The Prism exists to illuminate a new, identity-safe ecosystem, one that's built on the core element of biometrics.

Government Systems of Record and Regulation Are Integral to ID Empowerment

From our current standpoint, the biometric digital identity industry is bringing us toward the reality of a privacy-enhancing, user-asserted, interoperable digital identity that empowers the user at its core. This is not a new idea—the early days of Web3 and blockchain technology gave rise to the idea of Self-Sovereign Identity (SSI). But many early proponents of SSI ignored the need for strong identity proofing during the onboarding process, a challenge that has been addressed by contemporary mobile ID programs which leverage government systems of record to anchor a user's biographical identity.

As the identity landscape evolves, and mobile/digital ID programs emerge in real world deployments—be they mobile drivers licenses in the United States, European eIDs, or national registries in Africa and South East Asia—it is becoming clear that a government system of record is a key building block for a fully realized biometric digital identity. And while this may run against the government agnostic philosophy of early SSI concepts, the end result—if supported by international standards and regulations—will be effectively similar: users will have control over their identity data, with the ability to assert the credentials they

need on a transaction-by-transaction basis. But in this version of identity, relying parties will have the confidence of government identity at the root of every digital identity on their network, even in anonymous or pseudonymous transactions like age checks.

Taking Aim at Identity Excellence

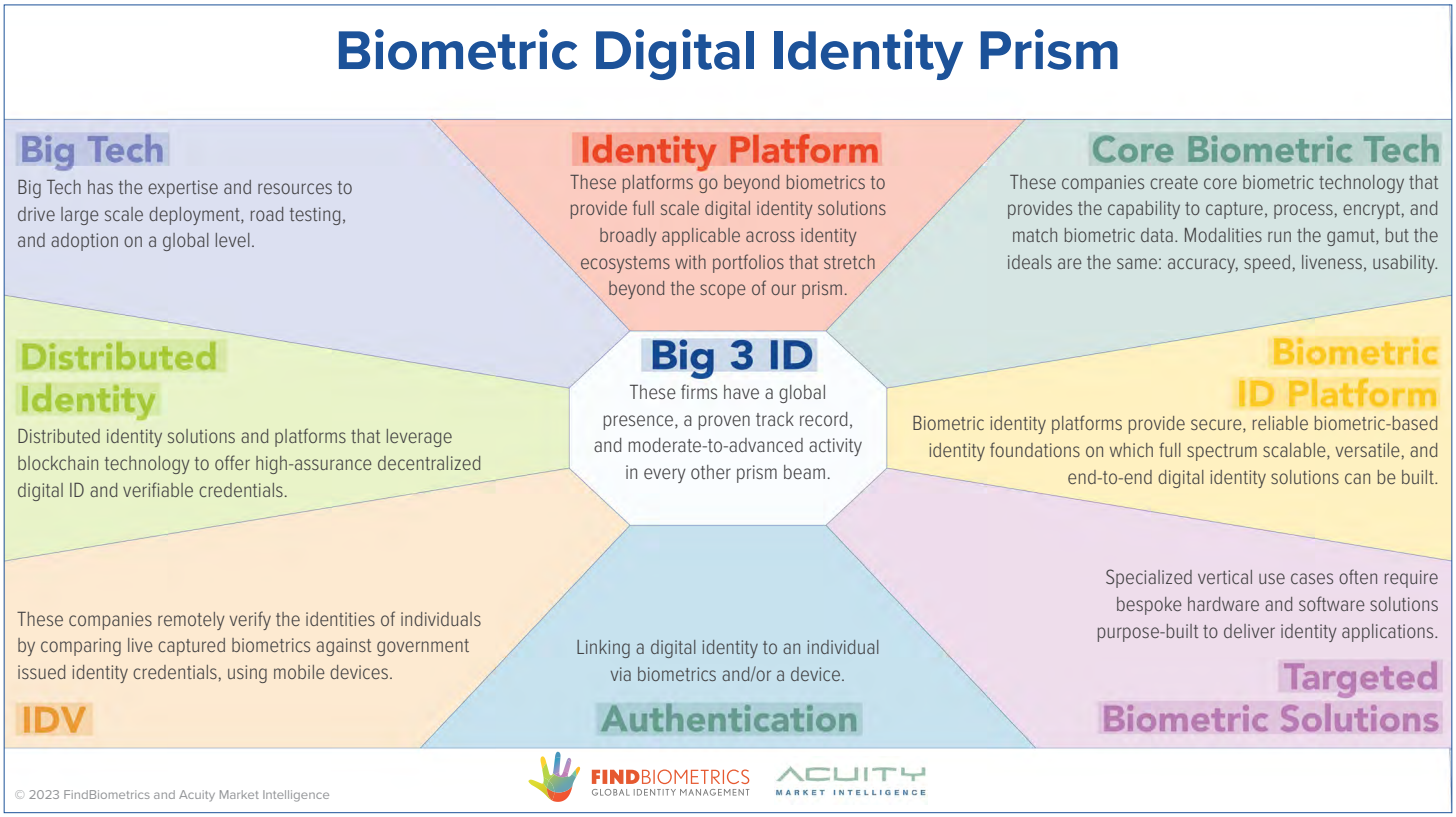
Human identity is complex and so are our digital lives. That's why the biometric digital identity prism is divided into eight segments we call "Beams." Consistently, while conducting the evaluation on this report and taking a high-level view of the industry landscape, we have seen that leading vendors consistently have well-defined target markets and use cases.

Something as fundamental as identity technology has a wide breadth of applications. A biometric digital identity solution can theoretically protect banks, optometry clinics, DMVs, chocolate stores, hotel rooms, and dating profiles. In the wake of the COVID-19 pandemic, a massive wave of biometric vendors flooded the identity and authentication markets to serve the urgent needs of remote work and digital transformation. Despite the plethora of potential customers in a range of industries, successful players followed well-defined strategies laser focused on serving specific use cases in well-defined target markets.

Prism vendors have succeeded by understanding their key differentiators and being purposeful in what they do. Seeing beyond technology-driven responses to immediate needs, they recognize the opportunity that accelerated digital transformation in one facet of an organization can define, drive, and open doors for larger scale evolutionary change across the entire enterprise.

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. FindBiometrics and Acuity Market Intelligence conceptualize 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.



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.

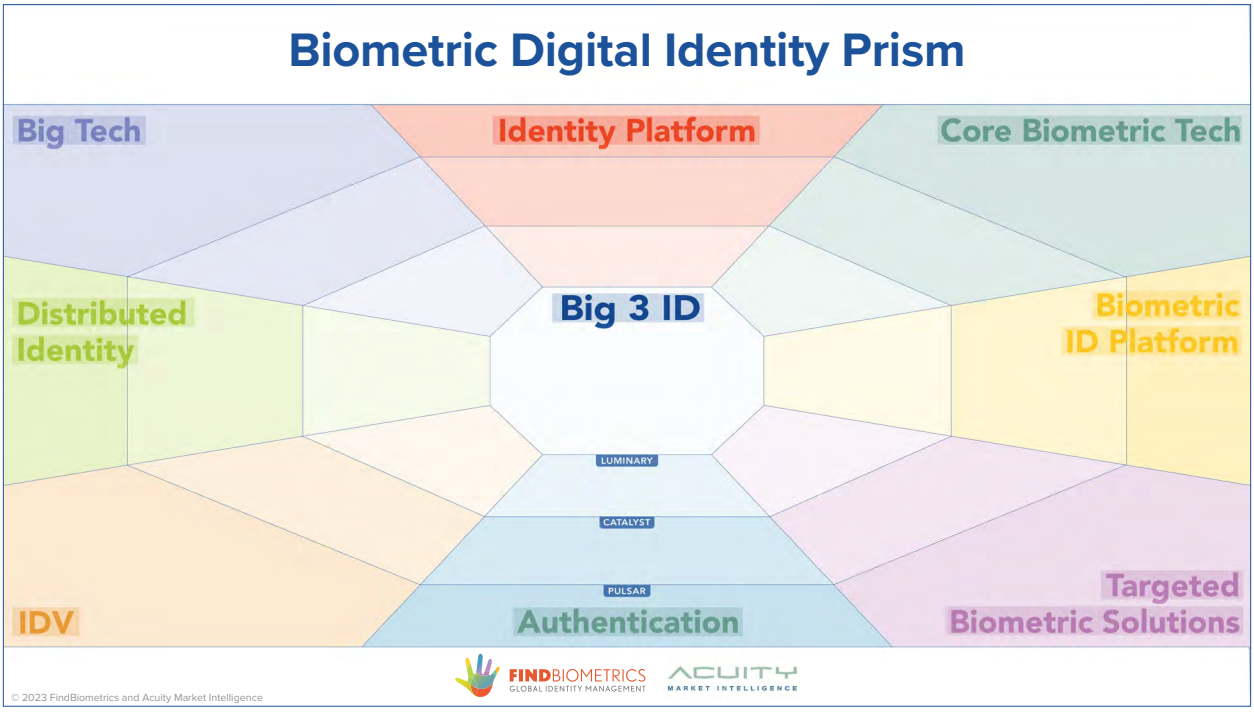
Luminary

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.

Refractors and the Big 3

The center of the Prism is anchored by the Big 3 of Identity – IDEMIA, Thales, and NEC. 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.

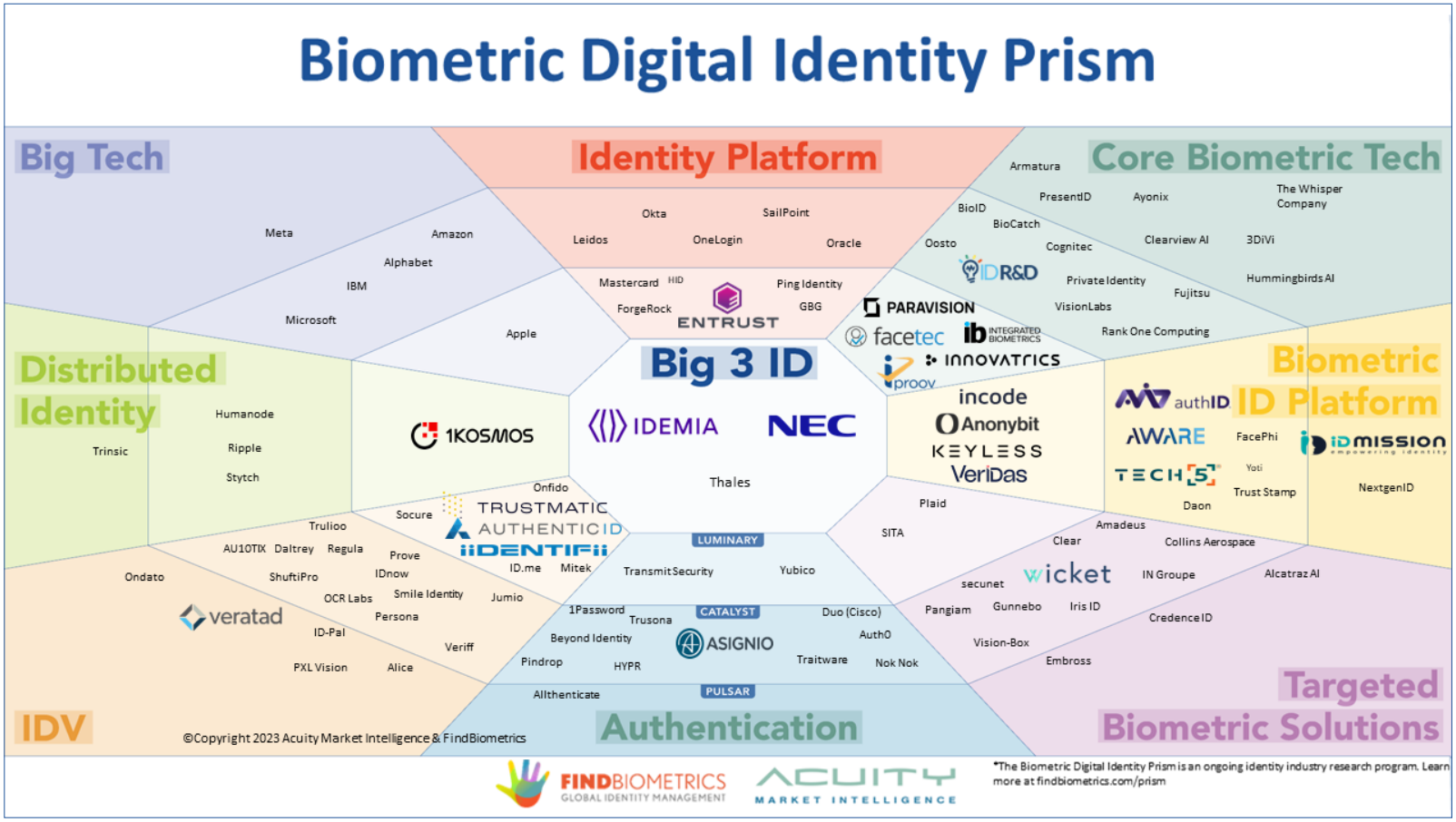
As the market evolves through acquisition, development, regulation, and innovation, the Refractor position may grow or diminish. Luminaries in Big Tech and the Identity Platform beams are best positioned to ascend to Refractor status. Meanwhile, the impending sale of IDEMIA's identity solutions portfolio will likely shift its buyer into the center of the Prism.



Vendors on the Prism Ecosystem

Important Note on Prism Beams:

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.

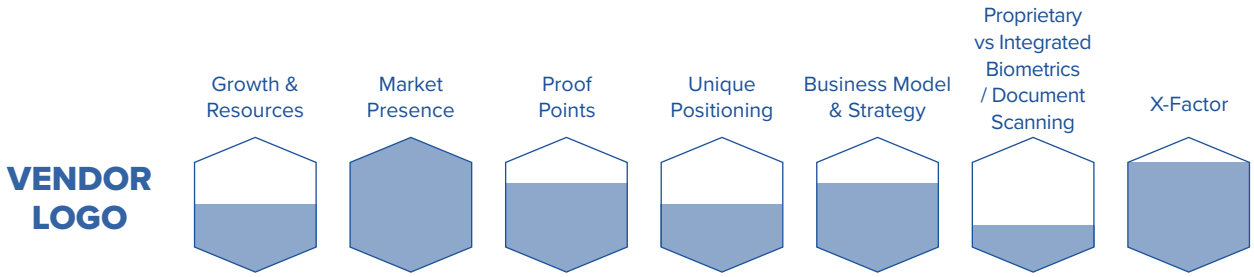


Evaluation Criteria

In order to place vendors on the Biometric Digital Identity Prism, we are assessing the leading companies based on six criteria.

- Growth & Resources
- Market Presence
- Proof Points
- Unique Positioning
- Business Model & Strategy
- Proprietary vs Integrated Biometrics
- X-Factor (Beam Specific)

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.



Given the shifting dynamics and standards of the biometric digital identity industry, vendors will be rated on a bell curve, and it should be noted that inclusion in the Prism indicates meeting a notable level of capability and potential. All included vendors in the Biometric Digital Identity Prism are worthy of consideration.

Prism Beams and Evaluations

The Prism is constantly evolving along with the biometric digital identity landscape. The evaluations presented here have been processed through independent research, industry surveys, and consultation with vendors, researchers, and analysts. If you see your organization here and believe it should be repositioned or re-evaluated, contact our team for a briefing.

This is not a comprehensive vendor list. If your organization is not represented here, please visit findbiometrics.com/prism and fill out our prism placement request form.

Important Note of Evaluations and Prism Placement:

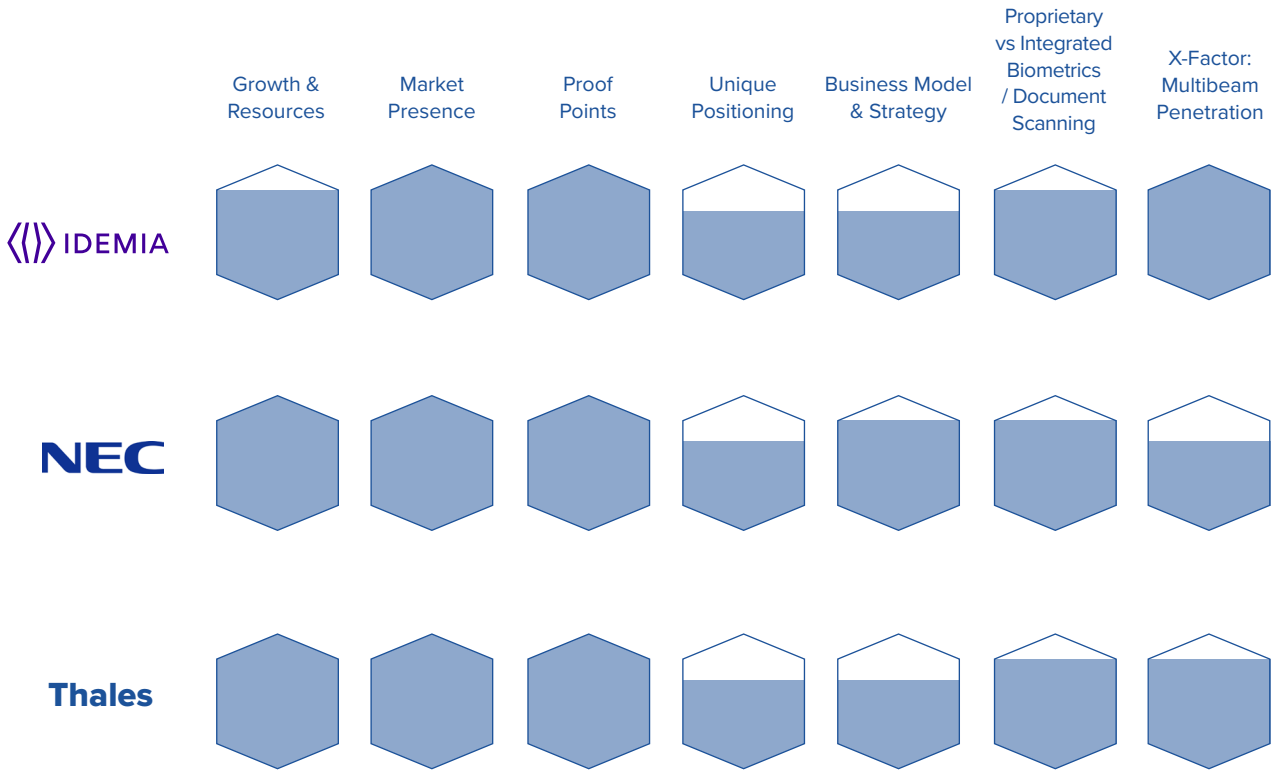
The vendor specific metrics in this report are based on publicly available data, survey data, interviews, and confidential briefings. It is presented in good faith as a representation of the biometric digital identity ecosystem according to the values stated previously in this report. **If you see your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

Big 3

These firms have a global presence, a proven track record, and moderate-to-advanced activity in every prism beam.

Prism X-Factor: Multibeam Penetration

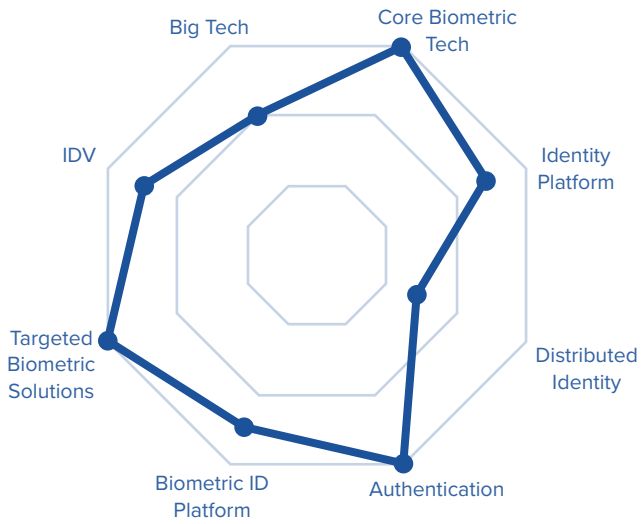
Evaluations



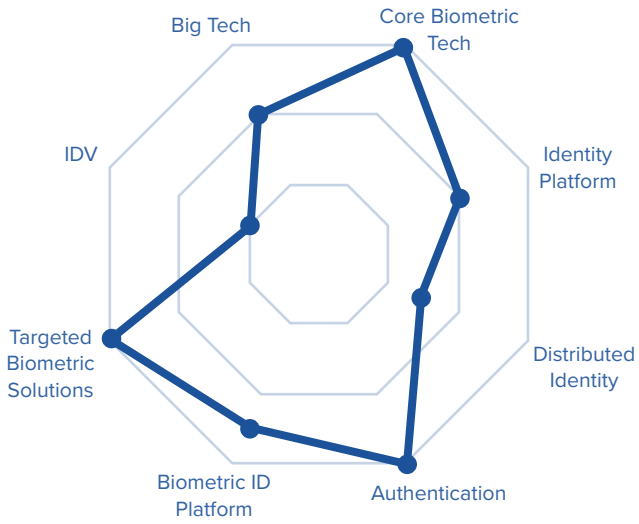
Refractor Beam Penetration

The Big 3 have made significant inroads into all Prism Beams, positioning them in the center of the biometric digital identity landscape.

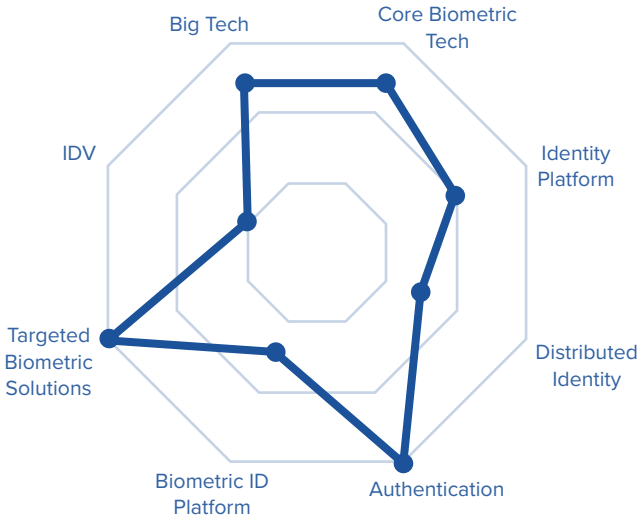
IDEMIA



NEC



Thales

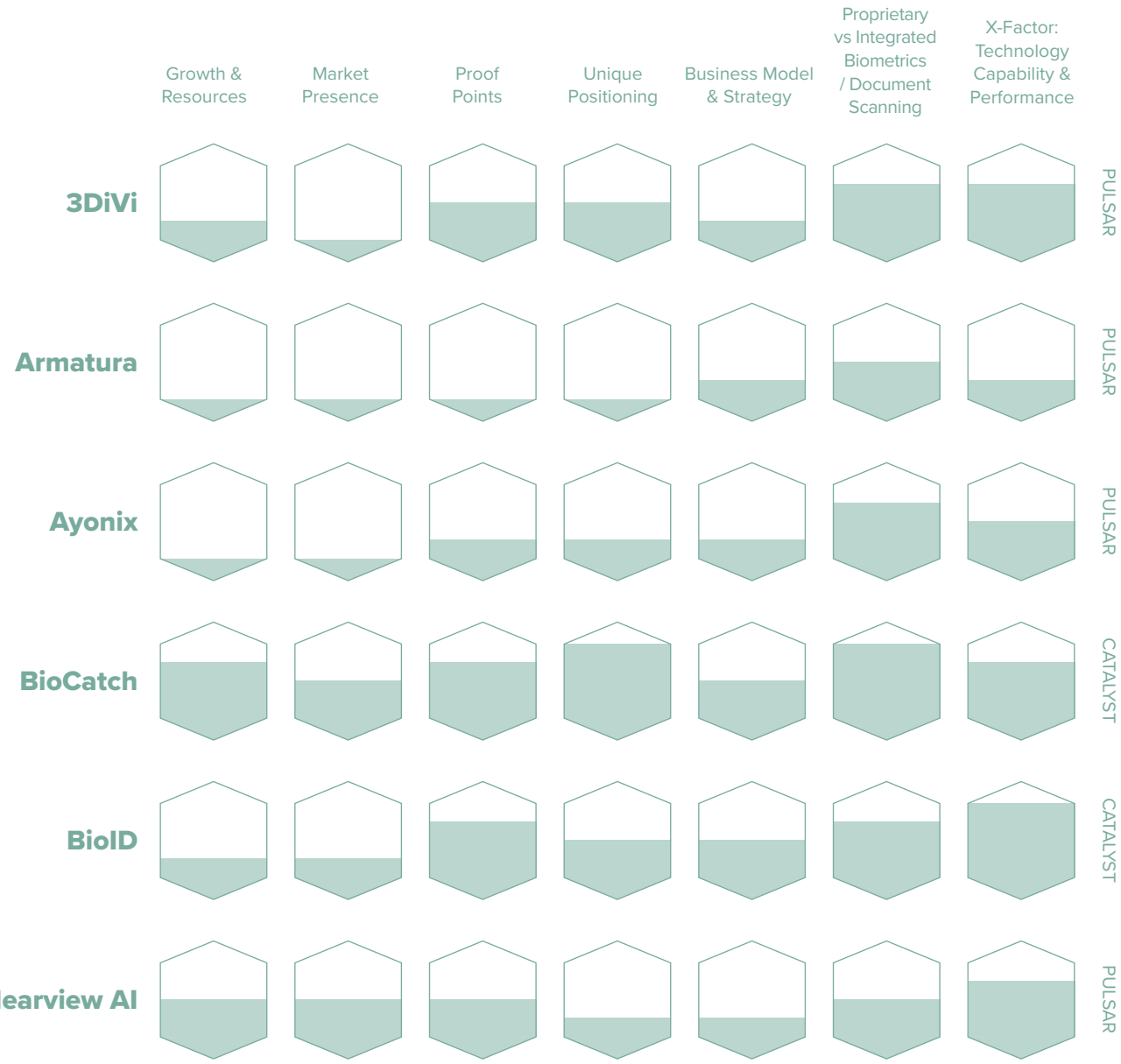


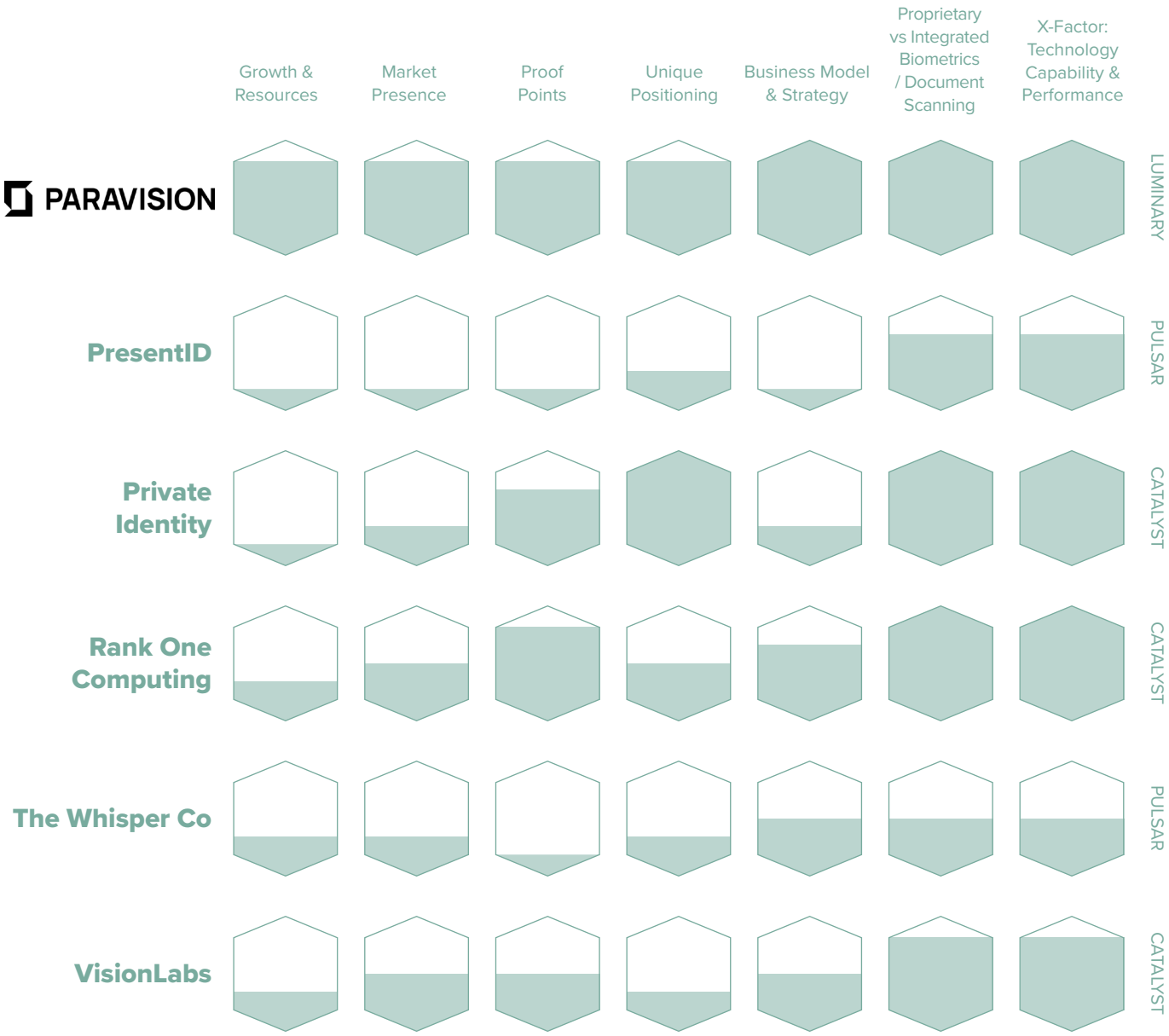
Core Biometric Tech

These companies create core biometric technology that captures, processes, encrypts, and matches biometric data. Modalities run the gamut, but the ideals are the same: accuracy, speed, liveness, and usability.

Prism XFactor: Technology Capability & Performance

Evaluations

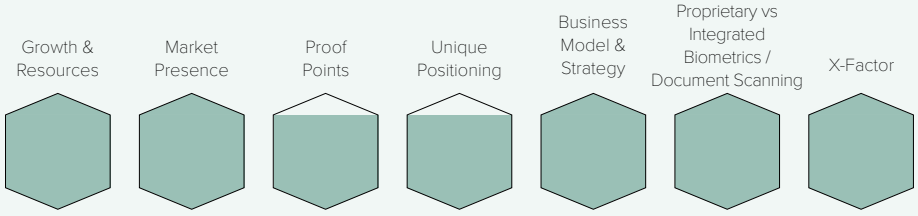


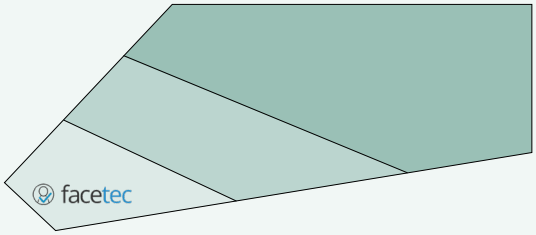


FaceTec

facetec.com

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





Founded in 2013, FaceTec is a notable pioneer in modern face biometrics, particularly on mobile. Their highly sophisticated 3D FaceMap system creates a detailed 3D biometric template for exceptionally high-performing liveness detection and face matching based on just a few seconds of selfie video. FaceTec has consistently reported significant gains in revenue and usage in recent years and continues adding value to its Digital Identity Suite with free features like Photo ID OCR, Barcode & NFC Chip Scanning, and anti-fraud layers like 1:N search for bad actors. FaceTec has reinforced trust by creating the industry's only Spoof Bounty Program, now offering total payouts of $600,000 for hackers who can successfully best its 3D Face Liveness software. What's more, third-party testing has determined that FaceTec's biometric matching is free from the demographic biases found in other facial recognition systems.

3D Biometrics Around the Globe

Over 500 million people on six continents have proven their Liveness remotely with FaceTec software using smartphones, tablets, laptops, and PCs. FaceTec's intuitive, accessible user interface requires only a quick "video selfie" and works effectively on low-cost devices with camera resolutions as low as 0.3 megapixels. FaceTec's software runs inside its customers' firewalls, unlike SaaS service providers, ensuring a privacy-by-design architecture, avoiding a centralized single point of failure many services are vulnerable to. Further, FaceTec never receives end-user PII or biometric data, preserving its inherent compatibility with privacy frameworks such including GDPR, CCPA, and BIPA. FaceTec's Neural Network models are inclusive of ethnicity, gender, and economic status.

FaceTec now provides almost two billion distinct 3D Liveness checks annually, with over 100 direct software customers and nearly 100 integration partners serving over 500 organizations globally. Examples include mobile driver licenses in Colorado, Utah, and Wisconsin, identity programs for the U.S. Department of Homeland Security's Electronic System for Travel Authorization (ESTA) program, the Canadian Parliament Remote Voting Verification System, and the Digital Dubai project.

Three-Dimensional Anti-Fraud Shield

FaceTec operates the world's first and only persistent Biometric Spoof Bounty Program, ensuring real-world security by incentivizing hackers to attempt to beat its biometric security platform. FaceTecs 3D Face Liveness and biometric matching software successfully defended over 130,000 bounty program attacks over four years, providing unmatched insight into the methods required to rebuff the most sophisticated, current threats to remote access management and biometric identity verification. By testing their AI so publicly, FaceTec is an example of how Core Tech vendors can lead the market through transparent testing, which has been recognized by groups such as the European Union Agency for Cybersecurity.

Designed to Verify People, Not Devices

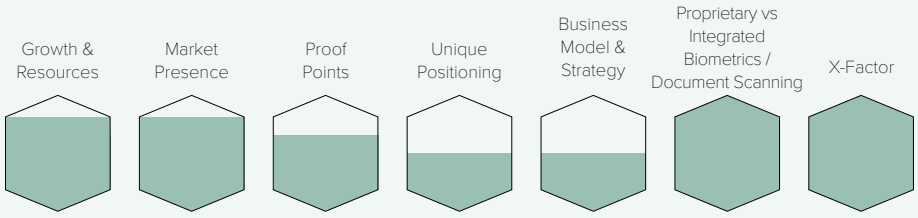
Unlike other 3D face authenticators requiring specialized hardware, such as Apple's infrared FaceID, FaceTec's software-based 3D face biometrics technology works on all popular operating systems and on a broad array of devices, including pre-FaceID, inexpensive handsets. This commitment to accessibility positions FaceTec as a proactive champion in the emerging global biometric digital identity ecosystem. Identity is part of who you are, and being able to assert it should have no relation to how expensive your phone is. FaceTec marries accessibility, performance, and innovation to play a definitive role in the Biometric Digital Identity Prism.

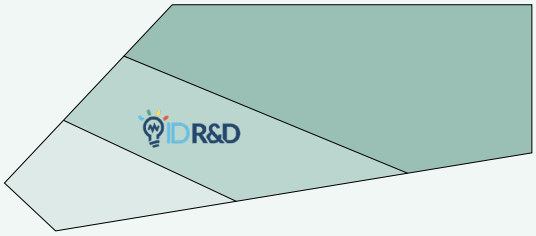
Contact FaceTec: JohnW@FaceTec.com 1-415-997-9235

ID R&D

idrnd.ai

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





True to its name, ID R&D has invested considerable effort in technological innovation, and has become an important vendor of face and voice biometrics technologies to major players in the identity and security industries including Thales and TECH5. ID R&D consistently ranks first in voice algorithm challenges, and was prominently represented among top-ranking algorithms in the NIST passive facial PAD evaluation report. The company's passive liveness technology for facial recognition and its anti-spoofing tech for voice recognition attracted the attention of IDV Luminary Mitek, which acquired ID R&D in 2021. The company continues its research and development efforts under its own brand name, and, in addition to its face and voice technologies, ID R&D also offers a document liveness solution for remote identity verification.

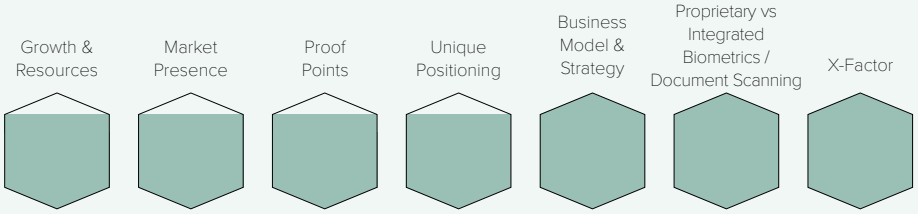
Thanks to its parent company's market reach and formidable resources, ID R&D is well positioned to continue its innovation as a Biometric Core Tech Catalyst. Its multi-biometric proficiency is a major boon, particularly when it comes to liveness detection, as platform-based identity solutions increasingly deploy voice recognition in addition to face—both of which are under a growing threat from AI-based deepfake attacks. The rapid rise of gen AI-powered chatbots and voicebots add yet another important use case for liveness. Similarly, document liveness is essential in preventing synthetic identity fraud during the onboarding process. ID R&D plays a fascinating role in the Biometric Digital Identity Prism, acting as a boon for its Luminary parent company while also providing its technology to other vendors in the Platform and Big 3 Beams, and illustrating the interconnected nature of the emerging industry ecosystem.

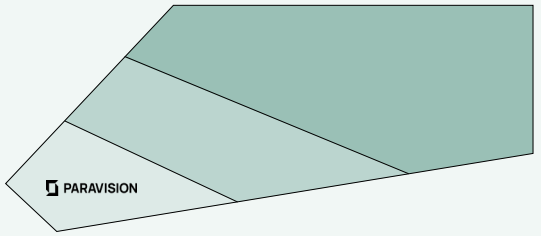
Contact Paravision: info@idrnd.net

Paravision

paravision.ai

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





Based in San Francisco, Paravision has made a name for itself as one of the top-performing Western vendors of facial recognition in independent testing programs like those run by the National Institute of Standards and Technology, whose face recognition evaluation programs ranked Paravision first in 1:N identification and 1:1 verification among all participants based in the US, U.K., and EU in mid-2023. The company has also distinguished itself with a set of AI Principles, committing to ethically built and conscientiously sold computer vision solutions; and its status as a principled, US-based facial recognition supplier has helped the company to win high-profile clients including HID, ID.me, Persona, Secunet, and Vision-Box.

Through its partner-based strategy, Paravision provides its formidable face biometric tech to other Prism vendors, enabling them to focus their in-house resources on their own core competencies. This Biometric Core Tech Luminary is the perfect example of how the Prism envisions the future of biometric digital identity: an ecosystem of vendors working in partnership to achieve safe, secure, and scalable digital identity. With proof points spanning key markets and a clearly defined, laser-focused roadmap, Paravision distinguishes itself as a leader in its field. Its ethically sound vision for the future of identity is aligned with our researchers, who see a bright future for the company.

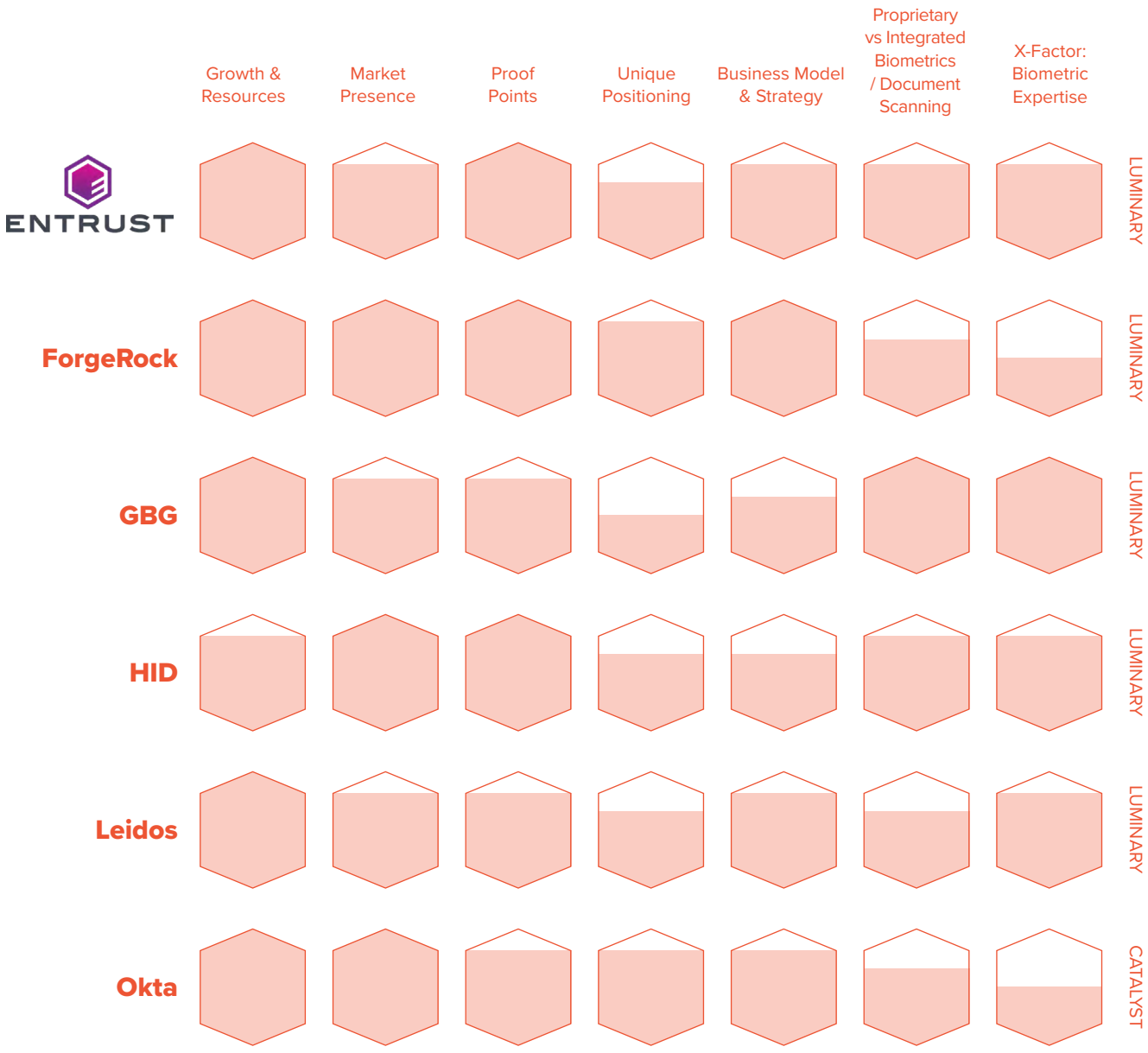
Contact Paravision: info@paravision.ai

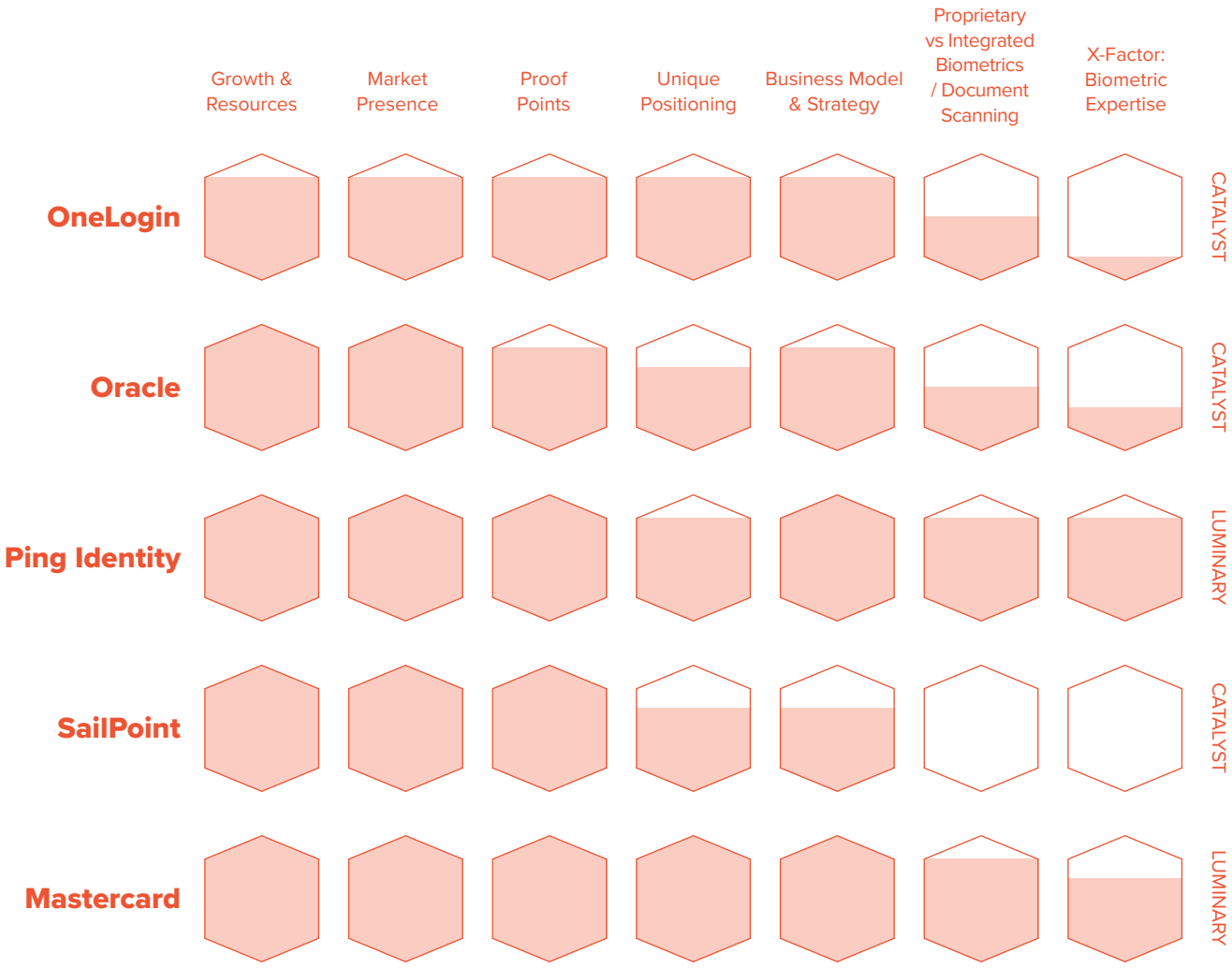
Identity Platform

These platforms go beyond biometrics to provide full-scale digital identity solutions broadly applicable across identity ecosystems with portfolios that stretch beyond the scope of our prism.

Prism XFactor: Biometric Expertise

Evaluations

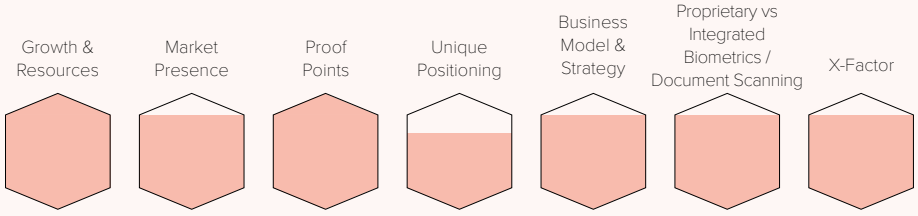


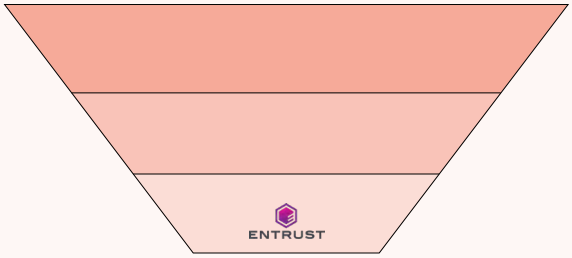


Entrust

entrust.com

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





Entrust was founded in 1969 as Datacard, a pioneer and leader in financial card, smart card ID, and governmental credential issuance. The company acquired Entrust in 2013 – a spin-off of Nortel in 1997 that developed the world's first commercially available public key infrastructure. The combined entity emerged as Entrust Datacard the next year, and changed its corporate name to Entrust Corp. in 2020 to reflect its focus on secure identity, data protection, and payments technologies. Its work now extends to mobile credentials, and the company is involved in high-profile projects including the development of a biometric immigration processing app for the United Kingdom's Home Office.

Entrust stands out as a Luminary in the Identity Platform Beam. With a global reach, established expertise, proprietary biometrics and ID scanning technologies, and activity in crucial ID use cases across a range of sectors, the company has the potential to become a Biometric Digital Identity leader in the next five years. Entrust differentiates itself from its fellow Identity Platform players thanks to its proactive stance on biometric technologies. While many vendors its size boast strong biometrics solution portfolios, Entrust is ahead of the curve in integrating biometrics into its identity solution portfolio (like financial and seamless travel/borders), and positioning them as integral to its digitization roadmap It is the opinion of our researchers that Entrust is among the most likely candidates to ascend to Refractor Status in the Prism (placed in the central "Big 3 ID" section).

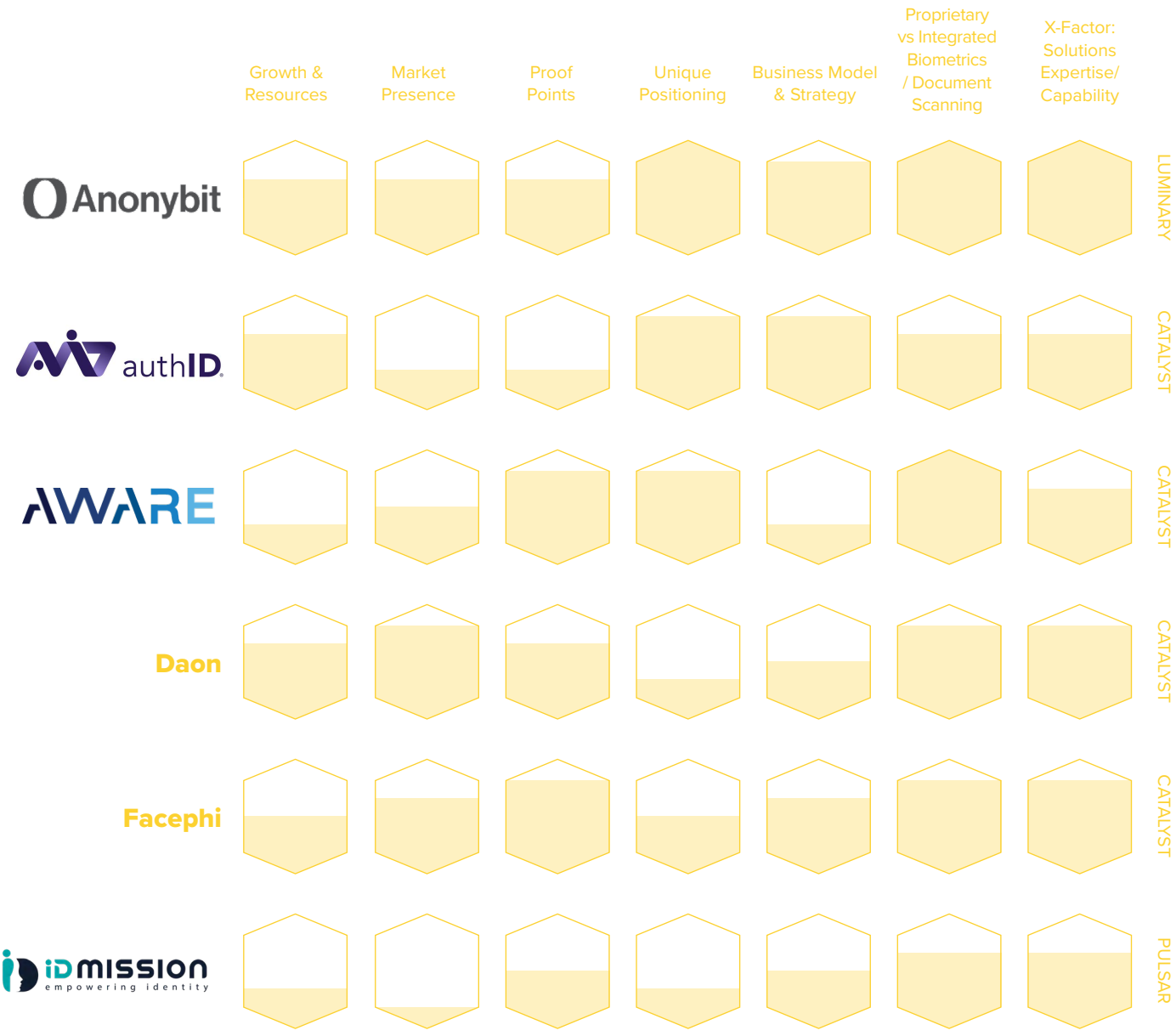
Contact Entrust: entrust.com/contact

Biometric ID Platform

Biometric identity platforms provide secure, reliable biometric-based identity foundations on which full spectrum scalable, versatile, and end-to-end digital identity solutions can be built.

Prism XFactor: Solutions Expertise/Capability

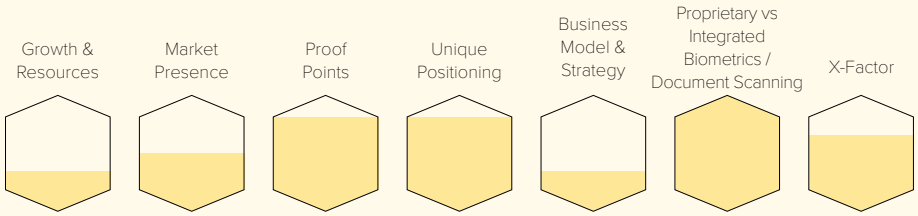
Evaluations

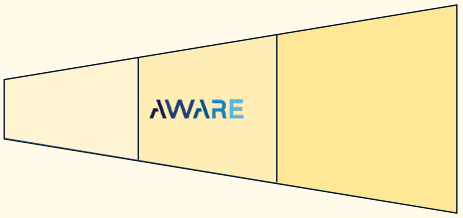


Aware

aware.com

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





Aware was founded in 1986, and it has evolved along with the biometrics and digital identity industries ever since. With strong roots in government and law enforcement, Aware has a foundation of robust capture, search, and matching technologies, trusted by agencies around the world. It boasts proprietary biometric technologies spanning the range of core modalities (face, fingerprint, iris, and voice), and serves orchestrated identity services and solutions to customers in the retail, payments, banking, enterprise, healthcare, travel, and government sectors. Operating in over 20 countries, Aware now offers government-trusted biometric digital identity to those sectors with the mission of balancing security and user experience.

Biometrics Expertise Keeps Aware Ahead of the Curve

With a portfolio of turnkey solutions, frameworks, SDKs and identity system building blocks, Aware's greatest strength is its biometrics expertise. If you want to know the history of biometrics, trace Aware's history. The firm has consistently anticipated market needs and developed or acquired technology to meet them. Notably, its Knomi® mobile biometric authentication framework was launched in 2017, just as liveness detection, face, and voice biometrics were entering mainstream commercial use. Anticipating the increased need for verification technologies in the onboarding process, Aware acquired Fortress Identity in 2022. This flexible attitude toward keeping its portfolio competitive puts Aware ahead of similarly mature players.

Ready to Connect, Deploy, Verify, and Authenticate

Aware's decades of innovation have done more than keep it on the cutting edge. In 2023, the company has a robust portfolio of biometric technologies in line with the evolving direction of biometric digital identity. These range from turn-key solutions, to biometric frameworks, to SDKs. It's BioSP™ is a powerful middleware solution for identity management, while its new AwareID® solution is ready to deploy out-of-the-box for low-code verification and authentication. Every vendor in the Biometric ID Platform Prism Beam is positioned thanks to its ability to fully orchestrate user identity, and it's here that Aware stands out: exemplifying the many forms that full-lifecycle identity can take through its products, frameworks, connectors, and building blocks, all fine-tuned for its customers' specific needs.

An Advanced Ecosystem Player

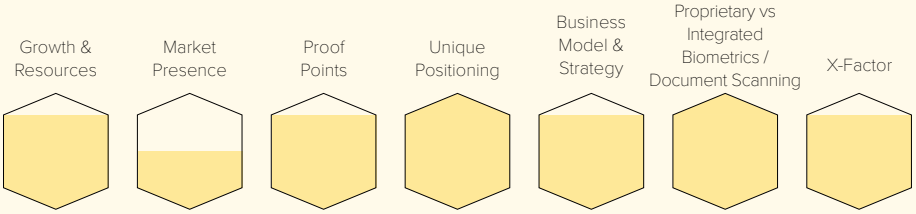
The emerging biometric digital identity ecosystem is diverse, interconnected, and global. Variety is integral to the future of digital ID. Aware's long standing commitment to interoperability in its technologies and its embrace of international standards enable the company to help clients avoid vendor lock-in, which happens when a single aggressive player takes advantage of the leap-frog effect, in which developing nations are able to deploy advanced identity systems because of their lack of legacy infrastructure. That adaptability and flexibility, along with its proven track record in developing markets like Africa, makes it a role model for the biometric digital identity industry while positioning it for success as the world moves into the next phase of digital ID.

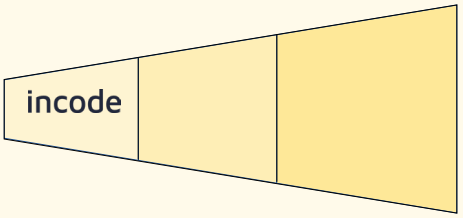
Contact Aware: sales@aware.com

Incode

incode.com

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





Headquartered in the San Francisco Bay Area, Incode offers an identity platform that includes a selfie-based identity verification tool as well as a digital ID solution designed to store virtual versions of physical IDs in a user's smartphone. The company has some major backers in the venture capital space, including SoftBank and J.P. Morgan, among others; and has evidently leveraged this funding to build an identity platform that is compliant with regulations including the European Union's GDPR and the California Consumer Privacy Act (CCPA), and verified against stringent standards such as ISO 30107-3 and SOC 2 Type 2. Incode has established a market presence across a range of sectors, and has made particularly notable inroads in financial services, online gaming, sports & entertainment, and hospitality.

A Culture of Innovation

Incode develops its own technology in-house. It fully owns an entire suite of identity verification technologies and KYB products. Face biometrics are the core of this Biometric ID Platform Luminary's technology supported by AI and machine learning to enable the best possible performance on the edge. This research and development driven company is guided by a mission of replacing the failing legacy identity infrastructure of yesterday with reusable identity, via its vendor agnostic orchestration platform. In recent years, as the identity industry experienced what Acuity Market Intelligence terms a 'rogue wave,' Incode has been able to scale quickly and to deftly navigate a turbulent market. Incode's continued growth under dynamic market circumstances is a testament to its culture of innovation.

For UX Optimized Identity Orchestration

Incode Omni, the company's flagship identity orchestration platform is sleek, fully automated, accurate, and privacy-first, standing out as superlatively user friendly. As biometric digital identity becomes commonplace, the industry needs to follow Incode's example of intuitive backend controls. While other vendors offer basic, text-based interfaces for managing identities, Incode Omni stands out as proof that identity innovation should not end under the hood: performance includes interface.

And Advanced AI Integration

The line between user interface and performance innovation blurs even further with this Luminary's approach to artificial intelligence. With the Incode AI Suite, the company has integrated generative AI into its orchestration workflows, effectively allowing administrators to ask the platform questions and receive actionable identity and risk level insights in real time. Beyond being a useful tool, Incode's AI Suite is another example of what can happen when formidable resources are channeled through an organization with a singular sense of purpose—powering a world of trust.

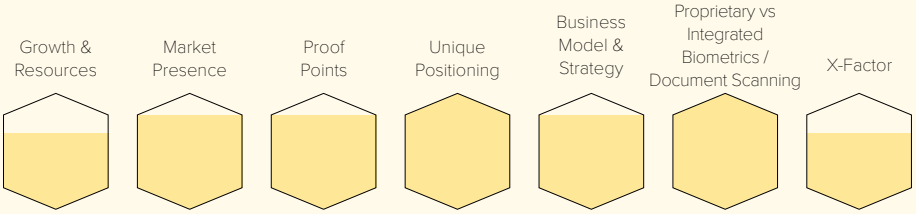
Contact Incode: christian.pascual@incode.com 1-352-745-2279

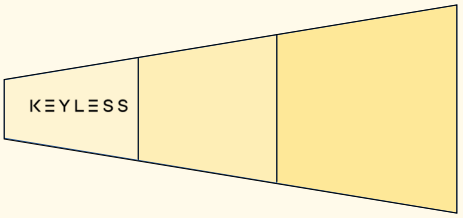
Keyless

keyless.io

KEYLESS

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





Keyless is carrying the torch for platform-based biometric digital identity. This Prism Luminary extends the traditional security perimeter to include the end user with its proprietary cryptography and face biometrics technology. Frictionless experiences, strong security, regulatory compliance, and rapid ROI are major selling points for Keyless' biometric authentication platform—offered through flexible deployment models, including cloud-native, hybrid, and on-prem—and the company prides itself on meeting all global compliance and data sovereignty requirements, including GDPR and CCPA, and regulatory requirements such as PSD2 SCA, with certifications pertaining to FIDO Biometrics, FIDO2, information security management, quality management, and more. This all adds up to a strong biometric authentication platform ready to move organizations—particularly those in the financial sector—into an era that relies less on traditional (and phishable) keys like passwords, tokens, and magic links.

Leveraging True User Identity with Zero-Knowledge Biometrics

Keyless is not simply replacing passwords with biometrics—its MFA-by-design solution positions true user identity as the primary credential for all transactions. Capturing two authentication factors in one look, Keyless defends against deepfakes and spoof attacks. It's great for user experience, too. With a single selfie upon enrollment, a user can continue to authenticate and assert their identity through every interaction on a Keyless-protected service, across any device. This is all facilitated through the company's trademark Zero-Knowledge Biometrics, a unique zero knowledge cloud computing model designed for privacy and compliance. With Keyless, biometrics are stored neither on devices nor in the cloud, simplifying compliance with data privacy regulations. Our researchers see this as a realization of a core concept of the Prism: that biometrics are not analogous to passwords.

Account Recovery in the Age of Automation

A persistent challenge for all post-password authentication systems is the account recovery step. When a user loses access to strong credentials, a system's weakness is revealed: many biometric authentication systems revert to a password or magic link for account recovery, making them as vulnerable as legacy systems, while solid device-based authenticator apps demand lengthy and costly call center processes that can take days. With Keyless, account recovery is a simple process that can get a verified user back on the platform as quickly as taking a selfie. As automated account recovery becomes an increasing priority for the identity ecosystem, Keyless is among the handful of vendors leading the way.

Fulfilling the Promise of Full-Lifecycle ID

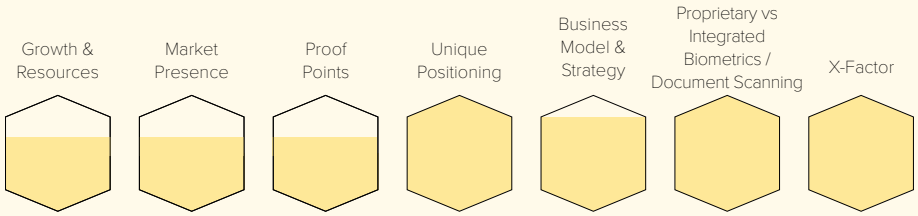
User experience is a priority of Keyless, and that is on display with its various controls to reduce friction, even beyond the enrollment and login steps. Modeled after the mainstream IAM single sign-on experience, the company has integrated with risk platforms to enable step-up authentication when it is needed based on the weight of the transaction. In taking this approach, Keyless helps its partners move beyond a defensive stance that treats every user like a potential liability, enabling them to operate from a position of active customer satisfaction.

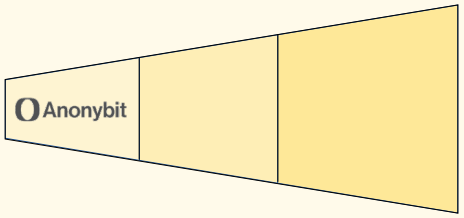
Contact Keyless: info@keyless.io

Anonybit

anonybit.io

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





Founded in early 2022 by biometrics industry veteran Frances Zelazny, Anonybit is pioneering a unique and unphishable approach to biometric digital identity. This Biometric ID Platform Luminary specializes in decentralized biometrics, offering a platform that breaks a given biometric template into shards that are distributed across multiple servers. Each shard is useless on its own, rendering the data essentially worthless in the event of an attack against any one server. Anonybit's fully orchestrated platform is algorithm agnostic, and the company invites vendors to adapt their tech to its platform.

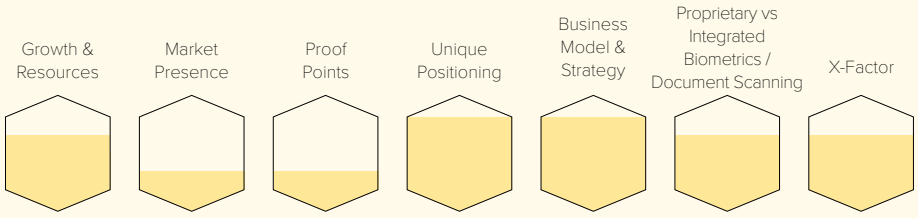
Privacy and data protection are essential to the future of biometric digital identity, so Anonybit's eponymous decentralized biometric storage technology is a showstopping differentiator. But it is important to highlight the company's strength as an integrated biometric identity platform. Many vendors, particularly in the IDV space, aspire to build themselves into platforms by adding additional point solutions that add authentication to their stack. Anonybit, by contrast, is a platform by design, taking a full identity lifecycle approach, orchestrating transactions, enhancing user privacy, and, of course, protecting biometric data in patented Anonybits.

Contact Anonybit: info@anonybit.io

authID

authid.ai

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



With its cloud-based biometric ID platform, authID shines bright as a Prism Catalyst, orchestrating identity while bolstering traditional security weaknesses with its flagship Verified product, powered by Human Factor Authentication. Having undergone a massive corporate overhaul in early 2023, supported by a new financing agreement, the company has rapidly evolved from an IDV player to a provider of end-to-end biometric digital identity that puts a premium on user experience. With a clear mission of enabling transferable, device agnostic digital identities that can be verified and authenticated in milliseconds after a one-time onboarding, authID is winning workforce customers around the globe and growing by orders of magnitude in its quarterly reports. Its technology is compliant with key regulations, supported by lab-tested liveness detection, scalable, and ready to deploy extremely quickly.

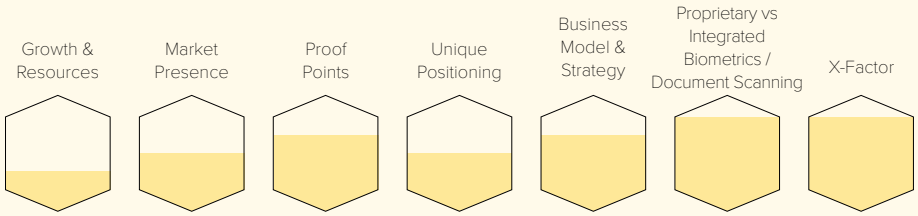
Speed is authID's characteristic strength—every aspect of its platform is fine-tuned with a frictionless, zero-trust customer experience in mind, from the administrative folks managing it through the employees onboarding and authenticating. But the firm's differentiating factor is its clear strategy and business model. This is a company that has identified the weaknesses of contemporary strong authentication systems, and rather than ask customers to abandon the mainstream options for something new, authID enhances what's already working. Critics of FIDO2 authenticators like passkeys generally focus on how they reduce the fraud attack surface to weak account recovery mechanisms, require new enrollments for each new device, and are not digitally bound to human identity. With its Human Factor approach to identity, authID fills these gaps by placing its real carbon-based users at the core of every transaction, enabling versatile biometric verification and authentication wherever and whenever it is needed.

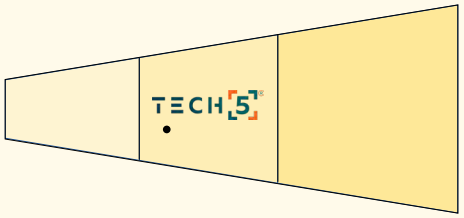
Contact authID: sales@authid.ai

TECH5

tech5.ai

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





With a leadership team spanning Switzerland and the United States, TECH5 is a global concern. The company places a strong focus on R&D and engineering, and has developed solutions for contactless fingerprint capture; 1:N identification via face, fingerprint, and iris recognition; 1:1 biometric authentication; and digital ID generation and issuance. The company is a member of the Secure Identity Alliance and the OSIA Initiative, and has been an instrumental technology vendor in large-scale projects, including a remote voter verification program in Oman and a pioneering digital ID initiative in Ethiopia. TECH5 extended its presence in the North American market through its acquisition of biometrics specialist Imageware Systems in early 2023. Recently, the firm received a patent for contactless mobile fingerprint technology.

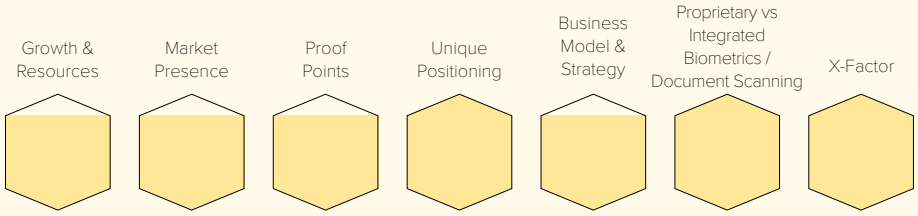
TECH5 is a Biometric ID Platform Catalyst thanks to its formidable portfolio of proprietary high-performance biometric solutions. But its innovations consistently strive to deliver on the inclusivity promise of biometric digital identity, building technologies for people in developing countries—introducing new methods of biometric portability, like its 2D Digital Storage for Biometrically Verifiable Digital ID. That inclusive paradigm, combined with 20 years of expertise and a track record of innovation, make TECH5 an important player in the Biometric Digital Identity Prism.

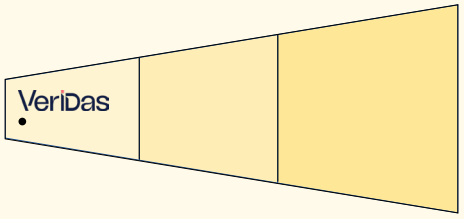
Contact TECH5: sales@tech5-sa.com

Veridas

veridas.com

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





Spain-based identity verification and authentication specialist Veridas has been in operation for a little over a decade, and now has a client roster spanning 25 countries. The company strives to meet a comprehensive set of identity needs across digital and physical realms. Veridas' portfolio of modular solutions includes ID document verification, face, and voice biometrics technologies. It also seeks to distinguish itself with adherence to stringent regulations such as the European Union's GDPR and California's CCPA, and through strong performances in evaluation programs run by the National Institute of Standards and Technology (NIST) as well as iBeta, which confirmed its compliance with the renowned PAD Level 2 liveness detection standard. It engineers its own Embedded AI Hardware to power a unique Facial Biometric Access Control platform.

With a powerful combination of resources, proprietary technology, and the ability to grow along with the industry in a sustainable way, Veridas has managed to scale its operations in accordance with the massive global demand for biometric digital identity, even as it accelerated during the pandemic era. The company has a well-rounded portfolio of proprietary technologies, including biometrics, that serve the full identity lifecycle. Strategically, this Biometric ID Platform Luminary has a clear vision of its place in the emerging digital identity ecosystem. As the Biometric ID Platform Prism Beam becomes more competitive in the coming years, Veridas will be well positioned as a leader in the space.

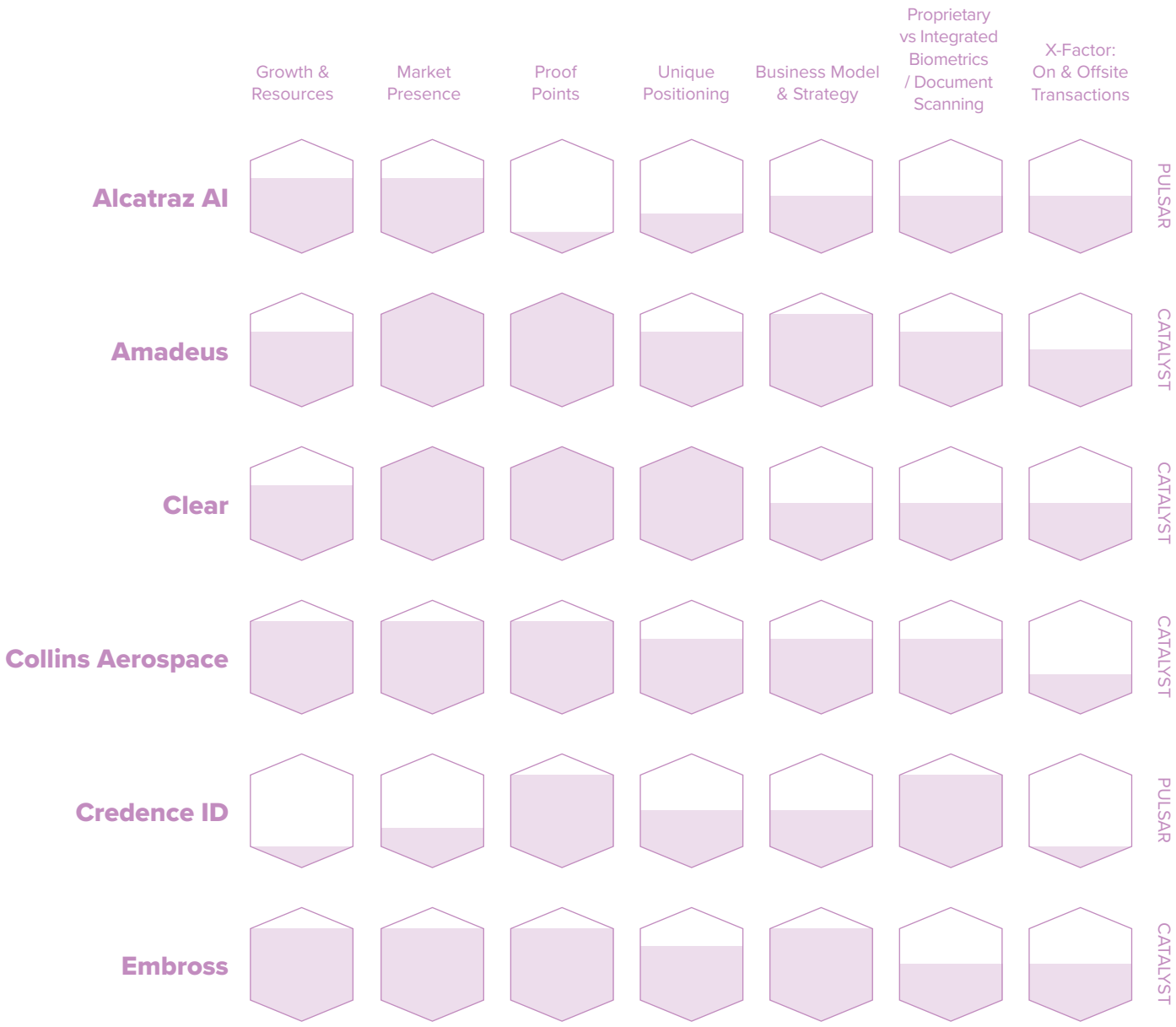
Contact Veridas: hello@veridas.com (+34) 948 246 295

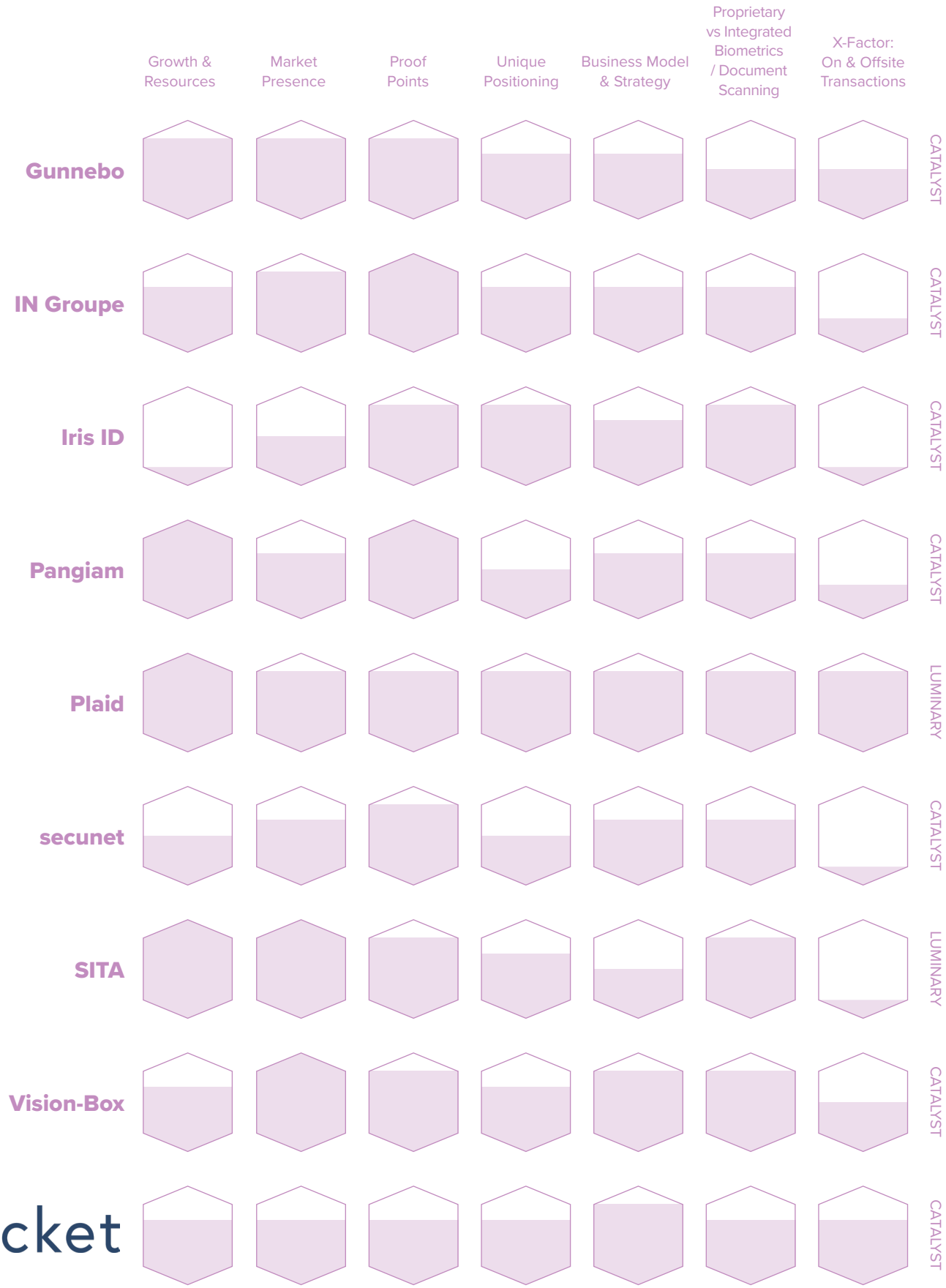
Targeted Biometric Solutions

Specialized vertical use cases often require bespoke hardware and software solutions purpose-built to deliver identity applications.

Prism XFactor: Integrated Mobile Onboarding, Payments, Other On & Offsite Transactions

Evaluations

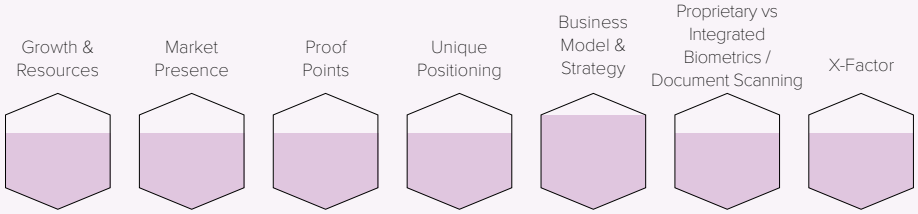


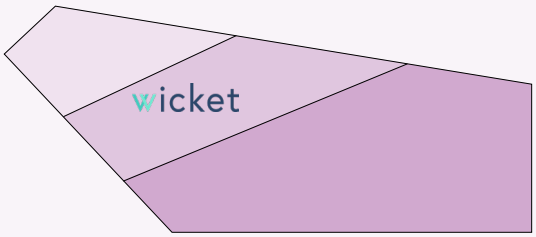


Wicket

wicketsoft.com

BEAM: **Targeted Biometric Solutions** / CLASSIFICATION: **Catalyst**





Wicket is a specialist in face-based entry for large-scale venues. Founded in 2020, the Cambridge, MA-based startup has established high-profile partnerships in the sports and entertainment sector—with over a dozen teams and stadiums using its tech, including the Cleveland Browns, the New York Mets, and Mercedes-Benz Stadium—and in air travel with Allegiant Airlines. It also boasts several deployments with conferences, rounding out its sports, live events, and corporate access control footprint. The company's solution enables end users who opt-in to enjoy seamless venue entry, allowing for highly efficient throughput. This offers considerable cost savings to its clients. The Cleveland Browns, for example, have seen an $8,000 cost reduction per entry lane using Wicket's solution.

A relatively new entrant to the Targeted Biometric Solutions space, Wicket burns bright as a Catalyst. With its high-profile deployments and customers singing its praises, the company has a proven track record after only a few years. From our researchers' perspective, it's Wicket's flexibility that makes it stand out—more than just ticketing, the company's solutions enable facility access control and seamless payments at concessions. Various market factors are shifting traditional hardware-based facility management strategies out of favor, and Wicket's value proposition is a perfect example of where the industry is heading: high-performance biometric identity management software that can be deployed through mobile devices like tablets. Stadiums, entertainment venues, airports, and even office buildings are all unique, and the Wicket model allows for rapid deployment at any facility, regardless of shape, size, or user throughput.

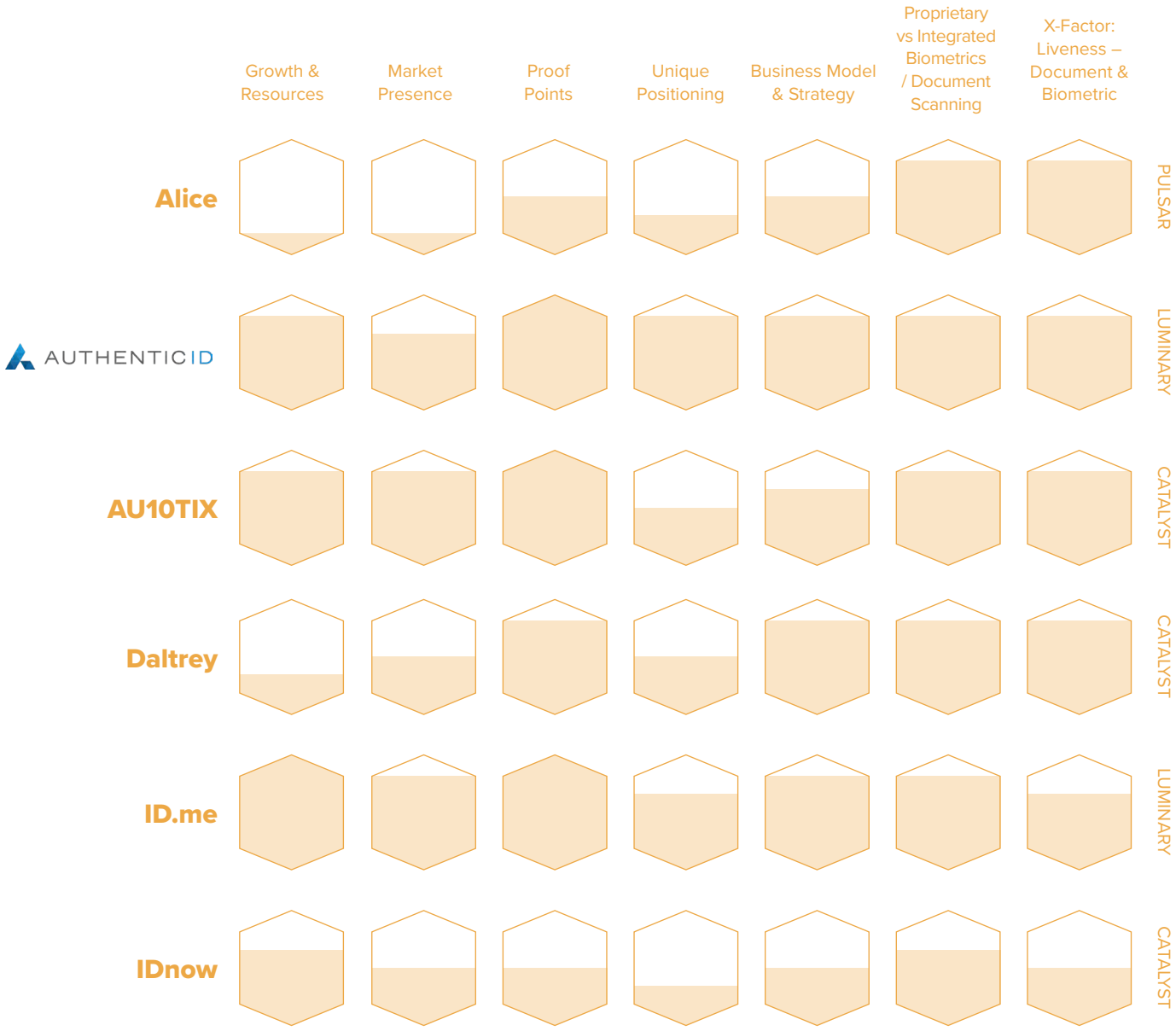
Contact Wicket: hello@wicketsoft.com

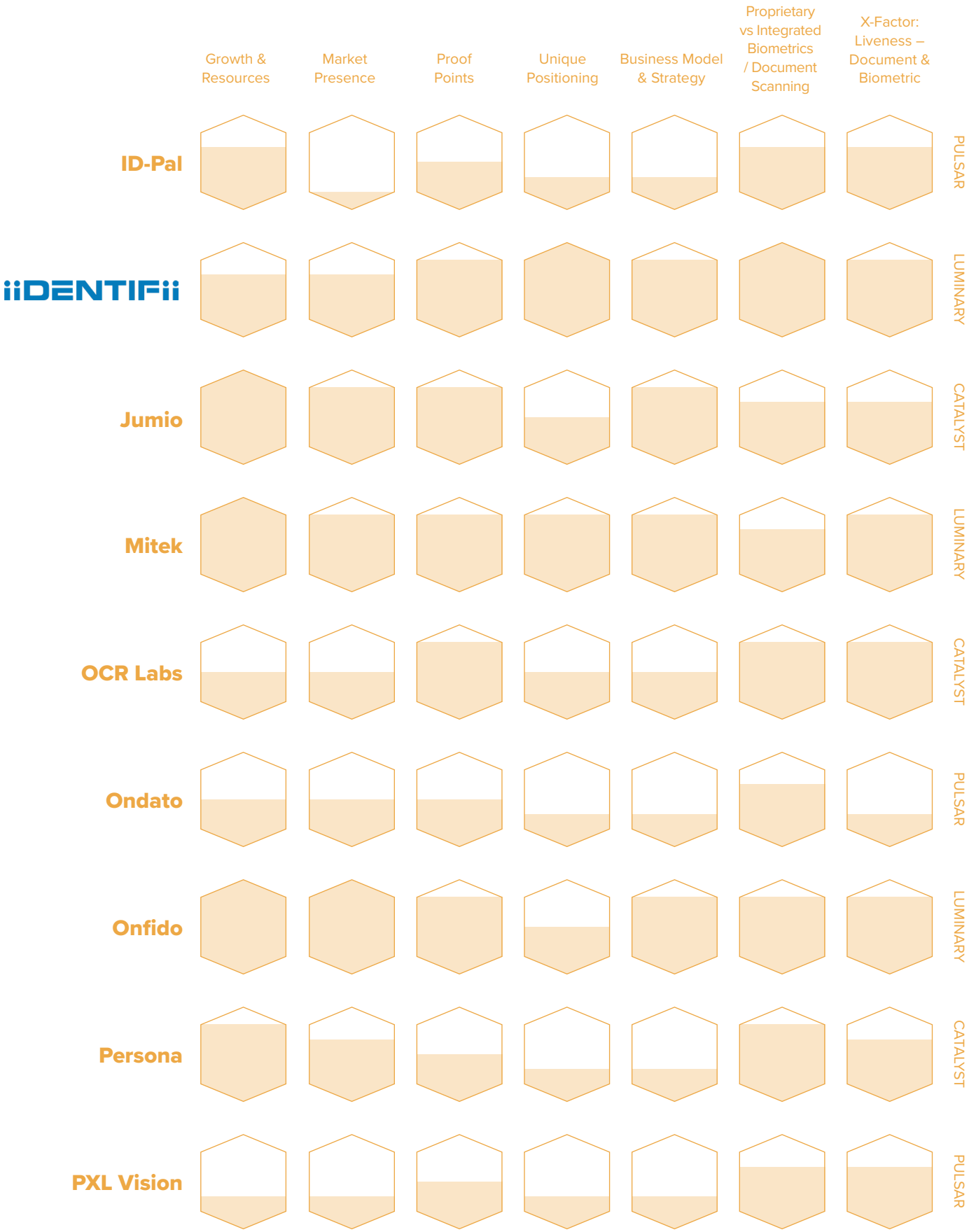
IDV

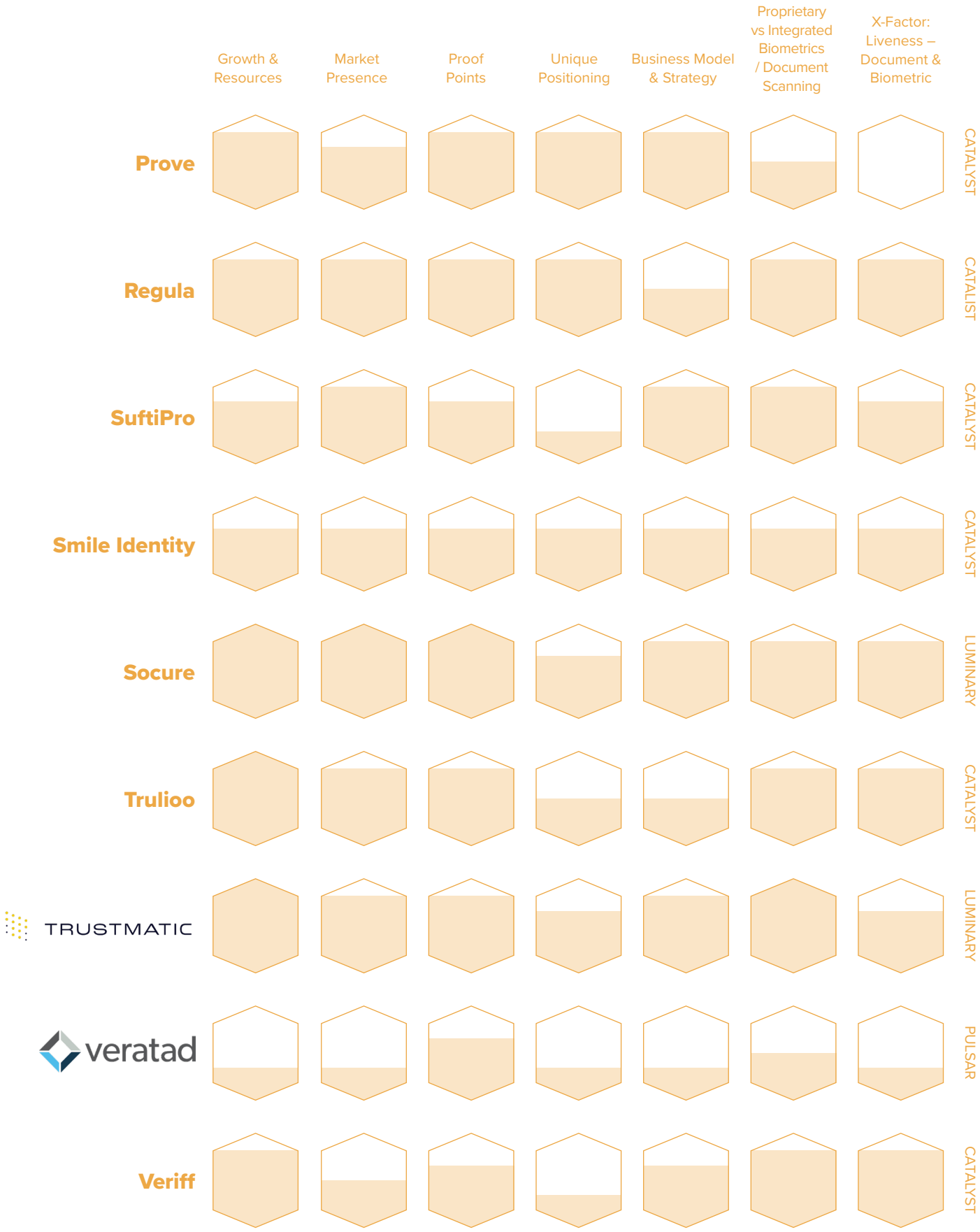
These companies remotely verify the identities of individuals by comparing live captured biometrics against government-issued identity credentials using mobile devices.

Prism XFactor: Liveness – Document & Biometric

Evaluations



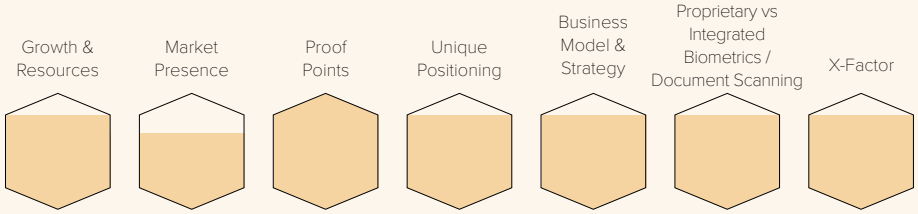


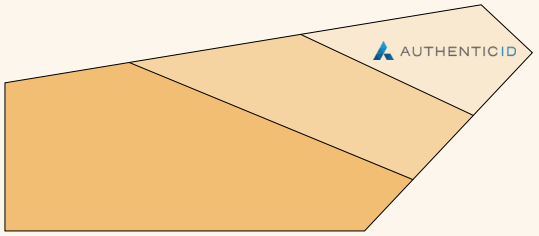


AuthenticID

authenticid.com

BEAM: **IDV** / CLASSIFICATION: **Luminary**





Founded in 2001, AuthenticID has built a portfolio of thousands of proprietary computer vision and machine learning algorithms that power its identity proofing and fraud detection technologies. The company's enterprise scale platform boasts an accuracy rate greater than 99 percent in detecting fraudulent documents, and its liveness detection solution is designed to analyze hundreds of data points, including trace evidence that would normally escape human detection.

Verification in the Age of AI-Enhanced Identity Fraud

In the identity industry we all know that fraud is an arms race, and recent innovations in artificial intelligence demand a proactive approach to IDV. AuthenticID has integrated machine learning into its ID document verification and biometric platform to ensure it meets the challenge of today's strongest identity threats. This is backed up by its signature watch-list solution, Fraud Shield, which utilizes biometric databases to blacklist prolific identity criminals. AI also enhances the user experience of the biometric enrollment process, with computer vision allowing for accurate document capture in poor conditions, meaning AuthenticID's high levels of accuracy only enhance its usability.

Accurate and Fair Identity Across Devices

AuthenticID is device agnostic, so users can verify and authenticate their identity on mobile, web, or desktop. Its AI tools ensure the biometric scanning and matching process limit bias, while also working to provide a seamless user experience. But the user experience focus doesn't stop there—the company's computer vision can collect users' biographical data and use it to auto-fill forms, paying its trusted identity forward while minimizing friction. And all of this is done with active user consent, ensuring compliance with increasingly stringent regulations, and putting a user's privacy and autonomy first. IDV Luminaries like AuthenticID demonstrate that biometric digital identity can only empower users if they are in control of their data from the first transaction.

Always Auditing to Stay Ahead of Bad Actors

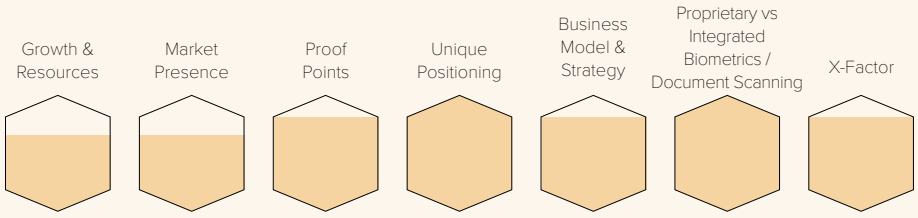
Assurance testing is integral to biometric digital identity, and AuthenticID makes regular security audits a pillar of its mission to deter fraud and enhance the business operations of its customers. While the company serves a wide range of industries including gaming, telecommunications, and healthcare, it prides itself on providing those customers with government- and financial-service-grade identity solutions, backed by up-to-date certifications. This proactive attitude toward testing echoes AuthenticID's use of AI technologies to keep up with our changing industry, and demonstrates its commitment to ethics and transparency. Given its long-term mission to "empower all mobile subscribers with the ability to confidently know that the people and organizations they interact with are legitimately who they claim to be," that strong foundation of compliance balanced with innovation makes all the difference.

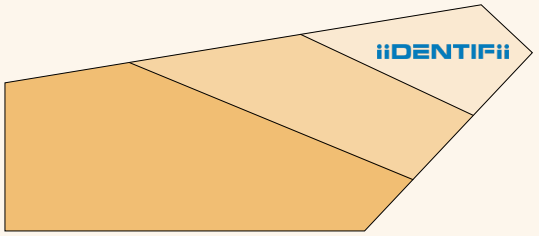
Contact AuthenticID: marketing@authenticid.com 1-844-656-1780

iiDENTIFii

iidentifii.com

BEAM: **IDV** / CLASSIFICATION: **Luminary**





iiDENTIFii offers a selfie-based onboarding platform that distinguishes itself through its use of 3D and 4D face scanning—its '4D Liveness' technology reflects a sequence of colored lights off a user's face to protect against advanced presentation attacks including deep fakes. An extra layer of verification in which the end user's identity information is matched against authoritative databases. Based in South Africa, iiDENTIFii was founded in 2018 and has become a proven key partner in multiple tier 1 African banks' efforts to implement enhanced Know Your Customer (KYC) processes to enhance resilience against identity fraud as part of an effort to get the continent off of a "grey list" maintained by the global anti-money laundering organization Financial Action Task Force (FATF). It has also raised millions of dollars in funding over the past year as VC and private equity investors have recognized its potential to target the broader Middle East and Africa market and beyond. This IDV Luminary stands out thanks to its relationship with Standard Bank, the largest bank on the African continent, with a presence in 20 African countries and seven international markets, through which it has built an enterprise scale solution that meets the highest KYC standards.

4D Biometrics for a Four-dimensional World

As face biometrics have emerged as the primary modality for mobile IDV transactions like eKYC and remote onboarding, they have become a vector of attack for fraudsters. iiDENTIFii's '4D' face biometrics technology significantly increases the amount of biometric data used to confirm a user's identity and liveness, offering natural resistance to the most common presentation attacks. Once the domain of high-cost biometric hardware scanners, iiDENTIFii's software-based approach makes it ideal for emerging markets in EMEA where identity verification is in high demand but boutique smartphones with specialized hardware are rare.

Anchored by a Source of Record

Further enhancing iiDENTIFii's product is its integration with government databases, adding an extra layer of verification and identity proofing. This integration is a gold star for iiDENTIFii and sets the firm as a role model for the industry. Government sources of record are foundational to the future of biometric digital identity—enabling the strongest level of identity proofing for high-risk transactions—and incorporating these databases directly into an IDV offering puts iiDENTIFii ahead of the curve. As the next phase of biometric digital identity emerges, moving toward self-sovereignty as defined in this report, government database integration will be crucial in the verification process.

Building an Identity-safe Africa

Thanks to its strong regional focus, iiDENTIFii has developed IDV technology best suited for its users' specific needs. From a mobile infrastructure standpoint, many areas in the company's jurisdiction face connectivity challenges, which in turn makes strong identity verification difficult, especially when calling back to a government source of record. iiDENTIFii addresses this challenge thanks to sophisticated redundancy, enabling its IDV technology to work even when networks fail. This level of thoughtful innovation is not only a differentiating factor in the company's home region, but is indicative of a larger advantage: in a market landscape where many firms try a one-size-fits-all approach, iiDENTIFii is successfully tackling unique challenges to provide next generation identity to those in need.

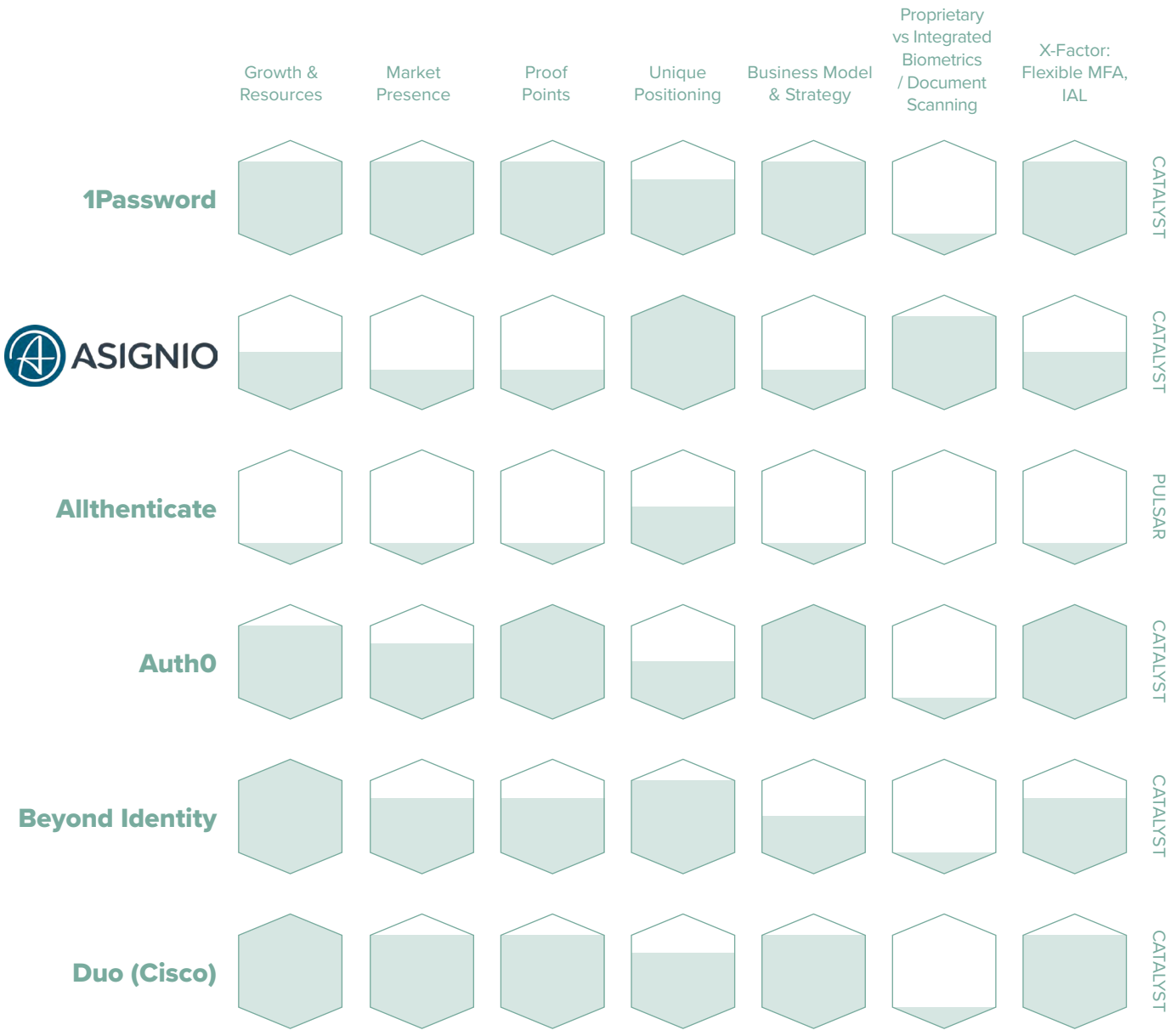
Contact iiDENTIFii: info@iidentifii.com +27 21 286 9104

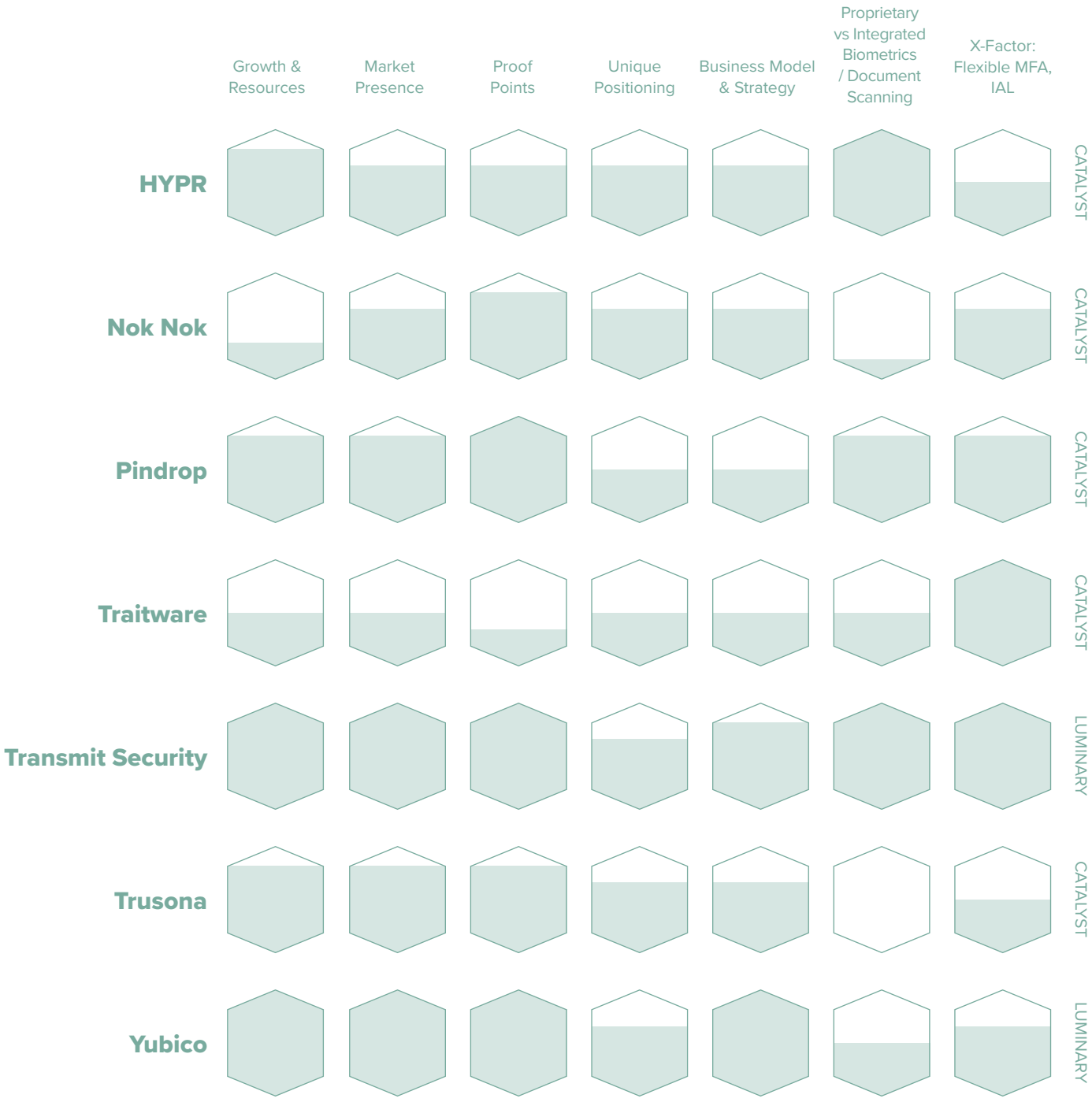
Authentication

Linking a digital identity to an individual via biometrics and/or a device.

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

Evaluations

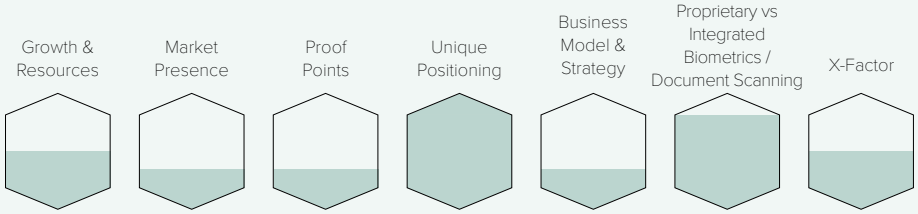


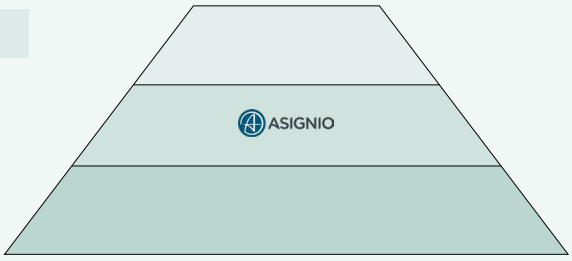


Asignio

asignio.com

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





Authentication Catalyst Asignio is pursuing a privacy-based, user-empowering mandate, as it provides customers with convenient multi-biometric security. But it's the novel nature of those biometrics that distinguishes it as an authentication solutions provider – Asignio leverages face biometrics and signature biometrics, captured simultaneously, in order to confirm a user's identity. By scanning a user's face while they trace a unique pattern on the touchscreen of a mobile device, Asignio leverages two biometric factors without adding friction, providing a natural form of liveness detection. With solutions for enterprise, government, financial services, healthcare, and emerging markets like education, the company is uniquely positioned in a competitive market.

While it's tempting to focus solely on Asignio's unique proprietary biometric technology, it stands out as an authentication solution thanks to its device-agnostic nature and the use cases it opens up. Integrations with e-signature providers enable biometric validation for document viewing and e-signing, while the same authentication process can be used to verify mobile payment senders and recipients. But most impressively, Asignio enables account recovery using biometrics, when many MFA and strong authentication solutions still rely on passwords, passcodes, or lengthy customer service interactions for that process. Asignio provides a fast and secure solution to what is otherwise a major fraud vector, supplanting passwords as the weakest link. It is this spirit of ingenuity and versatility that make Asignio notable among multi-factor authentication solutions.

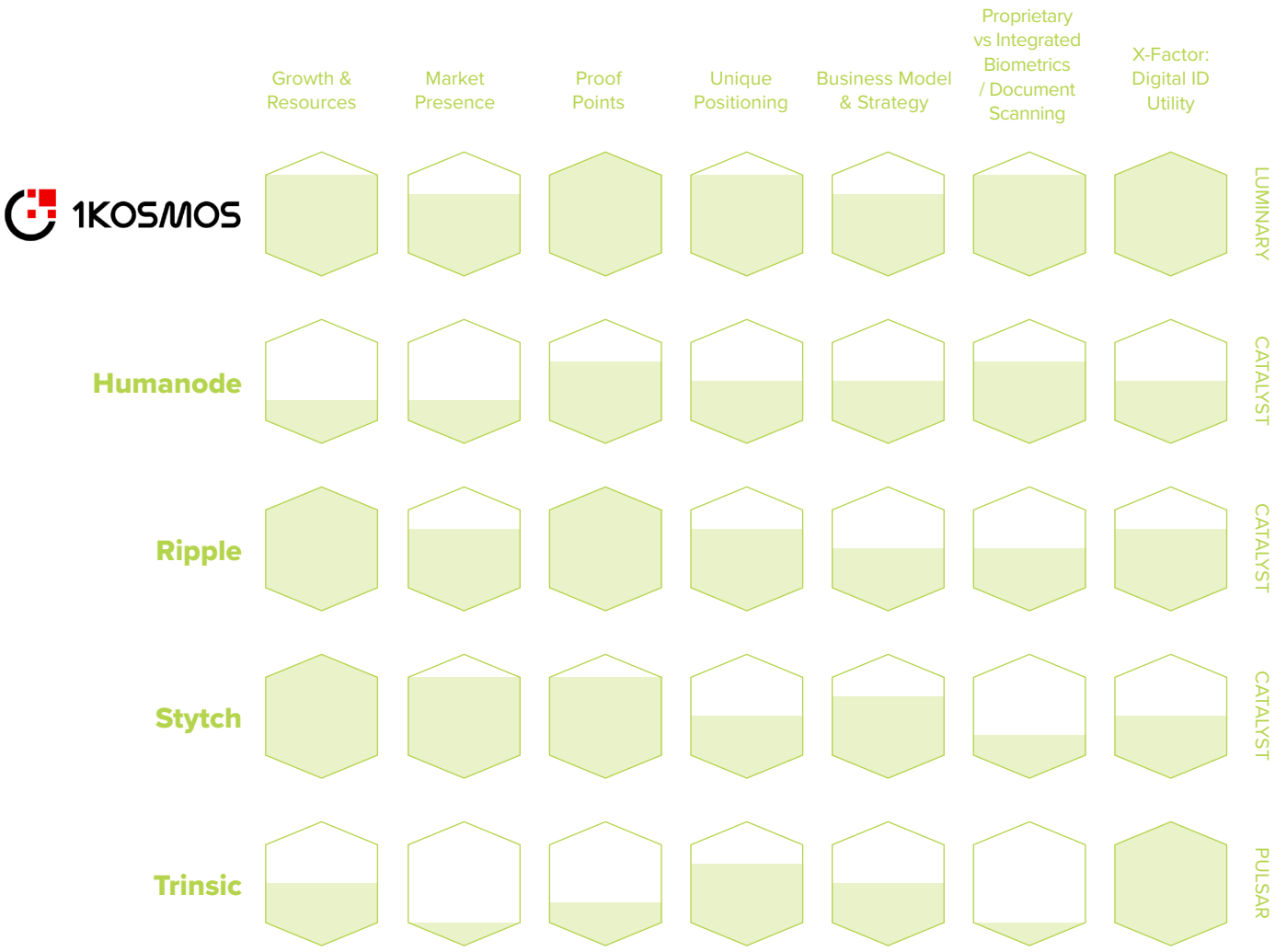
Contact Asignio: calvin.rutherford@asignio.com 1-360-840-3198

Distributed Identity

Distributed identity solutions and platforms that leverage blockchain technology to offer high-assurance decentralized digital ID and verifiable credentials.

Prism XFactor: Digital ID Utility

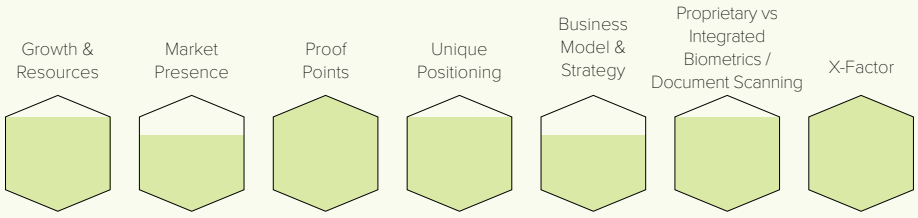
Evaluations

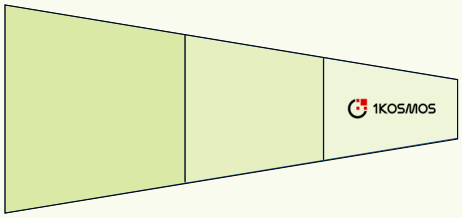


1Kosmos

1kosmos.com

BEAM: **Distributed Identity** / CLASSIFICATION: **Luminary**





1Kosmos is known for its BlockID solution, an identity verification and multifactor authentication platform that combines biometrics with a private blockchain to generate a verified digital identity for each end user. The solution registers a user's face biometrics using liveness detection and a selfie video, triangulates their biographic data from verified credentials, and binds that information to a reusable digital wallet. From there, the user can log into their accounts with a blink and a smile. The platform has attained certification to FIDO2, NIST 800-63-3, and iBeta's PAD Level 2 requirements, and offers a range of applications, including employee/ customer onboarding, non-phishable passwordless MFA into digital services, and even official ID for citizens through a Credential Service Provider managed service.

1Kosmos is leading the charge in the emerging Distributed Identity space because it takes biometric digital identity as seriously as the blockchain technology that positions it in this Prism Beam. With significant resources and proprietary face biometrics technology, this Distributed Identity Luminary is participating in the testing initiatives and standards programs to ensure it can deliver on the long-held promise of blockchain-based identity: reusable, strong identity that is device-agnostic with a wide breadth of application areas. As Distributed Identity matures in the coming years, our researchers expect 1Kosmos' currently novel methods to become the standard.

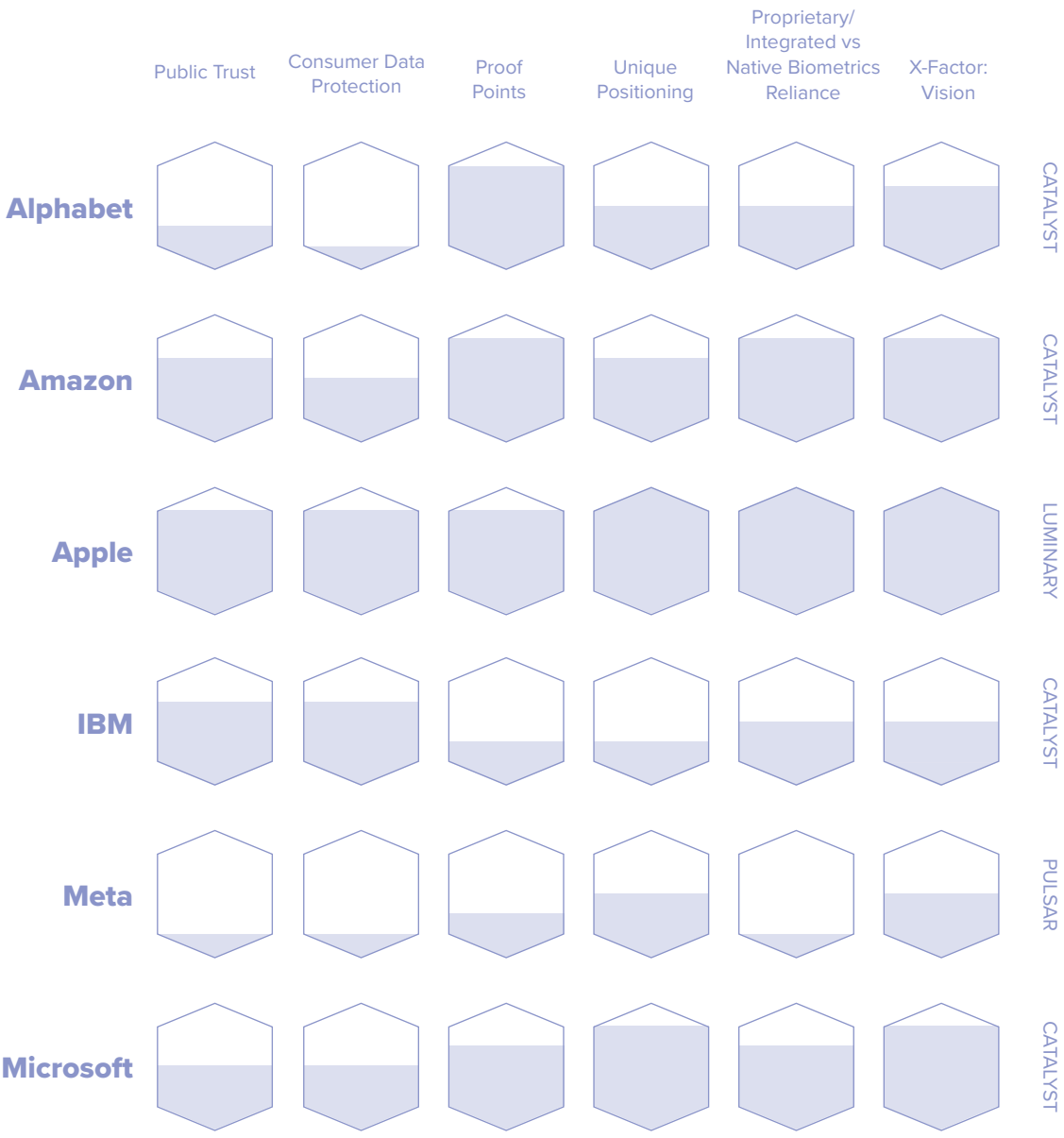
Contact 1Kosmos: Huzefa Olia, 1-833-850-5464

Big Tech

Identity is a key component of the next-generation Internet, where self-sovereign and privacy-by-design principles will drive innovation.

Prism XFactor: Vision

Evaluations



Showing Identity in a New Light

The future of biometric digital identity is bright. The vendors represented in this report all play an important role in a rapidly emerging identity ecosystem that reaches beyond the traditional borders of digital systems to incorporate true human identity. With biometrics at the core, digitized systems in financial services, healthcare, government, and travel & hospitality are prepared to enhance customer experiences, protect user data, and mitigate the ever-present threat of fraud. End users, meanwhile, will be empowered to assert their verified and authenticated identity across channels with ease, assured that they are in control of their most precious data.

As the market evolves, the Prism will shift to represent it, providing a guiding light forward into the next phases of biometric digital identity.

About the Authors

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. Tenacious strategic marketer with a prolific career hallmarked by success designing and executing ground-breaking strategies for technology innovators and leaders.

Maxine Most (@cmaxmost) is the founding Principal of Acuity Market Intelligence (www.acuity-mi.com), a strategic consultancy recognized as the definitive authority on global biometrics market development. Throughout her 30-year career, Ms. Most has evangelized emerging technology on five continents. Since 2001, she has focused on biometric and digital identity markets where she has earned a stellar reputation for innovative thought leadership and a proven ability to accurately anticipate biometric and digital identity market trends.

As an executive strategist, Most has provided expertise in emerging markets such as biometrics, authentication, and digital identity, e-commerce, interactive services, and 2D and 3D visualization and image processing. She has worked with startups, established technology market leaders, Global 1000's, 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, and presents 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.

Peter Counter

Peter Counter writes about technology and culture. As Editor in Chief of FindBiometrics and Mobile ID World he brings a multitude of technology writing experience, having covered industry news and written features on topics as diverse as dark fiber, call center solutions, satellite technologies, robotics, Augmented Reality, Internet of Things, telematics, IPTV, healthcare tech, and gaming. With a decade of biometrics and identity industry experience, Peter has been a four-time judge for the prestigious GSMA Global Mobile (GLOMO) Awards and is the host of the ID Talk Podcast.

Counter hosts the FindBiometrics Virtual Identity Summits – a series of full-day online events, presented quarterly, designed to educate and motivate vertical market decision makers on their path to stronger identity practices. With a strong focus on ethics and privacy, the Virtual Identity Summits spearhead FindBiometrics' mission of connecting digital identity leaders with their future strategic partners.

As the head of FindBiometrics' Research Team, Counter has provided guidance, strategy, and communications expertise to the world's leading digital identity and biometrics companies operating in financial services, government, healthcare, and travel vertical markets.

Alex Perala

Alex Perala is a writer and journalist covering biometrics, cybersecurity, and artificial intelligence. He is the author of FindBiometrics' daily ID Tech newsletter and weekly AI Update. He can be found on X at @alex_perala, and on Substack at @alexperala.

The Future is Prismatic...

Let Acuity Market Intelligence and FindBiometrics be your guiding light!

Contact info:

Maxine Most
Principal Researcher, Acuity Market Intelligence
cmaxmost@acuity-mi.com

Peter Counter
Ambassador & Editor in Chief, FindBiometrics
pcounter@findbiometrics.com

Lisa Sherman
Sales Executive, FindBiometrics
lisa@channelpronetwork.com

Dan Krippner
Sales Executive, FindBiometrics
dan@channelpronetwork.com

About FindBiometrics:

FindBiometrics is your leading industry resource for all information on biometric identification and identity verification systems and solutions. We have the latest daily news from the global biometrics and identity management business community, a comprehensive vendor list, informative articles, interviews with industry leaders, exclusive videos, links to biometric associations and a calendar for the most important and current industry events and conferences.

http://www.FindBiometrics.com

FindBiometrics is part of the ChannelPro Network, a division of EH Media LLC, a leading U.S. business-to-business media company and conference producer. http://www.ChannelProNetwork.com

---

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.