Delinea

Identity Security:

Why the future belongs to the platform

The identity attack surface is too broad to handle in silos

An important trend is underway in the modern enterprise. IT operations and security teams are converging.

IT manages access. Security monitors risk. Both teams are responsible for uptime, performance, and resilience. They need to coordinate constantly. When something breaks — whether from misconfigurations, outages, or attacks — both get pulled in.

Business leaders and regulators don't care whose fault it is. They want answers. Auditors ask about controls, not teams.

Security can't answer access review or assessment questions alone. IT can't defend against privilege escalation or data exposure without security policies and oversight.

Today, in an era of speed, complexity, and constant threats, IT operations and security teams have more in common than ever before and need to act as a unit, with shared goals.

That's why they need a shared platform.

Identity is the point of convergence

The only consistent control point for both IT and security is identity. Both functions depend on contextual information about identities to make informed decisions to reduce risk.

Context drives risk-based access to every resource, making the old 'privileged vs. non-privileged' distinction obsolete. Rather, every access across all identities (including fast-moving, ephemeral AI) is inherently privileged. What matters is who or what needs access, where is the access happening, where the assets are, and what the context is.

The stakes for identity security are high. In fact, the cost of identity-related attacks is higher than any other type of cyber-attack[1]. That means more eyes on those responsible for aligning everyone involved in identity management and security workflows – the CISO, CIO, and a growing cadre of identity security leaders.

Constantly changing context means IT and security teams need to work together and rely on accurate, shared data to safeguard identities in an agile fashion.

An identity security platform provides continuous access evaluation, including a dynamic privilege score that adjusts as risk changes.

[1] https://www.helpnetsecurity.com/2024/11/06/identity-related-data-breaches-cost/

Waste is the common enemy of IT and security

In an uncertain economic environment, every initiative and investment must fight for mindshare as well as budget and go to committees of multiple stakeholders for approval.

Unfortunately, most organizations have already spent lots of money on identity solutions, which has led to identity tool sprawl – dozens of systems, each responsible for addressing one aspect of the identity attack surface. For example, they may have:

- Identity and Access Management
- Privileged Access Management
- Identity Governance and Administration
- Single-Sign-On
- Multi-factor authorization
- Cloud identity services like AWS, Google Cloud, and Azure
- Identity providers like Okta and Ping
- Threat intelligence
- Analysis and notification systems

What is the cost of overlapping functionality and tool sprawl

	IAM	PAM	IGA/GRC	MFA	IdP	ITDR
CAPABILITY / FUNCTION						
Authentication & Authorization	✕	✓	✓	✕	✕	
Centralized Identity Directory	✕		✕	✕	✕	
Role-Based Access Control (RBAC)	✕	✕	✕	✕	✕	
Lifecycle Management (Joiner/Mover/Leaver)	✕	✓	✕		✕	
Policy & Workflow Orchestration	✕	✕	✕		✓	
Access Reviews & Certifications	✓	✓	✕		✓	
Session Recording & Monitoring		✕				✕
Password Vaulting / Credential Management	✓	✕			✓	
Federated Identity / SSO Across Apps	✕	✕	✕	✕	✕	
Multi-Factor Enforcement		✓		✕	✕	
Cloud Access Governance	✓	✓	✕		✕	✕
Anomaly Detection & Threat Correlation		✕	✓	✓	✓	✕
Real-Time Alerting & Notifications		✓	✓		✓	✕
Integration with SIEM / SOAR / XDR		✕	✕	✓	✕	✕

✕ Core capability

✓ Partial or commonly included via integration

Each tool requires individual subject matter experts to set up and manage, and infrastructure to maintain. Often, the functionality of these tools overlaps, yet they don't talk to one another, which means paying more than you need for licensing fees, while also creating more integration headaches and manual work for your team.

This situation has worsened over time because identities are scattered across hybrid and multi-cloud environments, created and managed across different departments. Beyond traditional IT admins, identities also include the general business workforce, developers, and non-human, machine identities that operate with elevated privileges. For each of these identity types, regular workflows span authentication, identity verification, access provisioning and reviews, privilege elevation, detection, and response.

The result is wasted budget and effort. Technology licenses, maintenance, integration, infrastructure, and training costs skyrocket. Worse, gaps and delays open the door for intruders. Indicators of compromise take time to unravel, and time-to-remediation is longer than it should be.

An identity security platform closes the gaps and improves operational efficiency for administration, integration, and remediation.

Privileged identities operating in your environment

In the modern enterprise, there are four identity types with privileged access that represent cybersecurity risk.

IT admin identities

IT admin identities, which include:

- IT ops teams, responsible for networks and infrastructure, such as servers and databases, a mix of Windows and Linux, in on-prem, private, and public cloud environments. They monitor systems, address technical issues, and update software.
- Help desk administrators, who manage support tickets from users and customers, and resolve support tickets.
- Cloud administrators, including the "Ops" side of "DevOps," who control the creation of virtual machines and containers and optimize performance.
- Security teams who analyze threats, investigate root causes, and respond to incidents.

Securing IT admin access is what most people think of when they think of Privileged Access Management, or PAM. But identity security is much more than that. It also includes:

Workforce identities

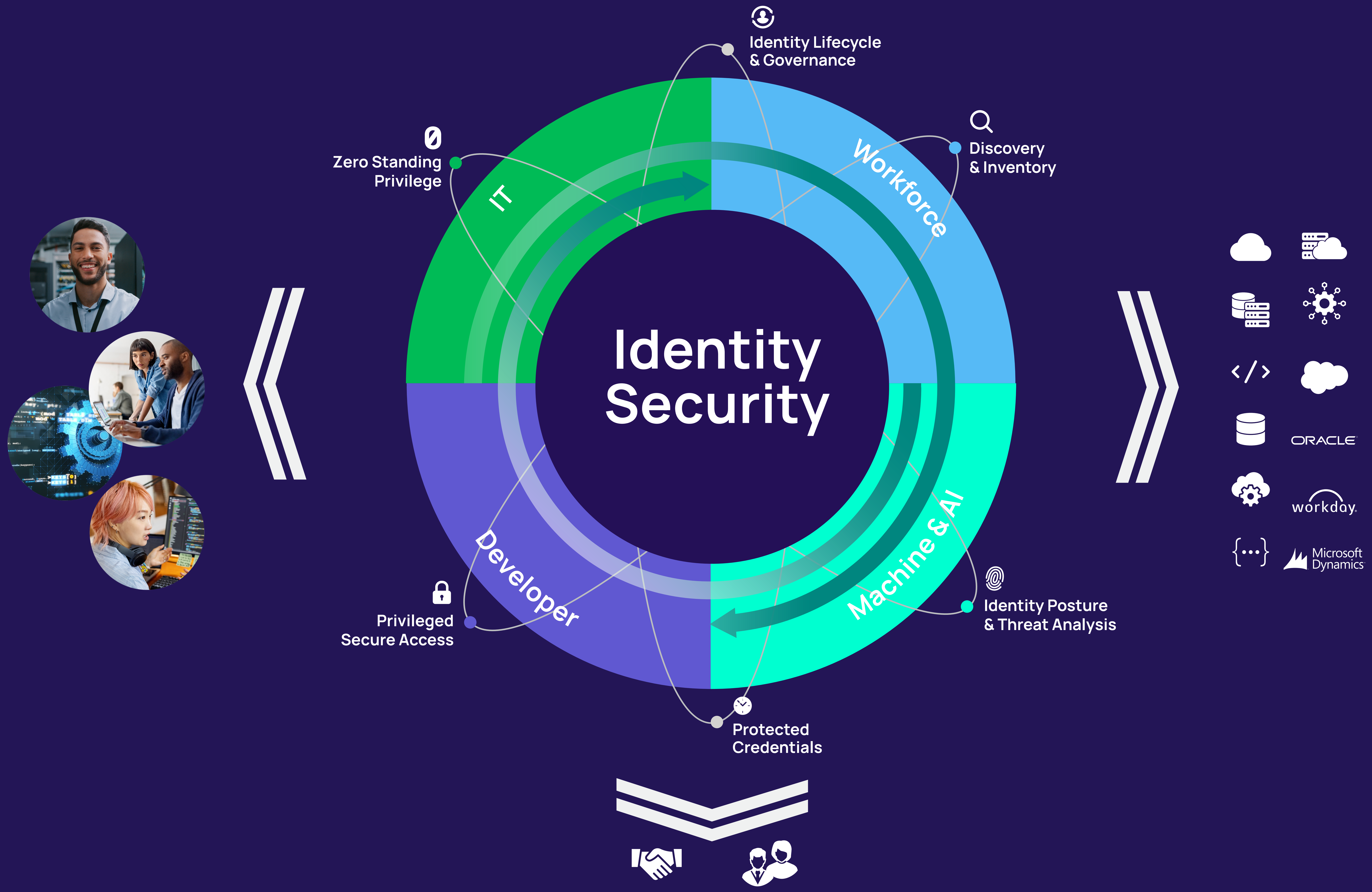
Workforce identities include business users, such as employees, contractors, vendors, and partners who access business applications. They do so from personal workstations and mobile devices, often remotely.

Machine and AI identities

Machine and AI identities are digital identities of devices and workloads and also include AI agents. Without proper human oversight, they can be provisioned incorrectly and easily become orphaned.

Developer identities

Developer identities have elevated access akin to IT admins, as they run critical systems in the CI/CD process, and dev environments separate from production.



Identity Security

IT

Workforce

Machine & AI

Developer

Identity Lifecycle & Governance

Discovery & Inventory

Identity Posture & Threat Analysis

Protected Credentials

Privileged Secure Access

Zero Standing Privilege

The identity security leader is the team captain

Like a captain, the identity security leader is often both player and coach. They are the on-pitch leader who sees the whole field and organizes the strategy so that each specialized function can execute at a top level, while also working together toward a common goal.

In enterprise terms, they need to manage identity security across functions and departments with different workflows and KPIs, as well as up to leadership, and down to every user in the organization.

To be successful, the modern identity security leader needs to:

- Have granular visibility throughout the **entire lifecycle** of each identity as it's created, permissions change, and it's deprovisioned.
- Understand all the assets each identity could access and does access across the environment and what they do at **each point of interaction**.
- Ensure the right insights get to the right people to make **data-backed, dynamic decisions**. This requires providing access to teams and systems with different jobs-to-be-done, like:
    - Provisioning human identities and access/identity configuration management
    - Rotating privileged accounts and credentials
    - Checking out privileged accounts to work on infrastructure or access applications
    - Creating service accounts and machine/AI identities
    - Reviewing and approving application access
    - Monitoring, alerting on identity access and behavior
    - Managing incidents, with root cause analysis, and identity threat detection and response
    - Conducting identity security posture analysis
    - Auditing and reporting
- Provide a **simple, consistent interface** that's easy for anyone to learn even if they aren't specialized in a particular software or identity type.
- **Easily maintain solutions** without expensive processes to learn, integrate, and deploy them.
- Leverage innovations that **speed up processes**, for example, automated, policy-driven access, AI-driven data analysis, AI-driven authorization, and natural language search. AI must provide **actionable** insights and automation, like an identity security copilot that continuously checks for policy drift, misconfigurations, and attacks, reducing manual overhead.

How to bring everything together

Consolidating the number of identity security tools you have to manage sounds enticing, but it's easier said than done. People are comfortable with the systems they currently use, especially if they were the ones who first set them up. Plus, some legacy tools simply don't play well with others.

You may try to stitch and glue everything together yourself. Microsoft, for example, offers web hooks, connectors, and open-source rules for building your own bespoke platform.

Unfortunately, very few people have the industry knowledge and technical chops to ensure systems communicate seamlessly with detailed data exchanges. It's tricky for experts skilled in one area of identity security to build a comprehensive system that accounts for the analysis and workflow needs of all the consumers of data. Plus, they may not consider industry standards that are essential for compliance.

Even if your internal experts do build an integrated solution, when those people move on to other organizations, someone else must maintain the system without really understanding how it was built.

Instead of spending valuable time and resources trying to do it all on your own, you can leverage a proven solution that brings best-of-breed identity security components together and surfaces shared data for all of them to consume, while also allowing you to integrate technology you already use.

So, how do you keep up?

Identity leaders and their teams need a seamless, smart ecosystem that incorporates all the workflows described above, and all the components of a best-in-class identity security program working together and sharing information in a single platform.

What to look for in an identity security platform

Some “platforms” are simply an interface layer on top of solutions that are disconnected under the hood. They look pretty, but they don’t solve the challenges of normalizing and synthesizing data for layered analysis and contextual decision-making.

Others are closed, black boxes. They’ve got so much spaghetti connecting the components they don’t want you to see it. And they assume you only use identity solutions that are sold as part of the platform.

Ask the tough questions to be sure any platform you consider meets the following requirements to gain the most from your investment.

1 Modular and composable

Modularity allows for rapid integration without a rip-and-replace. A modular, composable platform ensures you can build from a solid foundation, integrate with existing applications, and add on more capabilities and solutions as needed. That way, you can start small and expand along a maturity timeline that’s ideal for you without adding additional vendors. You can future-proof your solution as new identity security challenges emerge (e.g., quantum resistant crypto or new AI identity types).

2 Industry standards and protocols

Look for a platform that’s built using industry standards and protocols, so it meets compliance requirements today and is sustainable and extensible for the long term.

3 Key use cases and workflows

Any identity security platform should include six core components of identity security:

a. Continuous Discovery and Inventory

With built-in discovery, you can find and classify all privileged accounts and their related secrets, permissions, and MFA rules, across all on-premise, cloud, and application environments.

All of those elements should be kept in an inventory within the platform. This inventory ensures that all identities operating in your extended IT environment are well understood, reducing the risk of overprivileged identities and orphaned privileged accounts that should have been deprovisioned.

Because new identities and accounts are spun up and permissions change frequently, continuous discovery ensures you always have the latest information.

If (and when) you discover accounts that violate security policies, you should be able to bring them under central management and ensure they’re aligned with security best practices.

b. Protected Credentials

A centralized credential vault avoids the use of static secrets by automating complex credential management, including creation and rotation of secrets, so they have a limited lifespan.

With an enterprise vault, users can access shared privileged accounts, while granular privileged behavior can be tied to individual identities. You know which person checks out credentials for a shared privileged account and what systems they access.

In addition, your workforce should have access to browser extensions for one-click autofill, customizable templates, and dynamic password updates, so they can avoid the risks associated with browser-stored passwords.

For machine identities and AI, enterprise vaulting should also centrally manage credentials such as SSH keys, tokens, and certificates.

c. Privileged Secure Access

Your platform should ensure that all human and machine-to-machine communications are authenticated and authorized with fine-grained access control, preventing unauthorized access and ensuring that only legitimate interactions occur.

Context-aware multi-factor authentication (MFA) is an essential security control to verify human identities prior to allowing access. While MFA adds identity assurance against targeted attacks, MFA challenges that are too frequent lead to fatigue. By making MFA context-aware, you can choose to automatically add layers of protection for high-risk systems or activities. For example, you may choose to add layers of MFA for remote workers or third parties.

To mitigate risk, a platform should check against access policies occur at every point of interaction, including initial login, privilege elevation, and lateral movement across systems. Each interaction impacts the cumulative risk of each identity and provides additional context for security decision-making.

Today's hybrid organizations and agile workflows make static access policies, even role-based-access policies, inadequate. Instead of relying on fixed roles, intelligent authorization is dynamic and based on context, including changing behavior patterns and risk scores.

d. Zero Standing Privilege

Your platform should enforce consistent least privilege and just-in-time, just enough access for all identities. This ensures that identities have only the access they need, when they need it. That way, even if an identity is compromised, ZSP minimizes the blast radius and consequences because privilege escalation and lateral movement are limited.

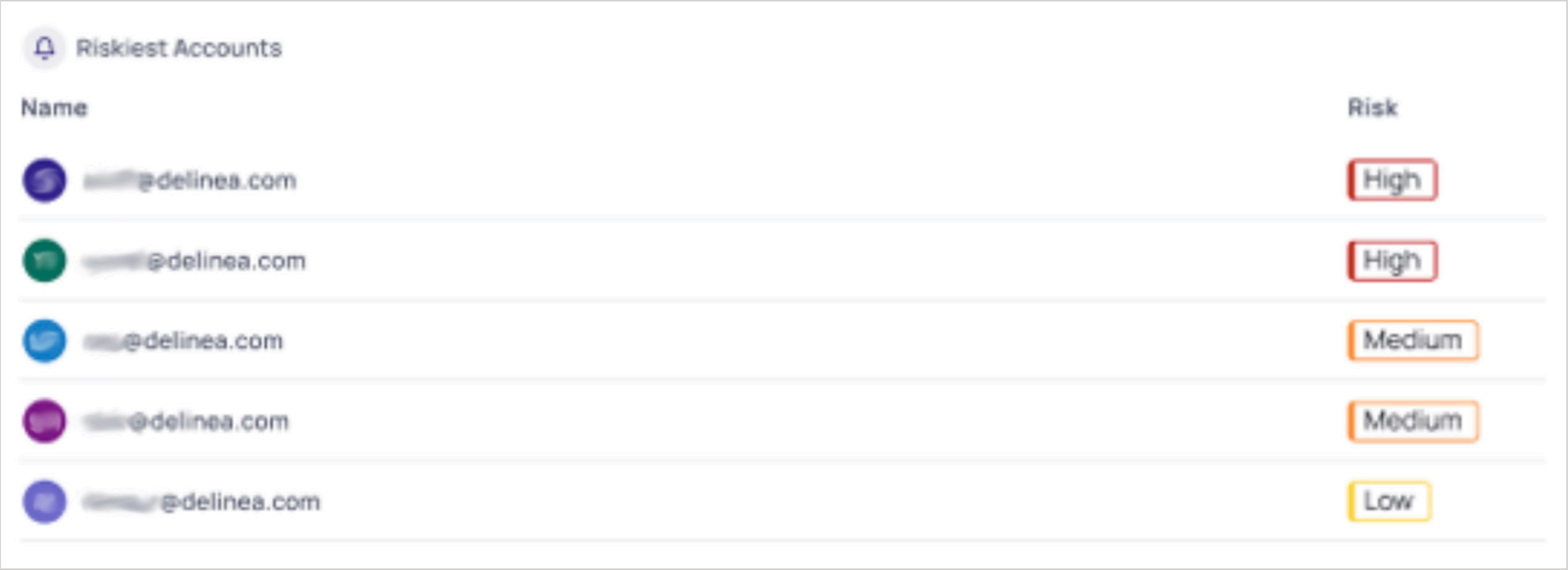
e. Identity Posture & Threat Analysis

As preventive controls within your platform, identity posture and threat analysis surface common identity misconfigurations, such as missing MFA or excessive privileges, and measure the associated risk. Risk is based on context, including the total or "effective" access of an identity throughout your environment.

Detective controls create an early warning system that gives you time to act before a small issue becomes a catastrophe. By recording, monitoring, and auditing sessions and comparing privileged behavior to a baseline, you can detect suspicious activities that may indicate compromise. Red flags could include an identity accessing sensitive data at unusual times, frequently requesting privilege elevation, or creating a back-door account. Threat detection can even tell you if an MFA bombing attack is sending multiple requests, hoping someone will confirm their identity and unlock access.

It's essential that monitoring and detection capabilities extend throughout your entire IT environment and account for different attack scenarios. For example, a threat agent may circumvent your central vault and attempt to access a server directly. That's why it's important to gather data and enforce access policies directly via agents on each server.

Understanding each identities risk score with evidence-based steps to remediate gaps



Riskiest Accounts

Name	Risk
[redacted]@delinea.com	High
[redacted]@delinea.com	High
[redacted]@delinea.com	Medium
[redacted]@delinea.com	Medium
[redacted]@delinea.com	Low

In response to threat indicators, you may choose to notify your security operations team so they can review threat signals with the appropriate context, or even enable automated actions. Detailed, evidence-backed insights and changing risk scores can automatically trigger actions such as rotating passwords, removing privileges, or adding layers of MFA, for any anomalous privileged behavior that is managed by the platform.

f. Identity Lifecycle & Governance

Your platform should automate the provisioning, deprovisioning, and ongoing governance of identities. This automation streamlines identity management processes such as joiner-mover-leaver (JML) management and access reviews, reduces administrative overhead, and ensures compliance with security policies and regulations.

In addition to governing human identities, you can bring governance to your automation workflows, including processes such as provisioning and deprovisioning accounts, injecting secrets, and managing changes like infrastructure-as-code.

4 Resilience is key to platformization

If you're going to put all your eggs in one platform basket, you better be sure that basket is strong enough to hold them. Any identity security platform you choose must provide the highest level of resiliency and fault tolerance.

5 Natural language queries democratize data

Any modern platform should leverage GenAI capabilities to democratize data and help you do your job easier and faster. You should be able to use **natural language to ask questions** about identities, such as their activity, access rights, and alignment with your organization's risk tolerance. Expect combined, contextual results based on data across all identities.

6 Unified controls with a personalized experience

Within your platform, all your stakeholders – PAM admins, IAM admins, IGA admins, security operations centers, etc. – should be able to access the security controls and information they need, while you, as the identity security leader, have a complete overview.

That cohesive visibility fosters collaboration and delivers a holistic understanding of access, privilege, and risk, eliminating the blind spots often created by legacy, siloed identity security solutions.

Only then can you as the team captain support the joint goals of IT and security.

Delinea

Securing identities at every interaction

Delinea is a pioneer in securing human and machine identities through intelligent, centralized authorization, empowering organizations to seamlessly govern their interactions across the modern enterprise. Leveraging AI-powered intelligence, Delinea's leading cloud-native Identity Security Platform applies context throughout the entire identity lifecycle – across cloud and traditional infrastructure, data, SaaS applications, and AI. It is the only platform that enables you to discover all identities – including workforce, IT administrator, developers, and machines – assign appropriate access levels, detect irregularities, and respond to threats in real-time. With deployment in weeks, not months, 90% fewer resources to manage than the nearest competitor, and a 99.995% uptime, Delinea delivers robust security and operational efficiency without compromise. Learn more about Delinea on **Delinea.com**, **LinkedIn**, **X**, and **YouTube**.