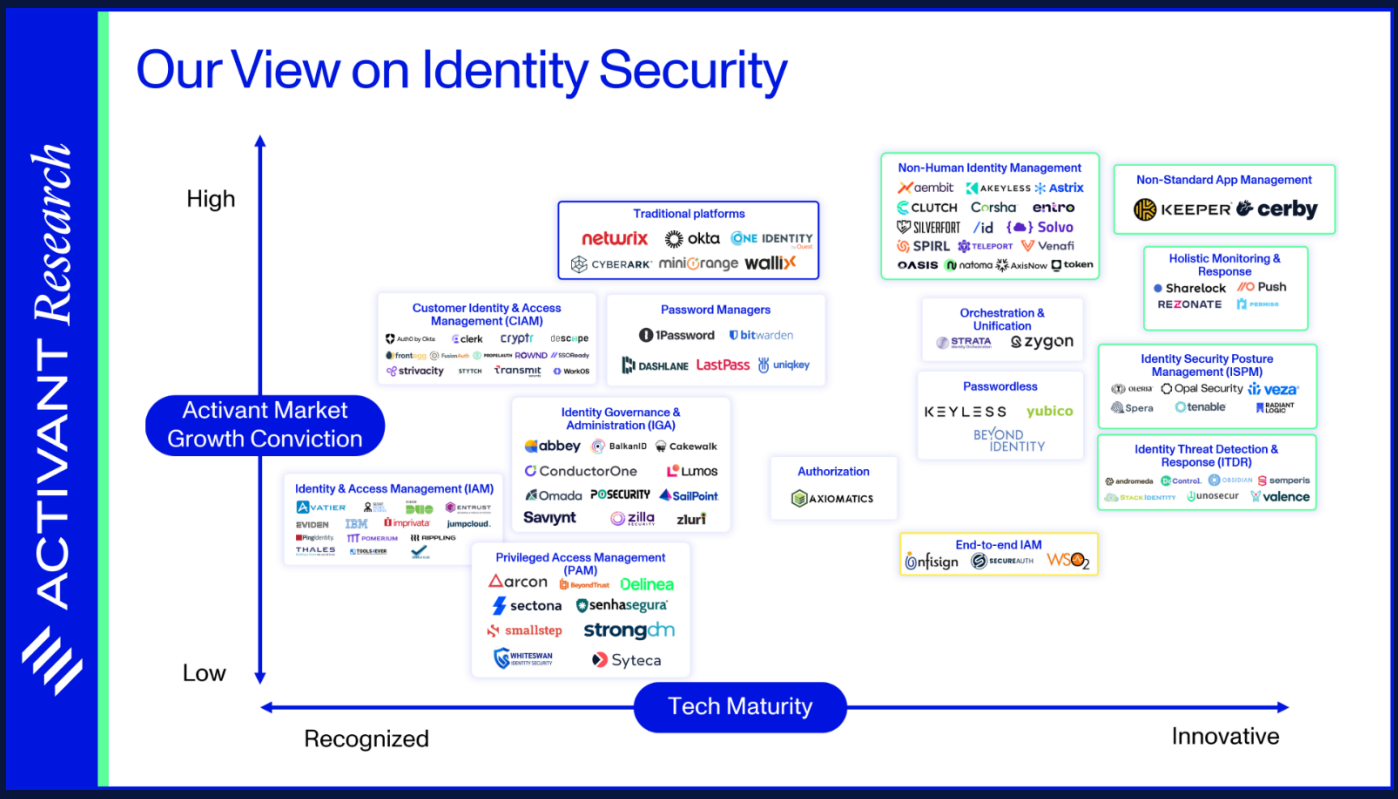
ACTIVANT RESEARCH

Taking Identity Security Forward

Locking down security's last mile



Jono Vickery, Cael Berg

Q1 2025

Introduction

Modern supply chains are incredibly complex. An iPhone, for example, is assembled across multiple continents, comprising over 100 components that are sourced from more than 200 suppliers in 43 different countries.[1,2] But with well-established standards and processes, it all just works. However, numerous challenges arise when transporting goods from local warehouses to the customer's doorstep - **the last mile**. The supply chain's last mile is often the most inefficient, unpredictable step and has the greatest impact on customer satisfaction. In cybersecurity, the same principles apply.

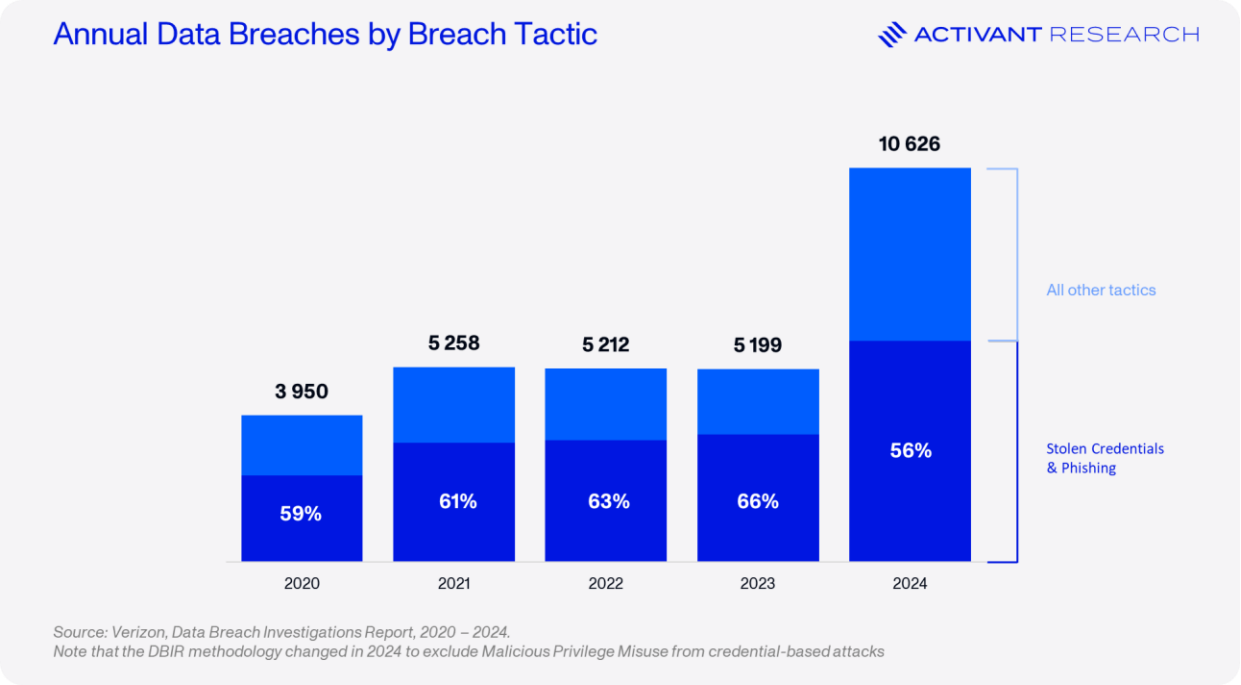
Cybersecurity is a $200 billion+ market, driven by substantial investments in firewalls, endpoint and cloud security. Despite these defences, enterprises are left grappling with one critical question: who should have access? That's Identity Security: it's **the last mile** of cybersecurity and, just like the last mile of a supply chain, it is fraught with challenges. In fact, **it is arguably the most fundamental weak point of modern cybersecurity.** Two-thirds of all data breaches involve a "human element" (*read: they leveraged identity*) and 94% of organisations have suffered an identity-related breach.[3,4] Hackers don't hack in, they log in. That may be a cliché in the identity security industry, but it highlights the need to fix security's last mile in order to solve the growing data breach problem.

[1] Thomasnet, Inside the iPhone, 2020

[2] Apple, Fiscal 2021 Supplier List, 2022

[3] Verizon, Data Breach Investigations Report, 2024

[4] CyberArk, Identity Security Threat Landscape, 2024



In this report, we look at how companies are currently securing the last mile, examine how outdated infrastructure, non-human identities and non-standard apps are leaving cracks for attackers to exploit, and consider the start-ups that are emerging to solve these problems.

The New Perimeter

Historically, enterprise security relied on a perimeter-based strategy, with firewalls acting as moats to protect internal networks. Trust was implicitly granted to any device within the perimeter, often identified by IP addresses. However, this model proved deeply flawed: once an attacker breached the network, they gained unrestricted access to critical systems and data. More importantly, new ways of working obsoleted perimeter-based security. Pandemic-induced work-from-home policies pushed people outside of the network, and the shift to the cloud pushed data outside of it.

As a result, companies are rapidly shifting to the zero-trust security model where no actor receives implicit trust. Without implicit trust, every single actor must be explicitly

authenticated and authorized to access any data or system. This shift makes identity one of the most foundational pieces of modern cybersecurity. **Identity is the new perimeter.**

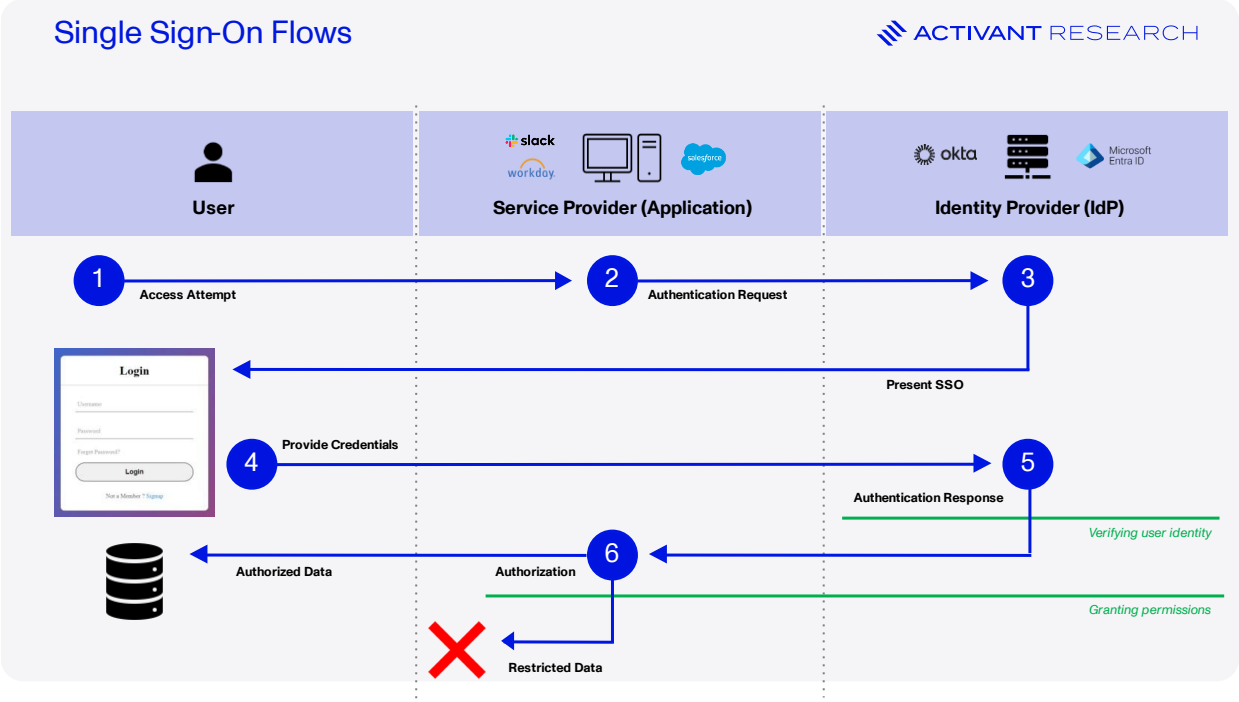
As we've established the critical importance of identity security in the modern enterprise, let's explore the infrastructure that enables the authentications and authorizations that zero-trust depends on.

Identity Infrastructure

Identity and Access Management (IAM) ensures that only the right people – or machines – have access to the right enterprise resources, for the right reasons.[5] At its core is a directory storing credentials like usernames and passwords, used to grant access (authentication) as well as dictate the level of access that the user has within the system (authorization).

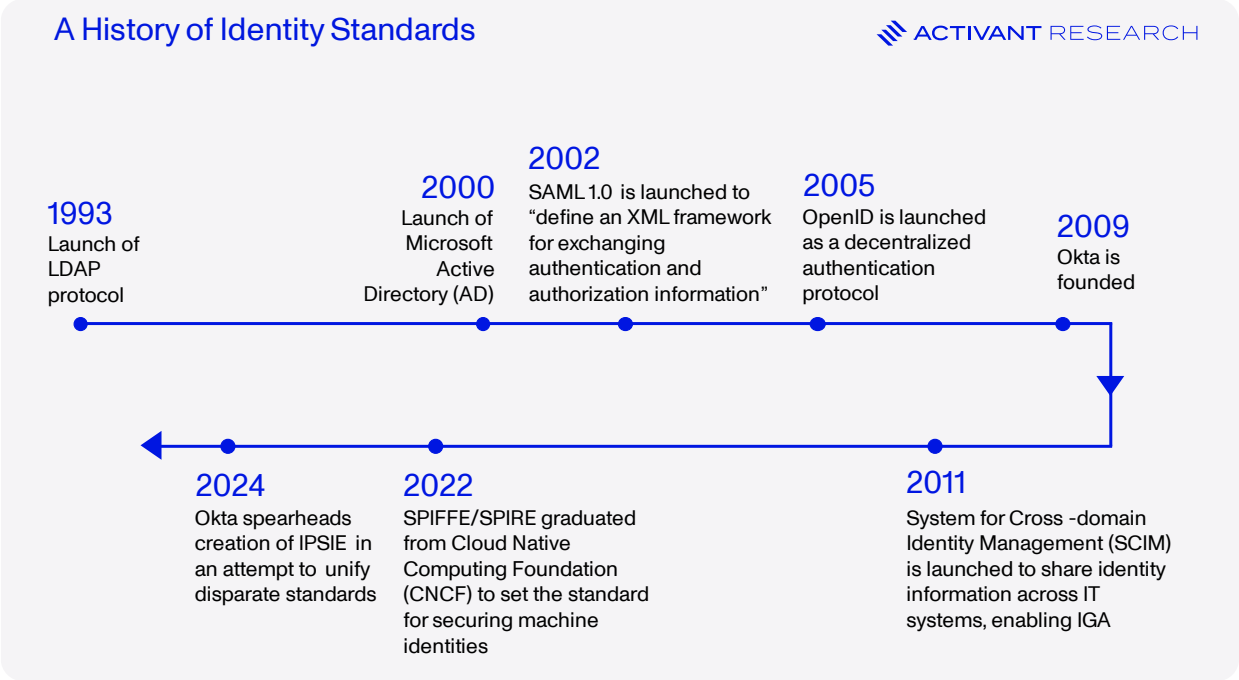
The sensitivity of data stored in directories drove the market towards centralized and specialized Identity Providers (IdPs). Microsoft dominated this market in the on-premises era, and Okta rose to prominence in the shift to the cloud. Centralized IdPs enable Single Sign-On (SSO), allowing users to log into hundreds of apps with a single credential. Finally, authentication processes make use of multi-factors authentication (MFA), such as checking a user is in possession of a registered device. See below for a technical breakdown of how SSO works today.

[5] Gartner, Identity and Access Management (IAM), 2024

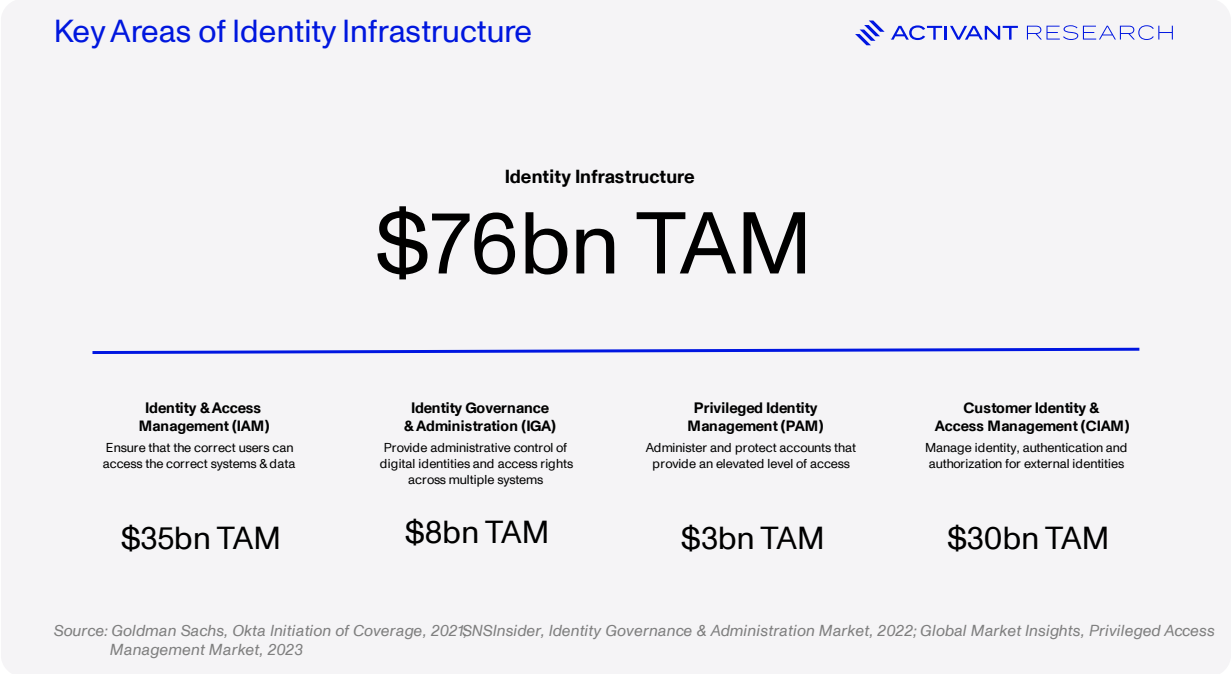


However, enterprises can use 10,000+ different applications, so making sure that these integrate effectively with a central IdP can be a software development nightmare.[6] The Lightweight Directory Access Protocol (LDAP) protocol addressed this issue as long ago as 1993 by introducing a vendor neutral standard for sharing directory information over the internet for authentication purposes. LDAP is still in use today, but has largely been replaced by standards like Security Assertion Markup Language (SAML) and OpenID, as well as mTLS and SPIFFE for non-human identities. It's critical to note that the market has repeatedly demonstrated an ability to collaborate and adopt the standards-based approach that underpins modern identity security, as demonstrated in the timeline below.

[6] MongoDB, 2023 Form-10K, 2024



The centralization of the IdP also renders centralized control to the enterprise IT team, giving it the ability to provision and deactivate users as well as manage their level of access: Identity Governance & Administration (IGA). A common identity security practice is to give all users the absolute minimum access that still allows them to get their job done (principle of least privilege). Unfortunately, some roles like IT admins require vast system and data access which poses a significant security risk. In these cases, Privileged Access Management (PAM) steps in to control, monitor and secure privileged accounts. Finally, Customer Identity and Access Management (CIAM), provides developers with the tools to integrate key IAM features into their products and to ensure that their customers have seamless sign-up and log-in processes with robust identity security infrastructure like SSO. Together, IAM, IGA, PAM and CIAM make up the four key elements of our Identity Infrastructure and a $76bn TAM, as detailed below.



Identity security's infrastructure has been built out over the past three decades, with more than 80% of enterprises having adopted IAM by 2021. Yet, we continue to see an increase in the number of breaches each year, the vast majority of which still occur through identity. Something must be missing.

Infrastructure is Not Security

In 2024, 165 Snowflake accounts were breached, including 560 million records of customer data stolen from Ticketmaster – one of the largest data breaches of the year.[7] Attackers orchestrated the breach by stealing Snowflake user credentials using malware and then simply logging in to accounts that had not activated MFA. Notably, some of the stolen credentials were accessed years ago and had not been rotated.[8] This breach points to the heart of the issue – **the presence of identity infrastructure does not in and of itself make an enterprise secure**. Yes, we've built technology to require usernames and passwords everywhere we go, but the attackers got hold of those, and the MFA codes too,

[7] Techcrunch, The biggest data breaches in 2024: 1 billion stolen records and rising, 2024

[8] Mandiant, UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion, 2024

if customers had even enabled MFA. The list of weaknesses in traditional identity security are plain:

1. **User credentials can be stolen:** Credential theft is rampant, fueled by phishing tools available on platforms like GitHub and malware subscriptions costing as little as $100/mo.[9] Stolen credentials often end up on the dark web, adding to a pool of 6.7 billion compromised accounts attackers exploit using credential stuffing programs.[10]
2. **MFA is not used and not impenetrable:** Only 28% of Microsoft users have activated MFA.[11] While MFA takes a huge step towards preventing account takeovers (99.9%, according to Microsoft[12]), MFA codes are susceptible to SIM-swapping, social engineering and phishing.
3. **Session cookies can be highjacked:** Once a user is logged in legitimately, their browser holds a small piece of data to remember information from the session. This is why you may be able to close the site and then reopen it without having to log in again. However, if attackers capture this cookie they're able to access enterprise resources without credentials.

What's more troubling is that these are all technically solved problems. We can set strong, unique passwords and rotate them frequently. We can enforce MFA on all accounts, shut-down SMS-based MFA and implement strong MFA/passwordless authentication like passkeys or YubiKeys. We can set session cookies to expire after short periods like 30 minutes. The average data breach costs $4mn+, so why have we not implemented best-in-class security?[13]

1. **Cultural Inertia:** The reality is that most management teams are not focused on security until ***after*** a breach takes place. Many of these best-in-class security strategies are difficult to implement (imagine shipping physical YubiKeys to 200,000 employee at 1,500 global Hyatt locations) and can cause serious business disruptions. Further, users are likely to push back on many security innovations when they create

[9] Malpedia, RedLine Stealer, 2024

[10] Dark Reading, 24+ Billion Credentials Circulating on the Dark Web in 2022 — So Far, 2022

[11] IT Brew, Lack of MFA adoption from Microsoft users raises concerns over security, 2023

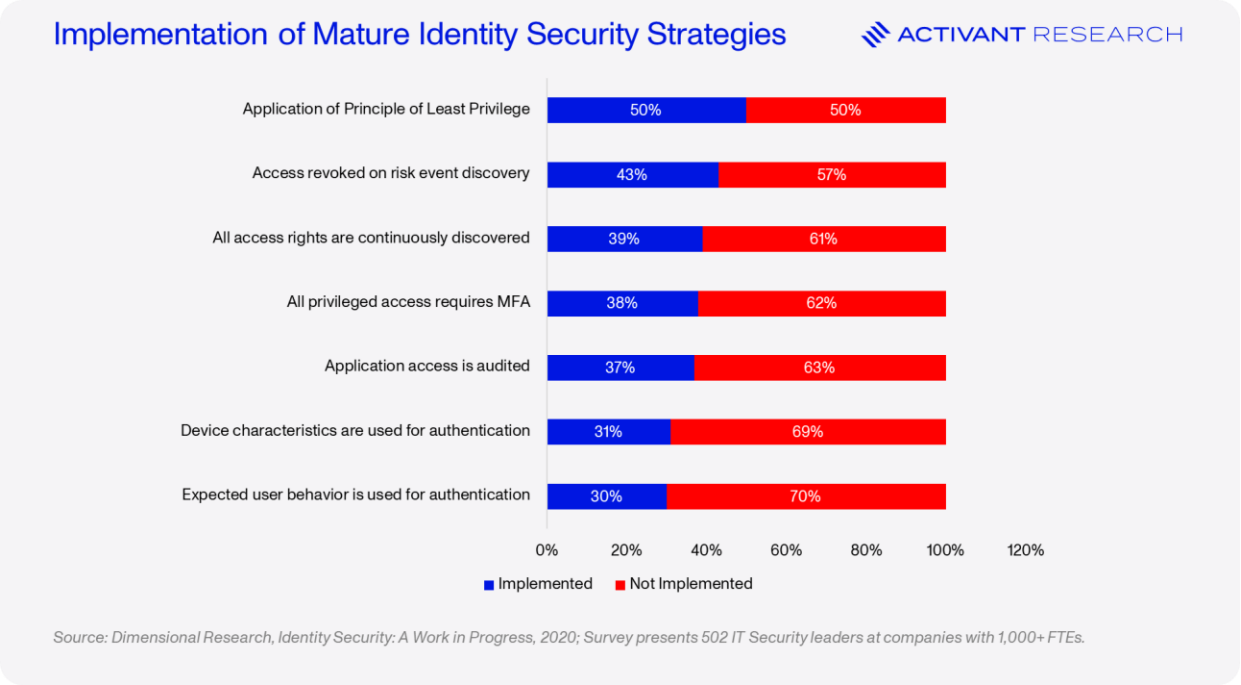
[12] Microsoft, One simple action you can take to prevent 99.9 percent of attacks on your accounts, 2019

[13] IBM, Turning data into value, 2022. Statistics are from a survey of 3,000 Chief Data Officers across 30+ countries

friction – inconveniences, such as carrying around a hardware key or being unable to log in without your phone, increase rather than reduce friction.

2. **Fragmented Identity Infrastructure:** Identity infrastructure is often fragmented due to mergers, divisional silos, or piecemeal technology purchases. In fact, 94% of organizations rely on ten or more identity security vendors.[14] This patchwork approach complicates visibility into critical metrics, such as MFA adoption rates, and makes deploying a unified identity security strategy nearly impossible.

As we can see below, these issues are widespread and **identity security maturity is extremely low across the board**.[15]



[14] CyberArk, Identity Security Threat Landscape, 2024

[15] Dimensional Research, Identity Security: A Work in Progress, 2020; Survey presents 502 IT Security leaders at companies with 1,000+ FTEs.

We don't need to build more infrastructure. More MFA methods and communication standards will not solve these challenges. We need security: automating the implementation of best practices, detecting and responding to issues, and blocking threats.

> When we were building our last start-up, we thought we had everything covered—an IdP, SSO, and all the tools you'd expect for identity security. But the reality was, we had no visibility or control over who had access to what. When we tried to solve this, every vendor we approached asked us to list our apps and SaaS tools—but that was precisely the problem: we didn't know. Existing identity tools weren't designed to tackle this issue. Modern solutions need to start with visibility, then layer on access and lifecycle management.
>
> **Ritish Reddy, Co-founder & CEO, Zluri**

Adding the Security Layer to the Identity Stack

Adding security to the identity stack is about leveraging existing infrastructure and supplementing it with tools that can automate and streamline the application of best practices, detect threats, and provide enterprises with full visibility into their identity infrastructure to flag and autonomously fix issues.

Identity Security Posture Management (ISPM) is an emerging technology where vendors like Opal Security and Oleria can scan data from enterprise systems to flag identity security risks such as access privileges that don't expire or haven't been used, helping to drive the principle of least privilege. With this information, security teams are armed to action their highest priority remediations and Opal Security can remediate these issues in one click with their bi-directional integrations.

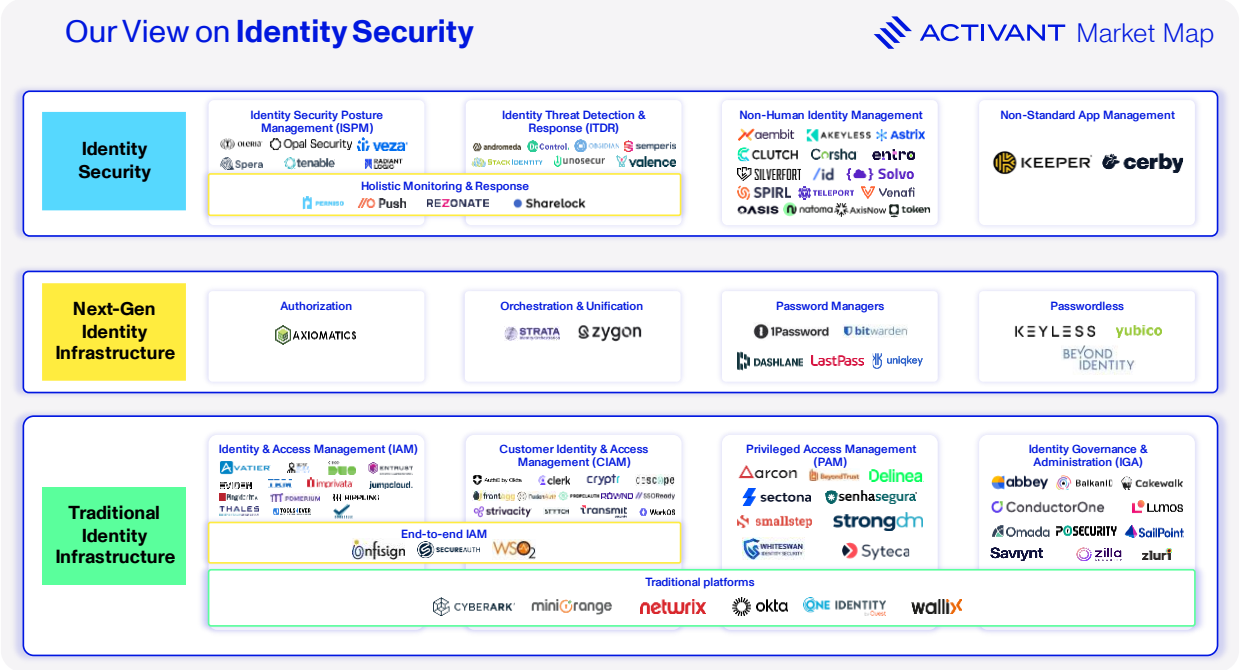
Once you've applied ISPM to harden your identity security and remove obvious attack vectors, Identity Threat Detection and Response (ITDR) platforms like Valence and Andromeda step in to monitor access data, flag risky identities and integrate with the SIEM to enable security teams to respond to events as they occur. Valence can action those remediations autonomously and Andromeda pushes threat data back into Identity Governance, leveraging AI to provide automated just-in-time access. Companies like

Push Security and Permiso are bringing ISPM and ITDR together into one cohesive platform to provide holistic monitoring and response.

For companies that suffer from fragmented identity infrastructure, Zygon and Strata both offer the ability to unify this infrastructure and create a centralized control plane. Zygon can automate workflows such as provisioning and access requests, while Strata looks to replace legacy IdPs one by one.

Also of critical importance are platforms that are working to innovate on the identity infrastructure layer. Beyond Identity provides an authentication method that removes the need for passwords altogether, cryptographically binding a user's identity to their device so that attackers can't rely on stolen passwords or session cookies.

With these new innovations, it's possible to implement multi-factor authentication methods that are passwordless and phishing resistant. It's possible to continuously monitor enterprise systems for potential identity security gaps and implement best practices, from the principle of least privilege to proper identity lifecycle management. It's also possible to monitor identity risks in real-time and universally log out high-risk identities. **Critically, it's not just possible – these solutions are autonomous, always-on and frictionless, overcoming cultural inertia.** Our Activant market map details this new identity architecture, with security being built on top of both existing and next-generation infrastructure.



IAM's dominant vendors, Okta and Microsoft, will surely fight for share in this new security layer. Okta is rapidly adding new features to its offering such as Extended Device SSO, automated threat remediation in its ISPM offering, and authentication for Gen AI.

Okta, for example, is highly advantaged when adding security on top of existing infrastructure because it is the provider for much of this infrastructure. The company already blocks three billion attacks every month and serves as the system of record for identity data at ~19,000 organizations.[16] The data advantages that it can accumulate are immense and the switching costs to an IdP are high.

However, many of Okta's new products are only set for 2025, which might make some think of them as vaporware. Critically, both Okta and Microsoft have suffered severe security weaknesses recently. Okta was breached in 2022 and again in 2023, and Microsoft's internal security was criticized by the US Government. Buyers will think twice about purchasing security tools from vendors who mismanage their own security and,

[16] Okta, Oktane Keynote: The future of Identity Security, 2024

while Microsoft and Okta hold massive advantages in the identity market, they may have dropped the ball.

If there is any doubt about using Okta or Microsoft as your identity infrastructure vendor, there are companies like Zluri looking to step in. Zluri provides next-gen IGA, functioning at the infrastructure layer to overcome the limitations of SCIM, with system-wide observability built in to also provide features that would otherwise be found in an ISPM or ITDR tool.

Building new security tools on top of existing identity infrastructure is an extremely exciting trend, but there are two major limitations to the tools we've discussed this far: 1) they are largely focused on securing *human* identities, and 2) these standards-based approaches fail when apps don't support SAML/OpenID. **Two key themes shaping the future of identity security are machine identities and non-standards-based approaches.**

The Rise of the Machines

Machine identities (also non-human identities or NHIs) refer to the digital services that tie our applications together and automate digital processes. They could be service accounts on the cloud, RPA bots, application APIs, IoT devices, and soon, AI Agents. With the rise of the cloud, microservices architectures and workflow automation, machine identities are growing rapidly and now outnumber human identities by a factor of 45x.[17] A 10,000-person enterprise needs to secure close to half a million machine identities and, once we bring AI agents into the enterprise, this issue may explode exponentially.

Attacks on machine identities, such as those at GitHub and Okta, underscore a critical issue: current identity infrastructures are designed primarily for human users. Machine identities operate fundamentally differently, posing unique challenges and exposing significant security threats.

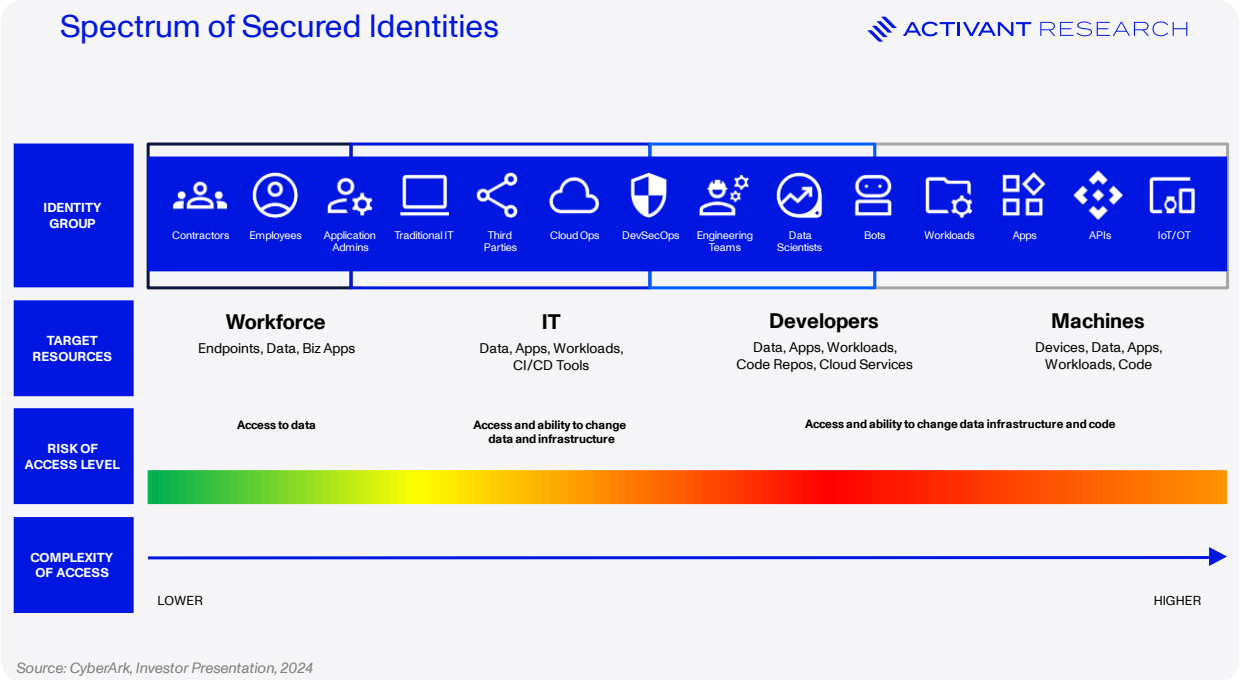
1. **Inability to respond to MFA prompts:** We can't apply existing human-centric MFA mechanisms to machines, leaving them doing single factor authentication.

[17] CyberArk, Key Considerations for Securing Different Non-Human Identities, 2022

2. **Elevated privileges:** Machine identities often have elevated privileges to get their job done, which makes them an attractive attack point, yet many machine identities have ***excessive*** permissions. For example, 23% of apps connected to Google Workspace have wide access permissions to sensitive data.[18]
3. **Lack of oversight:** There is a dearth of proper lifecycle management, review and auditing for machine identities, which is why only 2% of granted permissions are actually used.[19]
4. **Unpredictable action patterns:** The use of human identities can be subjected to anomaly detection because their usage patterns are highly predictable and access requests from unrecognized locations can be flagged. However, machine identities may work on an ad-hoc basis and their physical location could be any number of hundreds of global datacenters.
5. **Use of static passwords:** Like an API key hard-coded in a script, these can be extremely hard to rotate frequently. Cloudflare had its Atlassian Script Runner system breached due to hard-coded credentials that were exposed in an Okta breach.
6. **Difficult to create visibility:** These machine identities can be spread across different cloud providers and systems, which may not be interoperable, making it extremely difficult to create a full account of all the machine identities that an enterprise has granted access to and what actions they are taking.

[18] Astrix, Part 1: Non-human identity security – The complete technical guide, 2024

[19] Sysdig, Sysdig 2024 Cloud-Native Security and Usage Report, 2024



Source: CyberArk, Investor Presentation, 2024

As we can see above, securing machine identities is the most complex and riskiest area of identity. Identity infrastructure is making strides to address these issues, notably through the mTLS standard and SPIFFE/SPIRE (which leverage mTLS). SPIFFEE/SPIRE enable developers to define identity for machine workloads, how these workloads will obtain their cryptographically verifiable identity certificates, and how authentication takes place.

From a technical perspective, implementing SPIFFE/SPIRE is extremely challenging and implementers have faced issues such as reliability, scaling and observability – how do you keep track of digital certificates and their corresponding keys for hundreds of thousands of machine identities?[20] What's worse, SPIFFE doesn't answer key security questions like, "How many machine identities do we have right now and are they all being used?" It's just another example of the market building complex infrastructure for authentication but leaving real security as an afterthought.

That's why start-ups like SPIRL are abstracting away the complexity of SPIFFE and enabling customers to implement it with a few lines of code in the command line. Astrix,

[20] Uber, Our Journey Adopting SPIFFE/SPIRE at Scale, 2023

Entro and Oasis Security can scan your systems to discover machine identities, create and manage policies like offboarding, and assess risks. Aembit powers secretless identity - a just-in-time (JIT), short-lived credential that saves developers from having to store secrets at all. Teleport addresses the challenge of securing non-human identities by providing cryptographic, JIT credentials to all applications. Teleport's platform unifies human and machine identities across all infrastructure providers, removing passwords and secrets from the enterprise and providing a single pane of glass for identity management across the organization.

> Traditional identity tools were built for IT teams, where 95% of vendors focus. But engineering teams have been largely overlooked in cybersecurity. Everything in their world is automated and managed as code, rendering traditional tools incompatible. Critically, engineering workflows don't differentiate between human and non-human identities. Additionally, traditional IT-centric approaches to access control have historically been based on credentials. This makes them vulnerable to identity attacks that are impossible to defend against at scale, where cryptographic approach to identity is required, and the chain of trust reigns supreme.
>
> Modern identity security must be reimagined to address these unique demands.
>
> **Ev Kontsevoy, Co-founder & CEO, Teleport**

A Standard*less* Future?

The identity industry is heavily standards-based, but not every app is built to comply with SAML/OpenID, so these apps are forced outside of the identity perimeter. This can happen in the case of legacy apps (which could cost as much as $150,000 each to rewrite), modern apps which hold SSO behind expensive upgrades, or consumer-focused apps that simply aren't focused on building enterprise security like Instagram (where enterprise accounts could have thousands of users at consumer-facing brands such as L'Oréal).[21] All

[21] Forbes, Modernizing Application Identity At Scale, 2023

in all, **50%+ of enterprise apps are non-standard** – they don't comply with SAML/OpenID.[22]

This poses a major security risk – 52% of companies have experienced a cyber incident due to their inability to secure non-standard apps.[23] These apps cannot be secured with SSO, can't integrate with ITDR/ISPM services, and can't be subjected to powerful security features like universal logout and lifecycle management. Many employees or contractors may be left with access privileges to these apps long after they've left the company.

Cerby is solving the non-standard apps problem by building an identity mesh. Here, the company connects to existing IAM providers like Okta and Microsoft so that customers can continue to use their existing SSO accounts and then connects to non-standard apps through a combination of integrations and Robotic Process Automation (RPA). Through this mesh, Cerby extends SSO & MFA to apps that don't support it natively, lets IT admins do employee lifecycle management on 100% of their apps, and allows enterprises to manage multiple logins for single accounts such as social media accounts. Keeper's password manager also integrates with IdPs to enable customers to get 100% SSO coverage.

> Modern identity solutions simplify adopting Zero Trust principles, particularly with continuous authentication integrated into daily workflows. However, the Last Mile remains vulnerable, with attackers exploiting reduced visibility and control. Cerby bridges this gap, delivering consistent identity control and visibility across disconnected apps, identities, and workflows.
>
> **Belsasar Lepe, Co-founder & CEO, Cerby**

Today, Cerby is doing a small but critical job to extend Identity Infrastructure to cover 100% of enterprise apps. But they're not just an identity mesh, they are also building powerful security features into their own platform like automating employee offboarding and password rotation. In the long-term, it's an open question whether we will abolish all non-standard apps, or **if technological innovations like those at Cerby will allow us to achieve**

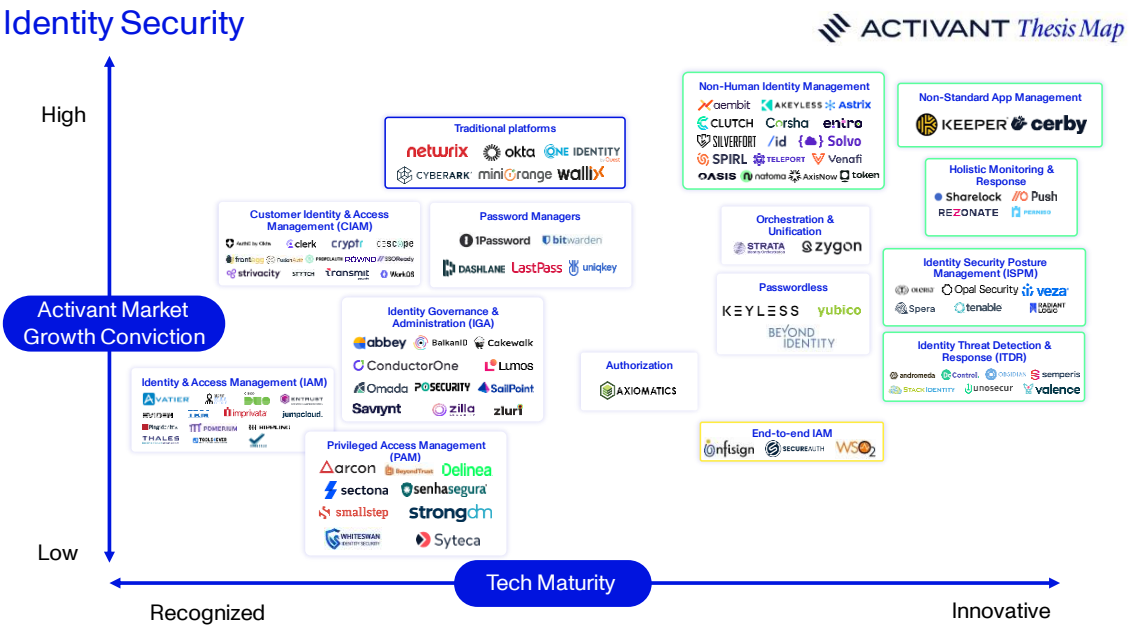
[22] Okta, Businesses at Work, 2024; Activant Analysis

[23] Ponemon, The Hidden Cybersecurity Threat in Organizations: Nonstandard Applications, 2023 (Sponsored by Cerby)

identity security without any worry for how the underlying apps we're securing are written.

On that note, innovation in CIAM from companies like Frontegg and Stytch are making it ever easier to ensure that new apps comply with key identity standards – it takes just five lines of code to enable SSO for your app with Frontegg. What these companies have done for the consumer sector, WorkOS is doing for B2B apps and SSOready promises to add SAML SSO to any app with just two API calls.

The Activant View



We're excited about the innovative segments of this new security layer such as non-standard app management, ISPM & ITDR, non-human identity management, and identity orchestration. Companies like Opal Security, Oleria, Entro, Andromeda, Zygon, Strata, Beyond Identity, Astrix Security, Oasis Security, Zluri and Cerby are driving this innovation and will be the major beneficiaries of the next wave of growth in the identity industry.

Conclusion

Identity is cybersecurity's most fundamental flaw if your enterprise is still running on outdated and fragmented infrastructure technologies. Cultural inertia accounts for why most enterprises are stuck without proper identity security practices. The solution could be investments in training and "change management" or it could lie in technology that makes identity security automated, always-on and frictionless.

It's time for enterprises to level up their identity security practices, so that we can stop reading about breaches in the news every morning – the tools to do so have arrived.

If you're building in this space, please get in touch.

Disclaimer: The information contained herein is provided for informational purposes only and should not be construed as investment advice. The opinions, views, forecasts, performance, estimates, etc. expressed herein are subject to change without notice. Certain statements contained herein reflect the subjective views and opinions of Activant. Past performance is not indicative of future results. No representation is made that any investment will or is likely to achieve its objectives. All investments involve risk and may result in loss. This newsletter does not constitute an offer to sell or a solicitation of an offer to buy any security. Activant does not provide tax or legal advice and you are encouraged to seek the advice of a tax or legal professional regarding your individual circumstances.
This content may not under any circumstances be relied upon when making a decision to invest in any fund or investment, including those managed by Activant. Certain information contained in here has been obtained from third-party sources, including from portfolio companies of funds managed by Activant. While taken from sources believed to be reliable, Activant has not independently verified such information and makes no representations about the current or enduring accuracy of the information or its appropriateness for a given situation.

Activant does not solicit or make its services available to the public. The content provided herein may include information regarding past and/or present portfolio companies or investments managed by Activant, its affiliates and/or personnel. References to specific companies are for illustrative purposes only and do not necessarily reflect Activant investments. It should not be assumed that investments made in the future will have similar characteristics. Please see "full list of investments" at https://activantcapital.com/companies/ for a full list of investments. Any portfolio companies discussed herein should not be assumed to have been profitable. Certain information herein constitutes "forward-looking statements." All forward-looking statements represent only the intent and belief of Activant as of the date such statements were made. None of Activant or any of its affiliates (i) assumes any responsibility for the accuracy and completeness of any forward-looking statements or (ii) undertakes any obligation to disseminate any updates or revisions to any forward-looking statement contained herein to reflect any change in their expectation with regard thereto or any change in events, conditions or circumstances on which any such statement is based. Due to various risks and uncertainties, actual events or results may differ materially from those reflected or contemplated in such forward-looking statements.