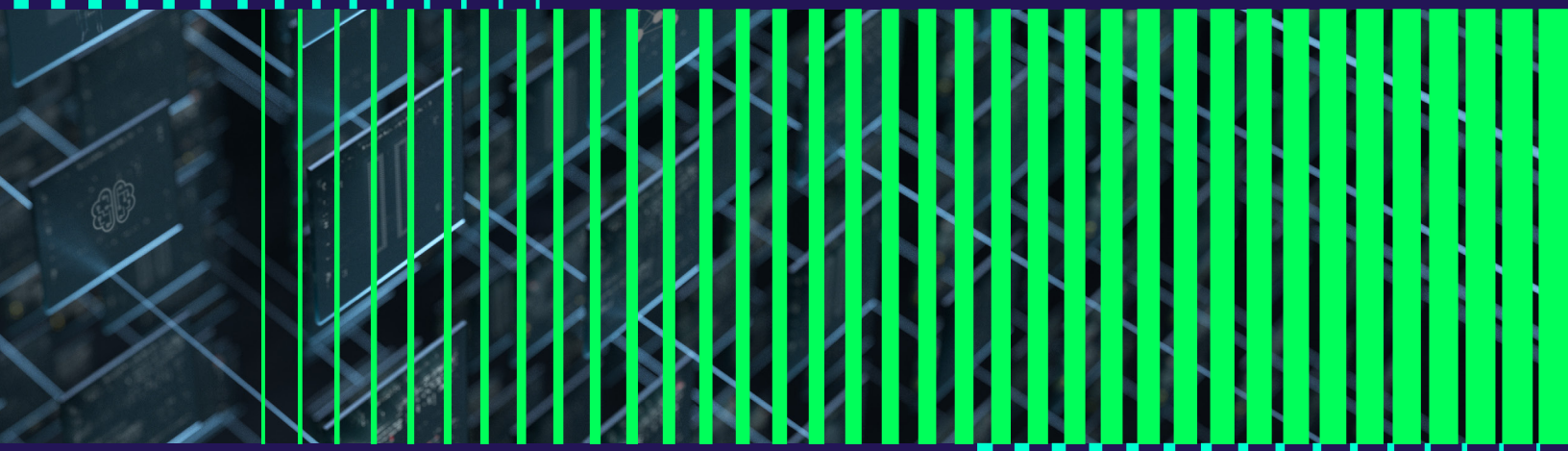
Delinea

Identity Security Maturity Model



WHITEPAPER

Identity Security Maturity Model

A framework to help organizations systematically lower privilege and identity-based attacks risk, increase business agility, and improve operational efficiency

Introduction

Identity security is the primary method attackers use to access sensitive systems. Protecting identity security on each system is extremely important to defend against these attacks. The Delinea Identity Security Maturity Model is a framework to help you systematically lower privileged access risk, increase business agility, and improve operational efficiency.

The model is based on security industry best practices and Delinea's work with over 10,000 customers of all types, ranging from organizations just beginning their identity security journey to the most experienced and advanced users.

As a leader in the identity security market, working to continually improve our customers' security posture and reduce business risks, we recognize the need to update and refine the definition of identity security maturity as the industry evolves. This latest model is multi-dimensional and provides actionable recommendations for step-by-step adoption.

You can apply lessons and guidance from the Model to your cybersecurity strategy regardless of your company's size, industry, or the number and type of systems you need to secure. It will help you navigate your journey based on your own risk drivers, budget, and priorities.

Approach

The Identity Security Maturity Model outlines four phases:

The more mature you are…
the more your attack surface is under your control

As you progress through the phases of the maturity curve, you expand your protection to include more types of privileged identities, sensitive data, and critical systems.

Most organizations have exponentially more privileged identities as employees. A by-product of cloud migration is a much larger attack surface due to an exponential increase in identities and virtual systems. Privileged identities include domain administrator accounts, local accounts, and non-human service accounts used by applications, AI agents, and databases for communications and data exchanges.

In a mature identity security strategy, "privileged user" no longer equals "IT user." It also includes business users who access financial, personal, or other sensitive information from web apps and developers who build products using AWS, Azure, Google Cloud Platform, or their own cloud.

The scope of privileged identities and use cases expands in each model phase. Organizations in the Foundational phase are focused on the administrators using Windows machines. Those in the Enhanced phase incorporate business users, developers, and third parties using Windows, Unix/Linux, and Mac workstations. The Adaptive maturity level also encompasses non-human identities, such as machines and AI.

The more mature you are… the more dynamic, automated, and integrated your approach

The meaning of "privileged access" includes not only who can access what, but also what they can do with that access and when they can do it.

Identity security maturity begins with static policies and controls and becomes more granular and dynamic with each phase.

Native operating controls aren't sufficiently granular. As you progress along the maturity curve, you add more granular controls and implement conditions and time limits to access. Ultimately, authorization controls become risk-based and adapt as your risk profile changes.

Intelligence and automation increase as well. The first shift is making the jump from manual to automatic password creation and rotation. From there, more capabilities are automated until your identity security solution is continuously learning and adapting as an intelligent system.

Integration is a key aspect of automation. As such, as the maturity curve rises, it includes adjacent technologies that are part of comprehensive, integrated identity security, including Cloud Identity and Enterprise Management (CIEM), Identity Threat Detection and Response (ITDR), and Identity Governance and Administration (IGA).

Dimensions of maturity

An essential addition to this model is a multi-dimensional view of maturity. Each maturity phase is characterized along three dimensions, including:

- **Governance, Risk, and Compliance (GRC)** – How strong is the integrity of your system and how much visibility and oversight do you have?
- **Privilege Administration** – How do you create, define, and manage privileges across your organization?
- **Identity and Access Management** – How strong are your authorization controls, and how granular are your access controls?

In the detailed description of each maturity phase below, you'll learn how to evaluate your maturity according to these dimensions. It's not unusual for an organization to be more mature in one dimension than another. Once you evaluate your current maturity level, you'll be able to prioritize security activities so that one dimension doesn't accelerate too rapidly without the support of the others.

Note that the three dimensions of maturity aren't tied to specific job roles or business functions. "Governance," for example, may be shouldered by people responsible for IT infrastructure or desktop teams, not necessarily by a central GRC function alone.

Note that the three maturity dimensions aren't tied to specific job roles or business functions. "Governance," for example, may be shouldered by people responsible for IT infrastructure or desktop teams, not necessarily by a central GRC function alone.

How quickly should you accelerate your maturity?

Acceleration isn't the same for everyone. Your identity security maturity should reflect your risk profile.

For some organizations, protecting access to a few critical systems significantly impacts their overall risk profile. Based on their risk tolerance, a company might implement authorization policies and controls for one department, geography, or type of privileged identity, and never roll them out to the full organization.

However, security risk increases as organizations begin to scale and migrate more workloads to the cloud, so maturity must keep pace. For example, when organizations grow business functions, they may not decide to—or may not be able to—hire experienced IT staff, which means that the same number of people are stressed to manage a broader, more diverse range of IT operations and security. The demand for IT automation may hasten their acceleration along the maturity curve.

Similarly, rapidly growing organizations tend to work with more vendors, partners, and contractors as they expand into new markets and provide more offerings. Organizations with substantial third-party risk will need to accelerate along the maturity curve faster than others.

Commonly, organizations undergoing digital transformation will likely have more services in the cloud and will need mature authorization policies and controls for cloud-based servers, DevOps tools, and service accounts.

Those bound by regulatory and compliance mandates will likely prioritize implementing least privilege policies, multi-factor authentication, and session monitoring ahead of other capabilities. As they mature, they will need to customize and share reports with executives and auditors easily.

The four maturity phases

The controls associated with each maturity phase reflect the order in which Delinea recommends organizations roll out their identity security strategy. This step-by-step adoption method helps you build a strong foundation that will support you as you scale.

PHASE 0: High Risk

The key for organizations in Phase 0 is recognizing their risk and planning for action.

Organizations in this phase secure their privileged accounts in a limited way, if at all. They typically set up privileges manually and may keep track of them via spreadsheets. As a result, they often provide excess privileges to people who don't need them, share privileges among multiple administrators, and neglect to remove privileges when users leave the organization or change roles.

They tend to have minimal complexity requirements for password creation and only single-factor authentication, which opens the door to password hacking.

Service accounts are created "in the wild," leading to poor documentation, poor mapping to applications or core services, and "re-usage," where a single account is used repeatedly for numerous services.

It's also common in Linux/UNIX environments for administrators to create their own local privileged accounts since they don't have a single unified account (like an Active Directory account) to log in across them all. This makes the attack surface very big.

Security and operations teams are typically unaware of the breadth of web applications in use and allow users to make independent decisions regarding privileged access and permissions.

These organizations have a high degree of cyber risk. If an external attacker or malicious insider has access to privileged accounts, they can steal confidential information, disrupt IT infrastructure— even shut it down—and cost millions.

Dimensions of Identity Security Maturity	Typical Characteristics
Governance, Risk, and Compliance	• No centralized vault for managing passwords, privileged accounts, or Secrets. • No centralized inventory of all assets in the environment. • No easy way to report on user access permission and privileges. • No easy way to reconcile who has access to what, who did what, and who approved access. • Failed audits.
Privilege Administration	• Managing administration for Windows servers using Domain Admin Group membership. • Managing local accounts on each Unix/Linux system and editing local /etc/sudoers files. • Users are often admins of their own workstations.
Identity and Access Management	• No centralized access and authorization controls. • No centralized identity management. • Admins access using local admin accounts. • Hard to tell who has access and what privileges they have.

PHASE 1: Foundational

The key for organizations in Phase 1 of maturity is to gain visibility over their attack surface and reduce it.

Once their eyes are opened, organizations begin to take control by vaulting shared privileged accounts. Using Privileged Access Management, they focus first on privileged accounts managed by domain administrators and other IT users.

Although organizations at this stage are more mature, they continue to operate in a reactive mode. They often have numerous, disconnected tools and practices rather than an integrated system centrally managed and controlled by policies. They don't differentiate access based on roles, don't have sufficient visibility over privileged identities, and can't easily or automatically produce reports or compliance documentation.

Organizations in this stage must make periodic pushes to continuously discover new privileged identities operating in their environment. Occasionally, business-critical applications experience downtime or fail because new usages of service accounts have not been associated with the corresponding service account managed in the identity security solution. This can lead to a breakdown in business operations, negative customer experiences, and mistrust between teams, making full adoption of authorization policies difficult.

Dimensions of Identity Security Maturity	Typical Characteristics
Governance, Risk, and Compliance	• Establish an accurate inventory of administrative privileged accounts and passwords. • Classify credentials and secrets.
Privilege Administration	• Vault and automate periodic rotation for all administrative accounts. • Vault Active Directory and Azure privileged accounts and manage privileged account Groups. • Discover and vault local administrative accounts. • Establish a secure administrative environment for both local and remote sessions. • Establish initial privileged access workflow.
Identity and Access Management	• Enforce MFA for access to vault, including secret check out and remote session initiation. • Establish Alternative Admin accounts to prevent using public identities. • Enforce Alternative Admin and MFA for remote access.

PHASE 2: Enhanced

The key for organizations in Phase 2 is to expand authorization policies to reduce the number of overprivileged identities and curb privilege sprawl. This is a combination of normalization — reducing excessive privileges — and consolidation — removing additional local privileged accounts for admins so they have only a single (AD) account for access.

In this phase, organizations broaden privileged user management to include not only domain administrators but also business users, developers, and vendors. In addition to implementing a central vault, they expand granular authorization controls to endpoints, including servers and workstations. To address the challenges of securing web and SaaS applications, they start to manage access to these apps centrally and apply granular authorization controls based on just-enough, just-in-time policies.

Identity security becomes a top priority during this phase and the next. Organizations at this level are committed to continuously improving their identity security practices.

Dimensions of Identity Security Maturity	Typical Characteristics
Governance, Risk, and Compliance	• Discover, classify, and manage local accounts, servers, Groups, roles, and security configuration files that might grant privileges across all assets. • Implement real-time session monitoring and application control policies for endpoints. • Enforce host-based session, file, and process auditing with integration to SIEM tools. • Integrate with ITSM to drive access control request workflows tied to help desk tickets.
Privilege Administration	• Establish privilege elevation policies for all endpoints (workstations and servers). • Establish just-in-time, just-enough privileges. • Vault Linux and local administrative credentials (passwords and SSH keys). • Expand remote access control to vendors and contractors without creating AD accounts.
Identity and Access Management	• Enforce multi-factor authentication at endpoints for direct log-in and privilege elevation. • Eliminate local accounts via identity consolidation for Unix and Linux. • Remove hardcoded credentials and config data from applications and scripts. • Automate authorization controls in DevOps workflows and tooling.

PHASE 3: Adaptive

The key for organizations in Phase 3 of identity security maturity is to increase automation and intelligence, taking the concept of continuous improvement to a higher level.

As such, they fully and automatically manage the entire lifecycle of a privileged identity, from provisioning to rotation to deprovisioning and reporting. At this stage, authorization policies are consistent and centralized for an automated defense-in-depth security strategy. Identity security controls are layered to break the attack chain at multiple points. If an attacker gets past one, they will hit another. Continuous monitoring automatically identifies anomalous privileged behavior and kicks off appropriate incident response activities.

The most mature identity security programs integrate authorization into other IT and security workflows and solutions and have a consolidated view of all privileged identities operating in their diverse environment, fine-grained control over their access permissions, and ongoing oversight.

Continuous discovery, governance, and automation

It isn't until the Adaptive stage of maturity that most organizations get an accurate picture of non-human machine identities and their identity security risk posture.

Following discovery, governance is extended to increase efficiency and oversight. Machine identities and service accounts are also automatically decommissioned based on policies without causing disruption to critical services or business processes. Organizations establish

workflows requiring approval prior to the creation of new service accounts. Enforced certification and entitlements ensure accountability and ownership.

Dimensions of Identity Security Maturity	Typical Characteristics
Governance, Risk, and Compliance	• Integrate with Identity Governance and Administration (IGA) tools for attestation reporting and risk-based approvals. • Leverage audit data, Artificial Intelligence (AI), and automation to detect, track, and alert to misconfigurations and identity-based threats. • Implement discovery, provisioning, and governance across identity and cloud service providers. • Harden operating systems and application components.
Privilege Administration	• Establish more granular policies for privilege elevation. • Automate onboarding of new managed assets.
Identity and Access Management	• Ensure all connections required for privileged operations must be mutually authenticated with cryptographic credentials. • Increase MFA from NIST Authenticator Assurance Level 1 (authenticating with an ID and password) to NIST Authenticator Assurance Level 2 (AAL2). AAL2 has more identity assurance due to the presence of a second factor. • Restrict privileged access to registered and company-owned endpoints. • Prohibit privileged access by any client system that isn't known, authenticated, properly secured, and trusted. • Require dual authorization for privileged operations on critical or sensitive systems.

How Delinea can help

As you progress on the maturity path, Delinea gives you the tools, resources, and expert advice you need every step of the way.

We know that the approach to identity security isn't the same for every organization. We meet you where you are and help you accelerate your progression. Our modular identity security platform is built to scale with you.

Our mission is to make you a self-sufficient security champion so you can own your identity security journey.

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**.

 MATM-WP-0925-EN