Brought to you by

Delinea

Identity-Centric Zero Trust

for dummies®

A Wiley Brand

Assess your current maturity level

Explore Identity-Centric Zero Trust use cases

Create a road map to Zero Trust

Delinea Special Edition

Lawrence Miller
Tony Goulding

About Delinea

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, the Delinea Platform delivers robust security and operational efficiency without complexity.

Learn more about Delinea on Delinea.com, LinkedIn, X, and YouTube.

Identity-Centric Zero Trust

Delinea Special Edition

by Lawrence Miller and Tony Goulding

for dummies®
A Wiley Brand

Identity-Centric Zero Trust For Dummies®, Delinea Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-394-29089-5 (pbk); ISBN: 978-1-394-29090-1 (ebk); 978-1-394-29091-8 (ePub).
Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager and Developmental Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Traci Martin

Sr. Client Account Manager: Matt Cox

Production Editor: Umeshkumar Rajasekhar

Table of Contents

Introduction

Cybercriminals no longer hack into organizations. Instead, they simply log in using weak, stolen, or otherwise compromised credentials in a multi-stage, identity-based attack. Once inside, they look for opportunities to move laterally to access more and more of your sensitive data and critical resources.

Unfortunately, traditional security approaches like firewalls and virus protection can't protect you against these types of identity-based attacks. Old-school, perimeter-based security solutions were built for a world of well-defined boundaries, but organizations today have a porous perimeter with users and resources continually moving in and out of the network.

Meeting the challenges of the modern IT environment means shifting from an implicit trust model to an explicit one. With Zero Trust security, you assume attackers are already inside your organization. Nobody is trusted automatically, even when they've cleared the network perimeter.

The Zero Trust model incorporates multiple security controls and technology solutions throughout an IT environment to protect and manage identities, devices, networks, applications, and data. All identities are verified, they have minimum rights, granular access is granted based on context, and activities are continually monitored to make sure security controls are working as expected.

About This Book

This book is for IT and security professionals who are building a Zero Trust program for the first time, as well as those already on their Zero Trust journey. You discover how the definition of Zero Trust has evolved beyond a network-centric on-ramp and how identity security solutions are also critical to achieving Zero Trust practices.

Inside, you find easy-to-understand explanations to help you save time creating your own step-by-step roadmap. You can also share the content with others in your organization to increase

awareness about the importance of Identity-Centric Zero Trust, gain buy-in and budget for your program, and drive adoption of cybersecurity best practices.

Icons Used in This Book

Throughout this book, we occasionally use special icons to call attention to important information. Here's what to expect:


REMEMBER

We use the Remember icon to point out information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!


TIP

Tips are appreciated, never expected — and we sure hope you'll appreciate these tips. The Tip icon points out useful nuggets of information that will save you time or money or just make your life a little easier — at least at work!


WARNING

Warning icon information helps you steer clear of issues that may cause further security risk to your organization.

Beyond the Book

Identity-Centric Zero Trust doesn't have to be an insurmountable challenge. If you're interested in learning more about Zero Trust and how it fits into a comprehensive identity security strategy, you can visit the Delinea website at `www.delinea.com`. Free educational resources include original research on privilege and identity-based attacks, assessment tools to discover vulnerabilities and benchmark your own Zero Trust practices, as well as how-to guides, templates, and checklists to accelerate your Zero Trust journey.

IN THIS CHAPTER

- Comparing different Zero Trust methods
- Grasping foundational concepts
- Seeing the evolution of Zero Trust
- Meeting business productivity requirements

Chapter 1
Understanding Why We're Still Talking about Zero Trust

Over 15 years ago, Forrester introduced the Zero Trust Model for information security. Today, Zero Trust is a widely recognized best practice that's endorsed by cybersecurity analysts, vendor-neutral reference architectures, and regulatory frameworks. Notable advocates include the Cloud Security Alliance, National Institute of Standards and Technology (NIST), and the Cybersecurity and Infrastructure Security Agency (CISA).

Zero Trust isn't simply a marketing buzzword. It's achievable, and for some organizations, such as United States (U.S.) Federal government agencies, it's required based on executive order. Many IT and security teams have moved beyond the basic question: "What is Zero Trust?" Yet, the question remains: "What is the best way to implement Zero Trust?" That's what this book covers.

Zero Trust requires moving from implicit to explicit trust. With a Zero Trust security posture, you reduce the likelihood of an attack and contain the potential impact should one happen.

REMEMBER

Zero Trust isn't a solution you can buy. Instead, it's a model that defines your approach. It's supported by capabilities of multiple technologies as well as people, policies, and workflows.

In reality, the "zero" in Zero Trust may never be achieved because no one has "zero" rights. We can instead say that Zero Trust could mean "zero administrative trust," which clarifies that it's the high-risk access and activities that should receive the strongest protections and scrutiny.

This chapter sets the foundation for understanding Zero Trust. You discover different Zero Trust models, see how Zero Trust has evolved, and connect Zero Trust to your business goals.

Comparing Network-Centric and Identity-Centric Zero Trust

The Zero Trust model requires security controls throughout an IT environment to protect and manage identities, devices, networks, applications, and data. Since the advent of Zero Trust, many organizations have begun with a Network-Centric approach, employing software defined perimeters and micro-segmentation strategies. This on-ramp to Zero Trust is a fine start to lay the groundwork for limiting access to high-risk resources, but it can't be the end of your journey.

Say a malicious insider or external attacker steals credentials that unlock high-risk resources. Even with the most robust network segmentation, that threat agent could impersonate an authorized user and operate under the radar.

What happens if an identity is misconfigured, is missing multi-factor authentication (MFA), or is accidentally granted shadow admin access that's inappropriate for their job function? Network segmentation won't limit or detect unexpected behavior.

That's why a comprehensive Zero Trust security strategy must include Identity-Centric Zero Trust. In fact, starting with Identity-Centric Zero Trust is a better choice than starting with Network-Centric Zero Trust, or doubling down on more of the same (more firewalls and the like). Those with limited budgets should prioritize Identity-Centric Zero Trust, even if it means diverting budget away from network security.

Identity-Centric Zero Trust practices are designed to

- Ensure only the right identities have access to critical resources and sensitive data at the right time.
- Avoid dangers of identities that are overprivileged or have standing access, especially likely in a complex, dynamic, hybrid cloud environment.
- Interrupt the attack chain so that even if threat agents get through initial defenses, their access is limited, and a cyberattack doesn't become a cyber catastrophe.

Zero Trust is related to privileged access, but standard Privileged Access Management (PAM) solutions like vaulting, session monitoring, and privilege elevation aren't sufficient to meet all Zero Trust best practices. Identity-Centric Zero Trust also involves adjacencies with other identity security systems and consolidates them in a coordinated strategy.

WHAT IS AN IDENTITY?

Privileged identities are everywhere in the IT environment. They're the building blocks for managing infrastructure, databases, applications, and services. Yet, for most people, they're invisible.

In an IT environment identities can be humans or machines.

Human identities include employees as well as third parties. Typically, human identities are initially created in identity directories such as Active Directory, or through federation with third-party systems. They include

- Domain Admins that control Active Directory users
- System Admins that manage servers, cloud platforms, and databases
- Superusers that manage Unix/Linux platforms
- Developers that have access to test and production systems, cloud platforms, as well as software in the development toolchain
- Contractors, vendors, or other third parties that access IT systems for troubleshooting, support, or outsourced development

(continued)

(continued)

- Business users that can access sensitive data and execute transactions via financial or Human Resources (HR) systems
- Business users with local administrative accounts on workstations, which allow them to install applications and execute commands

Non-human identities, also known as *machine identities,* are digital entities that run and manage applications, services, and scheduled tasks, Internet information services (IIS) application pools (.NET applications), and networking equipment such as firewalls, routers, and switches. Machine identities come in two main flavors:

- Workloads, which include virtual Windows, Linux, and Unix machines, applications, and containers
- Devices, which include user workstations, mobile devices, and operational technology

Machine identities are increasing rapidly, largely due to new technologies, including virtual machines and containerization, that create more machine workloads. They represent a substantial and often unmanaged portion of your identity attack surface.

There are anywhere from 20 to 100 machine identities for every human identity. Their proliferation has drawn bad actors, requiring focused effort to prevent, detect, and respond to machine identity-related threats.

Looking at the Six Foundational Concepts of Zero Trust

Six key concepts form the basis of your policies as you shift from implicit to explicit trust, limited access, and ongoing verification.

Least privilege access

The Principle of Least Privilege is foundational to Zero Trust. It means that all identities should have access *only* to the resources, systems, and data they need, *when* they need them. Anything more is excessive and unnecessarily increases risk. When access is limited to a least privilege state, if an attacker were to impersonate a user or steal credentials, they would only get so far.

With a least privilege approach, instead of granting broad access rights based on role or seniority, permissions become much more granular and restrictive. Least privilege access considers not just whether an identity can access an IT resource but also what they can do once inside, including changing data, executing transactions, making configuration changes, and so on.

Least privilege also supports requirements for Segregation of Duties (SoD) in business applications, such that users can only execute certain tasks at certain times and avoid toxic combinations of access rights. For example, a user shouldn't be able to both create a new vendor and pay that vendor.

Default Deny

The Default Deny concept prescribes that every identity operating in your environment should be provisioned with standard access. All users (even domain and system admins) should operate with standard privileges until they require a higher level of access.

Following this requirement also means disabling local admin credentials which are typically included in workstations by default. Yes, disabling local admin credentials means that people won't be able to download productivity apps, install printers, and make other changes unless you explicitly allow it.

Many organizations have learned the hard way that removing privileges, including local admin rights, can backfire if people can't access systems to do their jobs.

Access by Policy

Through policy-based controls you can centrally define and manage granular access to meet least privilege best practices. Though they may start with standard access rights, many identities can't remain in a non-privileged state if business is expected to move forward. In a Zero Trust model, you can determine when privileges may be granted and how. Policies can adjust as identities expand and new use cases emerge.

With Access by Policy, you avoid shared privileged accounts. This is important for two reasons. One is they have god-level permissions. The other is they're anonymous, so there's no accountability when using them. Access by Policy assumes an individual account with minimum rights that can be elevated for legitimate

purposes, and it ensures accountability because it's tied to a unique person.

REMEMBER

Policy management isn't a once and done activity. It follows a life cycle, as identities, access requirements, and risks change. You can create different types of policies as you implement Identity-Centric Zero Trust.

Provisioning, reprovisioning, deprovisioning policies

Provisioning, reprovisioning, and deprovisioning processes are critical to ensure all identities have access to only the resources they require. Identity Lifecycle Management (ILM) optimizes the practice of defining and administering privileged access through policy-based controls.

An identity's life cycle encompasses all the things that happen to an identity that need to be provisioned, tracked, and managed. This is broken down into life cycle events:

- **Joiners:** Joiners are identities — human or machine — that are joining your organization. These could be new employees, customers who registered on your website, or third parties who need access to your systems and resources. An identity is required before entitlements can be assigned or access can be provisioned.
- **Movers:** Movers are identities that are changing in some material way from how they were initially provisioned. Maybe an employee has changed roles and needs different access to an application or platform. Perhaps a consultant is moving to a different project and needs access to new systems or resources. In those cases, old access must be removed and only the access for the new role or project be provisioned.
- **Leavers:** A leaver could be an employee who's retiring or taking a new job, a vendor that's been replaced, or any other situation where you need to end the relationship with your organization. To effectively manage this part of the ILM, HR systems and IT provisioning solutions need to be in sync, so when an identity leaves, their access is removed at the same time.

Privilege elevation policies

Privilege elevation is key to limiting lateral movement by preventing a foothold from becoming a beachhead for continued attacks. Policies grant just-in-time (JIT), just-enough privileges that exist under limited circumstances. With dynamic access controls, you can configure policies so users can only use privileges for a specified period, at specific times, on certain servers, or other criteria. After privileges are no longer required, the user or account returns to their default, standard permissions.

REMEMBER

Because JIT privilege elevation eliminates standing privileges, many manual and tedious IT tasks are eliminated, such as credential rotation, privileged access expiration, and account deletion.

Application control policies for workstations

Workstations and their users are often the first to get compromised. Application control policies for workstations help you reduce risk while ensuring productivity. They elevate applications that users need without requiring admin credentials or IT support to approve them. You can create granular application control policies for allowing, denying, and restricting applications.

After you determine which applications are safe to run, you can add them to a trusted allow list based on their name, signature, certificate date, or other criteria. After you set up an initial allow policy, you can apply it to all protected endpoints. From that point, instead of managing each application request one by one, most application elevation is automated, with little work from IT, and seamless to users.

Based on advanced threat intelligence, known malicious applications can be automatically denied. For the remaining unknown applications, sandboxing restricts applications until your team has time to review and approve them.

Machine identities, including workloads and devices

Your Zero Trust policies should cover your entire attack surface, including non-human identities. Privileged access isn't limited to infrastructure, databases, and network devices. It extends to the cloud, big data projects, and DevOps automation, as well as containers or microservices in hybrid cloud environments.

Especially for DevOps, embedded passwords in code or stored in repositories must be replaced by application programming interface (API) calls to obtain vaulted passwords programmatically. Ideally, instead of using static vaulted passwords, DevOps should obtain temporary, short-lived tokens from the vault.

Risk-based verification

A core tenet of Zero Trust is to confirm that identities are authorized to access your IT resources, with layers of identity assurance that verify users are who they say they are. First, you should establish identities for privileged users via enterprise directories. These identities should be vetted by HR and automatically disabled when employment is terminated. The last thing you want is for a former database admin to retain privileged access rights.

Even for identities that are managed via your directory, Identity-Centric Zero Trust mitigates risk by requiring additional proof of identity before granting privileged access.

WARNING

Usernames and passwords alone are insufficient because they can be easily stolen, guessed, or reused. MFA should be enforced at key points, including vault login, password checkout, secret retrieval, server login, and privilege elevation. Rather than an always-on approach, you can use an adaptive or step-up approach to provide users with a better experience, only exposing them to MFA when necessary. *Risk-based authentication* is like step-up authentication, but it's dynamic instead of static. It creates a user behavior profile over time and compares user activity with that baseline to determine a risk score. If the score is too high, the authentication process can trigger MFA.

Security monitoring

Zero Trust is nothing if not skeptical. After you've set up your Zero Trust model, you need to ensure that everything is working as expected. You can do that in several ways:

- **Continuous and automated discovery:** This checks for identity misconfigurations, missing MFA, and backdoor privileged accounts that have been created outside of the accepted processes and parameters. This can be done through Cloud Infrastructure Entitlement Management (CIEM), Identity Detection and Response (ITDR), or both.

- **Through Identity Governance and Administration (IGA):** Regular access reviews ensure that people who have been granted privileged access should continue to have it.
- **Session monitoring and recording:** This checks for anomalous behavior that doesn't fit within expected parameters. Identity Detection and Response (ITDR) systems listen for signals and respond quickly to shut down identity-based attacks in progress. Host-based session recording solutions ensure that recording controls can't be bypassed, even if the vault is bypassed. They also can go beyond auditing commands and provide process launch and file system change auditing for your most critical resources. Recorded session activity can also be transcribed, and the resulting metadata can be used to search videos for needles in the haystack.

Understanding expected behavior allows you to flag possible access abuse or misuse. For example, you may want to know if users are attempting to log in unsuccessfully, gaining access for the first time in months, using a different IP address, or logging in at unusual hours. Any of these can signal an attack. If one occurs, monitoring helps digital forensics identify the root cause and critical controls to reduce your risk.

The Evolution of Zero Trust for an Uncertain Future

Technology has matured to make Zero Trust implementations possible. You can expect the attack surface to continue to change rapidly, risk factors to be even more dynamic, and IT teams to be stretched thin. Manual, static processes won't be able to keep up.

To maintain a Zero Trust security posture, your security controls must adapt to the reality of a constantly changing attack surface and risk profile, especially in a hybrid, multi-cloud IT environment. In the future, organizations will only be able to achieve scalable, risk-based Zero Trust with intelligent, dynamic policies.

For example, unlike traditional static authorization methods, in which access control decisions are based on predefined roles and permissions, dynamic authorization accounts for context of the

access request, such as the user's location, device, time of access, and current threat levels. Dynamic authorization has an inherent, risk-based model for making decisions. As risk scores change, so do access requirements.

In addition, AI-enabled solutions will become a vital strategy. AI capabilities are already bringing together skills and knowledge of multiple experts — security analysts, detection engineers, incident response experts — with your history and industry patterns — to do much more than any internal team can. Look for AI to support repeatable workflows, early detection of identity-based attacks, and even automated remediation.

Balancing Security with Productivity

The past 15+ years have taught organizations that Zero Trust can only be successful if it meets productivity requirements. People need seamless access to needed systems and data.

When security is complex, people find ways around it. Instead of blaming users, find ways to relieve their responsibility.

Technologies that support Zero Trust must work automatically and intelligently, based on policies. They must work as a system to enable a continuous identity and context-aware adaptive trust model. Integration must be seamless in relation to context, risk analysis, centralized management, and comprehensive reporting.

IN THIS CHAPTER

- Reducing breach risk
- Enabling secure cloud migration
- Ensuring regulatory compliance
- Accelerating IT modernization and digital transformation initiatives
- Providing secure remote access
- Securing the DevOps pipeline

Chapter 2
Exploring Identity-Centric Zero Trust Use Cases

In this chapter, we describe several real-world use case scenarios for Identity-Centric Zero Trust.

Proactive Breach Avoidance

Compromised credentials remain the leading attack vector, making Identity-Centric Zero Trust crucial for reducing risk. When a privileged identity is compromised, attackers can impersonate legitimate users, moving undetected to exfiltrate data, cause damage, and cover their tracks.

Identity-Centric Zero Trust minimizes risk with controls across the identity attack chain, addressing reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Multi-factor authentication (MFA)

requires identity confirmation at every interaction, including initial access and privilege elevation.

Even if attackers obtain privileged credentials, just-in-time (JIT), just-enough access policies limit their activities. The blast radius is contained, making it difficult for attackers to escalate privileges and move laterally.

Identity security capabilities discover and analyze identity-related data, identifying vulnerabilities before issues arise. You gain visibility into identities, access privileges, resources, activities, and risk insights. Visual access graphs show who has access to what, detailing relationships between human and machine identities. They highlight permissions, roles, overprivileged accounts, stale access, misconfigurations, and privilege escalation paths. This visualization clarifies access relationships in multi-cloud environments, enabling remediation and reducing attack likelihood and impact.

Secure Cloud Migration

As organizations shift workloads and data to the cloud, securing hybrid environments becomes challenging. Enforcing a consistent identity and authorization security model across all platforms is essential.

When securing your cloud migration, consider the following:

- **Misconfigured access and authorization:** Cloud migration involves tedious work, often leading to mistakes (it's kind of like giving everyone a master key for convenience). Poor access control management can result in unauthorized access and data breaches. Clear policies are essential to define which human and machine identities can access specific data and resources.
- **Weak identity management:** Tracking identities becomes challenging in a larger cloud environment. Comprehensive visibility and control are crucial to verifying privileged identities and their permissions and preventing vulnerabilities.
- **Entitlement creep with limited visibility:** As your network fragments with new workloads, applications, and users,

visibility diminishes. This leads to hasty permission grants without proper review. Comprehensive discovery, centralized management, enforcement, and continuous analysis are needed to detect anomalies.

Identity-Centric Zero Trust reduces risk in the cloud by

- Establishing a single identity infrastructure across on-premises and hybrid cloud environments
- Discovering human and machine identities, service accounts, groups and group memberships, permissions, roles, and policies, cloud resources, SaaS apps, PaaS access logs, and usage patterns
- Controlling privileged access, enforcing context-based MFA
- Assessing your cloud identity security posture, including identifying misconfigurations and potential threats
- Providing insights (detailed logs, reports, dashboards, session recordings, and incidents) to demonstrate regulatory compliance and simplify root cause analysis

Complying with Regulations and Frameworks

Constantly changing regulations make compliance increasingly challenging and costly. To assure the public that sensitive data like credit card numbers and health records are protected, organizations must comply with various mandates, industry standards, and frameworks such as

- **European Union (E.U.) General Data Protection Regulation (GDPR):** Highly important for those handling personal data of E.U. citizens, regardless of where the organization is located
- **Payment Card Industry (PCI) Data Security Standards (DSS):** Critical for organizations that handle credit card transactions to ensure secure processing and protect cardholder data
- **United States (U.S.) Health Insurance Portability and Accountability Act (HIPAA):** Essential for healthcare organizations in the U.S. to protect patient health information

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):** Widely adopted across various industries in the U.S. for improving cybersecurity posture
- **U.S. Federal Information Security Management Act (FISMA):** Important for U.S. agencies and contractors to ensure the security of federal information systems
- **U.S. Sarbanes–Oxley (SOX) Act:** Significant for publicly traded companies in the U.S. to ensure financial transparency and prevent fraud
- **The 2021 White House Cybersecurity Executive Order:** Outlines Zero Trust goals, requiring federal agencies to implement Zero Trust in their systems

Countless regulations and standards make it exponentially harder for modern hybrid enterprises to implement necessary security controls and prove their effectiveness, particularly for organizations manually managing shared privileged accounts.

REMEMBER

These regulations and standards embrace the least privilege model as well-established best practices. By implementing least privilege access, Identity-Centric Zero Trust is a solid foundation to fulfill compliance mandates.

IT Modernization and Digital Transformation

Organizations are pursuing digital transformation, akin to moving an office to a virtual data center. This transformation renovates the office for modernity and efficiency. As digital footprints grow, so does the attack surface, making an Identity-Centric Zero Trust strategy essential for deploying new technologies without increasing risk.

These initiatives leverage technologies like behavioral analytics, machine learning (ML), big data, cloud, containers, DevOps Continuous Integration/Continuous Deployment (CI/CD) pipelines, and microservices. Identity security solutions must manage access for humans, machines, services, and application programming interfaces (APIs). This transformation revisits IT infrastructure, workloads, and applications, utilizing Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), and explores cloud-hosted

identity security benefits, such as refactoring apps with containers or microservices, using cloud platform APIs, and managing resources with infrastructure as code.

Things to consider:

- **Identity sprawl:** New cloud services and applications lead to accumulating logins and passwords, making management difficult and increasing credential compromise risk.
- **Identity security:** Digital transformation introduces roles with high access (for example, Amazon Web Services (AWS) management console). Privileged identity management is essential to monitor and control these accounts, preventing insider threats and misuse.
- **Multi-factor authentication:** Adding phone push notifications or Fast Identity Online 2 (FIDO2) authenticators reduces unauthorized access risk.

Secure DevOps

DevOps enhances business agility and reduces software time-to-market but also increases the attack surface and risk. As new technologies support DevOps, identity security becomes more complex. Security and IT operations teams must manage and audit permissions and credentials for numerous identities and system accounts. Traditional methods, involving manual interventions and restrictive controls, hinder development and operations agility.

For many teams, secure DevOps practices are secondary to tasks like writing infrastructure code, fixing build server issues, diagnosing build failures, assisting new developers, and setting up environments. But having identity security solutions in a DevOps environment help to

- **Establish identity assurance:** Consolidate identities, apply MFA, and control access with risk-based factors.
- **Grant least privilege access:** Provide just-enough, JIT privileges and automate privilege elevation requests.
- **Limit lateral movement:** Use access zones, trusted systems, and conditional controls, and minimize VPN access.

- **Audit everything:** Monitor sessions and use AI to analyze recordings for anomalous behavior.
- **Automate for agility:** Discover systems, automate software installation, enroll systems, vault passwords, and provision access.


TIP

Identity-Centric Zero Trust reduces risk by managing machine identities and securing access across the entire enterprise ecosystem, including DevOps environments.

PRIVILEGED REMOTE ACCESS

Delinea Privileged Remote Access provides browser-based, VPN-less sessions with least privilege controls to help IT and security leaders minimize risks and inefficiencies associated with remote access.

As part of the cloud-native Delinea Platform, Privileged Remote Access provides centralized authorization for remote sessions with credential injection to eliminate the exposure of privileged credentials on the endpoint.

By applying context and intelligence to remote access, session monitoring and AI-driven auditing enhance governance and user activity tracking. Unlike traditional methods, Delinea enables efficient, time-bound access with faster provisioning and deprovisioning of remote sessions.

Important capabilities in an identity security solution for both on-site and remote users includes the ability to

- Offer clientless, VPN-less access, reducing risks of traditional VPNs like broad access and vulnerabilities.
- Provide critical asset access for vendors, contractors, and remote workers through federated authentication.
- Enforce MFA to verify user legitimacy and human presence, supporting SAML federated identities.
- Protect credentials via Security Assertion Markup Language (SAML) and automatic rotation, guarding against insider threats and leaks.
- Provide real-time session oversight with termination ability, audit trails, and anomaly detection.
- Analyze sessions for anomalies, enhancing detection of unusual behavior.

IN THIS CHAPTER

- Figuring out your level of maturity
- Benchmarking your progress along the journey

Chapter 3
Assessing Your Current Maturity

Every organization is on its own journey toward Zero Trust. Some accelerate quickly, while others struggle to make progress. In this chapter, you discover a maturity framework to help you chart your course. By understanding the typical stages of implementation, you can create your own roadmap and determine the most effective order for rollout.

REMEMBER

The maturity framework is designed to help you systematically lower the risk of privileged and identity-based attacks, increase business agility, and improve operational efficiency. This step-by-step progression helps you build a strong foundation that supports you as you scale.

The more mature your organization, the more your identity attack surface is under control. As you progress through the phases of the maturity framework, you expand your Zero Trust strategy to include more types of privileged identities. In addition, your approach to achieving Zero Trust becomes more dynamic, automated, and integrated. The journey begins with static policies and controls and becomes more granular and dynamic with each phase. Ultimately, you develop an identity security system that's intelligent and continuously learning.

The maturity framework consists of four levels (from lowest to highest). In this chapter, we cover those levels and the action items to help you evaluate your organization's current state of maturity.

Level 0: High Risk

At the most basic level of maturity, you have little or no technology to help you define, manage, verify, and monitor privileged access. The main characteristics of organizations at this level include the following:

- No accurate and current inventory exists of multi-cloud systems, applications, identities, accounts, groups, memberships, and user activity. With no visibility, you're at risk of unsanctioned (shadow IT or threat actors) assets being created, such as virtual machines, resulting in risk.
- No centralized management of policies governs granular access, authorization, and multi-factor authentication (MFA) across all IT systems and applications, and no comprehensive logical security controls enforce such policies.
- You manually do provisioning, adjusting, and deprovisioning access during Human Resources (HR) joiner, mover, and leaver (JML) processes, interacting with many systems and applications that have inconsistent identity management tooling.
- You locally manage passwords and other credentials on each server. The quality of service (complexity) is generally low, and you don't routinely change passwords. You track and manage them via spreadsheets.
- You can't effectively scope account permissions based on job function and tasks. Administrators routinely use superuser accounts with full rights and can create their own local admin accounts.
- You don't know who has access to what and what privileges they have. Reporting on user access permissions and privileges for audits and incident investigations is spotty at best, requiring manual event harvesting and correlation of user activity across systems and applications.

WARNING

These activities, if performed at all, are manual, effort-intensive, and error-prone, and they represent high risk. Visibility across your identity fabric is limited; you don't know what's out there, whether it's sanctioned and aligns with identity security policy, or how it's being used (or abused). User life cycle management of JML processes is also manual, resulting in inappropriate access, permission creep over time, and orphan accounts persisting after people leave. You don't scope administrative rights to job functions, so full admin rights are the norm. Privileged account passwords are managed manually, rarely changed, and often shared. Little wonder why threat actors are laser-focused on compromising identities as a primary tactic in their playbooks.

Recognizing this level of risk and planning for action leads to Level 1: the foundational phase of maturity.

Level 1: Foundational

A central focal point for any comprehensive identity security program is oversight by chief information security officers (CISOs) and other security leaders. This equates to visibility, taking a thorough inventory across your infrastructure and identity fabric.

At this foundational level of maturity, you're introducing capabilities that give you a solid foundation. The focus here is on visibility and attack surface reduction. Identity security tools automate discovery, giving you visibility into what you have and enabling you to govern, manage, and better control access and authorization.

Organizations at this level of maturity typically have the following characteristics:

- You continuously discover local and domain admin accounts and credentials to provide a central inventory. The scope is all primary systems:
  - Identity providers, such as Active Directory, Entra ID, or Okta
  - Cloud service providers, such as Amazon Web Services (AWS) and Azure
  - Servers, such as Windows and Linux

- Enterprise resource planning (ERP) systems, such as SAP and Oracle NetSuite

- You vault all discovered accounts and credentials. Passwords are automatically rotated on a schedule or after use, and complexity rules are applied. This mitigates the risk of reuse, sharing, and cracking.
- You introduce Identity Lifecycle Management (ILM) for all user changes (JML) driven by authoritative data such as Human Capital Management (HCM). Roles and permissions are centrally managed and applied along with the enforcement of Segregation of Duties (SoD) rules to prevent toxic combinations.
- A secure web portal allows verified employees to access secrets and servers remotely. Granular role-based access controls ensure only authorized users can view and access secrets and servers. This eliminates VPN dependence, simplifies access management, and reduces security risks and VPN costs.
- You secure privileged remote sessions via bastion or jump servers as trusted points of ingress to private cloud-hosted servers. Session activity is recorded for manual review.
- You apply MFA policies to secret access and server login for additional identity assurance and to block illicit bot and malware access attempts.
- Self-service access request workflows allow administrators to request access and elevated permissions, subject to approval. Grants are scoped to the task and temporary, supporting least privilege and zero standing privileges.
- Identity threat protection analyses user activity to detect account-based attacks such as brute-forcing, account takeover, and privilege escalation.
- Identity posture management reports on risk across your identity fabric. You discover and analyze permissions to identify and fix basic security posture issues.

You now have visibility across your identity fabric, effectively managing identities, access, and authorization. A vault becomes your centralized credential management system, securing and controlling access to secrets such as account passwords. It's the main portal through which users access secrets and launch

remote sessions to servers. You centrally manage the life cycle of identities and their associated accounts. You're now able to reduce your attack surface and risk.

Level 2: Enhanced

An enhanced level of maturity goes beyond foundational identity security measures (see the preceding section) that focus on authentication using vaulted secrets. Now, the focus is on intelligent authorization.

Authorization is a crucial control to reduce operational risk and requires modern, lean, adaptive, and intelligent controls facilitated by machine learning to support Zero Trust access. This approach ensures trust and maintains the integrity of authorization controls by utilizing machine learning (ML) capabilities to provide and consume policy insights and recommendations for roles and entitlements.

This is a two-pronged approach:

- One approach is identity consolidation, for example, eliminating unnecessary privileged accounts to reduce your attack surface and giving administrators only one account to access Windows, Linux, and Unix systems. You enhance identity assurance via MFA, which also stops bots and malware.
- The other approach enforces the Principle of Least Privilege by granting administrators minimum rights (zero administrative trust). When the admin needs to perform privileged activities on a server, identity security controls elevate privilege just-in-time (JIT). This elevation targets a specific app or command to prevent unfettered access. It can also require explicit approval, be subject to MFA for identity assurance, and be temporary to avoid standing privileges.

Unified policy management implementing best practices such as OASIS XACML and Open Policy Agent (OPA) ensures a consistent global definition of roles and policies, reducing risk and administrative overhead. Host-level clients enforce these policies, controlling server login and privilege elevation.

An enhanced maturity organization has specific characteristics:

- Expand discovery and vault all passwords, not only those in critical systems and applications. Expand vaulting to include SSH keys.
- Consolidate identities by eliminating unnecessary ones and giving admins one account to access any system.
- Enforce least privilege by giving admin user accounts minimum rights.
- Ensure accountability by only permitting admins to log in with their individual accounts instead of shared privileged accounts so all activities tie back to that user.
- Enable workflows for review and approval of JIT privilege elevation requests. Optionally integrate with external workflow engines such as ServiceNow.
- Automatically revoke elevated permissions on expiration or explicit check-in to avoid standing privileges, sharing, and misuse.
- Incorporate Identity Governance and Administration (IGA) preventive risk analytics to flag inappropriate requests such as access to highly sensitive assets and Segregation of Duties (SoD) conflicts.
- Expand ILM beyond internal users to vendors and contractors.
- Expand privileged remote access to vendors and contractors and support federation to avoid managing third-party accounts.
- Enforce MFA for direct login to servers (versus vault-initiated in the Foundational level of maturity) and when elevating privilege.
- When identifying identity-based threats on business-critical applications, automatically execute remediation actions such as disabling an account or adjusting group membership.
- Expand vaulting, least privilege application launch control, and JIT access request workflows to workstations, vaulting the local superuser account and enabling policies that govern which applications users can run.

- Enable host-based session recording (versus vault/proxy-based in the foundational level of maturity) and real-time session monitoring, with optional integration with Security Information and Event Management (SIEM) solutions.
- Institute regular identity certification campaigns for critical business applications to ensure user access to these apps is reviewed and approved.

Level 3: Adaptive

At this level of maturity, you're addressing key foundational and enhanced capabilities (Levels 1 and 2) that are essential for your business and risk posture. You can now focus on more advanced capabilities around governance, analytics, automation, continuous extensibility, and adaptive intelligence.

Your organization has sufficient maturity to address both vaulting and advanced authorization with privilege elevation while hardening the environment through several initiatives:

- Centralized management of service and app accounts
- Vaulting DevOps secrets
- Enforcing host-based session, file, and process auditing and recording
- Feeding privilege audit logs to a SIEM solution
- ML-based behavior monitoring of privileged account usage to detect threats

Essential characteristics of a mature organization include

- Expanding ILM to all user types, including applications and services
- Expanding ILM to include critical business applications and physical assets on-premise and in the cloud, enabling change control
- Enabling continuous monitoring and risk assessment
- Maintaining a forensic audit trail for all access grants (to what, what level, who granted, and why)

- Enhancing Security Operations Center (SOC) productivity and incident investigations by performing analysis and detection of identity-based threats
- Supporting National Institute of Standards and Technology (NIST) Authenticator Assurance Level 2 MFA for increased identity assurance
- Supporting dual authorization for privileged operations on critical and sensitive systems
- Enabling access and governance reporting and analytics to automatically analyze and assess identity, access, and risk, feeding intel into identity and access certification processes, and enabling review and sign-off for critical business applications
- Establishing credential management for service accounts and dependencies
- Establishing more granular least privilege policies
- Leveraging security designer tools to simulate security changes to critical applications, such as Oracle NetSuite, and running an analysis to identify potential risks
- Leveraging transaction monitoring for tighter controls
- Enhancing conditional access with risk scoring for identities and targets
- Automatically assessing effective access rights for users to understand the actual level of access a user has and enabling tightening of least privilege access to applications
- Leveraging audit data, ML-based analytics, and automation to detect, track, and alert on identity-based misconfigurations and attacks
- Automating responses and remediation for detected attacks
- Post-discovery, automating the onboarding of new managed assets to include installing access control agents, vaulting local privileged accounts, disabling superuser login, enrolling the asset into the identity security platform, and provisioning default policies that allow trusted administrators to manage the assets
- Based on identity posture risk assessment, fixing deep posture issues and privilege escalation paths
- Automatically analyzing recorded session activity to identify anomalous activity

Defining Your "As Is" and "To Be" Security Posture

The goal for every organization should be to adopt the best practices described in the preceding sections. But how do you know what's appropriate? Should you simply strive to implement it all or a subset?

TIP

A gap analysis helps you prioritize. The gap analysis is an evaluation to compare your current ("as-is") state to your desired future ("to-be") state. You may already be aware of high-profile gaps in existing security controls or look for the gap analysis to highlight potential risk areas not currently represented. The gaps pinpoint areas of relative risk and will help you prioritize what to address and when in a phased approach.

To help you evaluate your current ("as is") state, check out the following activities:

- **Take inventory of your attack surface.** Every identity and account can be a potential attack vector. The first step to reducing your attack surface and risk is understanding what you have, including human and non-human user accounts. Start with privileged user accounts, such as local *NIX "root," Windows "administrator," and domain administrators like AD and Entra ID. Also, consider admin accounts for major platforms, including cloud and hypervisor admins (Amazon Web Services [AWS], Azure, Google Cloud) and major enterprise applications like SAP, Salesforce, and Oracle E-Business Suite.

  

  WARNING

  Don't overlook federated identities for third parties. Delve deeper into service and application accounts, accounts used in DevOps Continuous Integration/Continuous Deployment (CI/CD) pipelines, and those embedded in code, big data, and containers. ***Note:*** Your current state of discovery is likely immature, so your visibility into these identities may be limited.
- **Assess your identity security technologies.** Implementing any maturity level without security technologies is nearly impossible. A critical starting point is clearly understanding what types of identity security solutions and workflows are already in place within your organization.

- **Assess your identity security processes.** The JML processes by which you grant, monitor, manage, and remove privileged access should be examined. As you move to the cloud, many existing processes may need to change to accommodate new dynamics and use cases. Some questions to help you assess your current state of security processes may include the following:
  - Who decides who can access your servers or privileged accounts?
  - Do you have disparate processes for different privileged systems (for example, Windows versus Unix and Linux or data center versus cloud)?
  - What entitlement recertification process do you follow to give someone access? To monitor or remove that access?
  - Who manages the user accounts used to access privileged accounts and systems?
  - What process do you follow to validate their identity?
  - What type of credentials are used for privileged access? Static or short-lived tokens?
  - Is this process performed at NIST 800-63 Identity Assurance Level 2? Level 3?
  - What process do you use to handle lost MFA credentials or forgotten passwords?
  - Who monitors the effectiveness of your processes and controls?
  - What process do you follow when you detect abnormal or malicious activity?
  - Who reviews the audit logs or watches the recorded sessions to detect potential threats?
- **Expand to cover the breadth of your attack surface.** While many organizations have some solutions for addressing Zero Trust, they typically haven't applied controls and policies throughout all areas of the organization for all use cases, which is especially difficult in hybrid and multi-cloud infrastructures.

  Consider the following questions:
  - Is your existing authorization solution designed to address modern hybrid cloud scenarios?

- How are you handling privileged access to cloud workloads and containers?
- How are you discovering identities, accounts, roles, policies, and entitlements in your cloud service providers?
- How will you automate authorization controls into your DevOps workflow and pipeline and drive adoption?

- **Identify your maturity level and plan to improve.** Assess the level of maturity that best represents your organization to determine your "as is" state. It's not unusual that your organization may be more mature in one aspect of the maturity framework and less mature in another.
- **Plan your "to be" state.** After you know the gaps in your current maturity, you can develop your vision for a "to be" state, create plans and a realistic roadmap to reach that vision. You don't have to do everything at once. Instead, focus on the actions that have the most impact.
- **Focus on the goal of Identity-Centric Zero Trust.** Instead of blindly implementing solutions, look for technologies that specifically advance the state of Zero Trust in your organization and reduce your risk of identity and privilege-based attacks. Make sure any solution you select helps you progress along the maturity curve at your own pace without having to do any rework.

Chapter 4 explains how to implement Identity-Centric Zero Trust for your organization at each level of maturity.

IN THIS CHAPTER

- Starting with a solid foundation
- Setting up solutions
- Expanding to new use cases

Chapter 4
Putting Identity-Centric Zero Trust into Action

In this chapter, you get started with Identity-Centric Zero Trust and discover opportunities to accelerate your journey. Although the maturity framework is a phased approach, you don't have to strive for 100 percent implementation of all capabilities in phase 1, then 100 percent in phase 2, and so on. Many organizations determine the security policies and controls they implement based on risk thresholds and organizational priorities. However, you should focus on achieving core capabilities in each phase to protect data, systems, and processes that carry the most risk to quickly give you the most value.

Discover and Vault

Organizations new to the concept of Identity-Centric Zero Trust should start by building a strong foundation:

1. **Discover all privileged identities.**

   Include all privileged accounts — human and machine — on-premises and in the cloud.

2. **Centralize your management.**

   Privileged Access Management (PAM) vaults provide a centralized, secure location for managing passwords and other secrets, such as application programming interface (API) tokens, Secure Shell (SSH) keys, and certificates. They create, rotate, and expire secrets and manage the process for users to check them in and out to gain access to IT resources.

REMEMBER

All components of a PAM solution are critical security infrastructure, so ensure your vault has a built-in disaster recovery capability. This ensures you have emergency access to critical systems by replicating data from one vault instance to another, allowing quick access to vital systems if the primary data source becomes inaccessible.

Establishing a secure admin environment

Your vault includes sensitive data and must be highly secured. You want to reduce risk of introducing infections when privileged identities access vaulted accounts and credentials. To accomplish this, you must ensure that access to your vault is only achieved through a clean source.

Therefore, access should only be achieved through approved Privilege Admin Consoles (PACs), including web-based, native client, or thick client access to sensitive systems via a locked-down and clean connector gateway that serves as a distributed local jump box. Distributed jump hosts or connector gateways serve the dual purpose of load balancing in the same network and supporting multiple, different private networks. These connector gateways go where the resources are located: the Demilitarized Zone (DMZ), Infrastructure-as-a-Service (IaaS), virtual private network (VPN), or virtual private clouds (VPCs) within an IaaS environment.

Securing remote access

The beauty of a properly designed admin environment is that it enables remote staff to access resources 24/7 and is perfect for outsourced IT or outsourced development users. Because a secure admin environment handles all the transport security between the

secure client and distributed connectors, it eliminates the need for a VPN. It also enables you to authenticate your internal and outsourced IT users through Active Directory, Lightweight Directory Access Protocol (LDAP), a cloud directory, or even Security Assertion Markup Language (SAML)–based federation, which has the additional benefit of not having to manage the user's account. You can use one or any combination of these identity stores to grant granular, privileged access to resources for business partners and third-party vendors.

Unlike a VPN that gives users visibility to the entire network, this approach places the user on a specific resource with least privilege and privilege elevation, preventing them from moving laterally to other servers without explicit approval. For example, you can provide your most privileged internal IT admins access to as much of your infrastructure as necessary while limiting access by an outsourced team to only the servers and network hardware that their roles require.

In addition, users can securely access resources even when working remotely. For logins outside the corporate network, you can require additional layers of authentication.

Discovering and registering all machines

To properly implement Identity-Centric Zero Trust, you must have complete visibility of domain-joined and standalone Windows, Linux, and Unix systems and their associated local user and service accounts. Domain accounts that are used to launch Windows services and scheduled tasks on infrastructure and systems should also be discovered and managed centrally. Port scanning can discover additional network devices, Windows, Linux, Unix systems, and local accounts for resources not in Active Directory.

Discovery must be performed on an ongoing — ideally continuous — basis to ensure devices and systems are discovered and registered. When systems are removed, decommissioned, or otherwise disconnected from the network, their status must be appropriately updated.

Vaulting shared, local, and alternative admin accounts

To minimize the attack surface, best practices include avoiding shared, local, and personal privileged accounts among multiple people or systems. However, knowing that this approach may not be practical or achievable immediately, you can manage shared privileged accounts through your vault. PAM vaults keep secrets that unlock privileged accounts in an encrypted store, control access to them, and rotate them automatically.

A PAM vault can ensure that only authorized privileged users, including employees and third parties, can check out secrets that grant privileges automatically, based on policies for role-based access controls.

Authorized users can be logged in using shared accounts without knowing passwords, and the vault won't expose them. So, if needed, IT admins can use shared accounts without the risk of password sharing or unauthorized access. In addition, vaults can automatically change the password after use to mitigate the risk of being cracked and reused.

It is essential to understand the fundamental principle behind using a vault. Ideally, you want to prevent routine use of the "keys to the kingdom" including high-risk privileges such as root and administrator, by vaulting them. These shared privileges should only be used in emergency situations. For daily tasks, your admins would log in with privileged accounts tied to their unique enterprise identities for accountability.

Enforcing session auditing and monitoring

Identity-Centric Zero Trust requires a never-trust, always-verify, enforce least privilege approach to security. Session auditing and monitoring support forensic analysis, help enforce Zero Trust, and align with compliance requirements. With session monitoring, you can watch privileged activity in remote sessions in real time and instantly terminate suspicious sessions. Recordings and audit logs provide easy reporting and support investigations for forensic analysis.

Identity Consolidation and Least Privilege Access

Identity-Centric Zero Trust helps you shrink your attack surface by reducing excessive privileges and privilege sprawl. This is a multi-pronged approach that involves consolidating privileged identities and limiting privileges for all identities to only those that are required. Instead of standing privileges, elevated privileges for all identities are granted just-in-time (JIT), with granular, time-bound, just-enough privileges.

Establishing alternative admin accounts

Establishing alternative dash-A admin accounts is a best practice to disassociate admin-level privileges from their email addresses. In addition to administrative tasks that require privileged access, users perform many daily job functions (such as checking email, doing Internet research, and managing service tickets) that don't require privileged access to infrastructure for a large portion of the workday.

REMEMBER

Alternative dash-A admin accounts should be associated with the privileged user but distinct from their other standard user account. These passwords must be vaulted and frequently rotated. No admin roles or rights should be preassigned. Instead, access requests and approvals should be used to elevate access and privileges to be JIT. The PAM vault should initiate login sessions without revealing the account password. and subsequently rotate the password.

Consolidating identities

Managing privileged user identities and associated roles and entitlements is challenging but necessary. The objective is straightforward: Unify management of privileged access to reduce silos and overall complexity and provide a smaller set of unique, fully accountable privileged identities.

Multi-directory brokering allows your PAM solution to act as a bridge from non-domain-joined machines back to your enterprise directory. This capability enables you to leverage the many

benefits that a directory service offers concerning identity management, federated authentication, and role-based privilege management that spans all your platforms.

This means eliminating as many local privileged accounts as possible and consolidating identities across Unix, Linux, and Windows in your global enterprise directory, thereby avoiding a substantial administrative effort as well as the security risks of managing identity silos at every system. Arguably, it's more important to give privileged users a single, unique identity and get them to log in as themselves (that is, using their enterprise ID) versus logging in with a shared account, thereby ensuring better accountability.

TIP

Consolidate Unix and Linux identities under a unique ID in Active Directory or other enterprise directory for centralized identity, role and privilege management, and federated authentication. Doing so can increase IT productivity, lower IT operations costs, and reduce your attack surface.

Enforcing JIT, just-enough privilege

A key element of Identity-Centric Zero Trust is to grant users only the privilege they need to do their jobs. Temporary and scoped assignment of entitlements for what a user can do and which machines they can access is also managed through privilege elevation policies. By defining granular permissions, you can prevent lateral movement. JIT privilege grants users just-enough (least) privilege for only as long as they need to perform a specific job function. Governing access through JIT and just-enough privilege allows access to be temporary and time-bound with request and approval workflows.

Ideally, access and elevation controls should be enforced at the host level, using agents on endpoints, to avoid legitimate users working around a vault or proxy and to ensure protection from bad actors directly accessing systems via backdoor accounts.

Remove local accounts from workstations

You can limit local privileges on workstations so users can't install applications or execute commands unless they're part of a pre-approved allow list. This helps defend against ransomware attacks that target users through phishing or other social

engineering campaigns. Say a user clicks on a nefarious link intended to download malware and execute a malicious application. Without privileged credentials on their workstation, they won't be able to do so unless that application is marked as known and applied to the allow list. Any unknown applications can be sandboxed and reviewed.

Enforcing multi-factor authentication

Multi-factor authentication (MFA) adds protection by ensuring that privileged users are properly authenticated before they're granted access. MFA requires a minimum of two factors: something the user has (such as a hardware token, email account, or smartphone), something the user knows (username, password, PIN, or security question), or something the user is (inherence using a biometric such as fingerprint or facial scan). MFA can also be based on something the user has done — such as expected behavior or the location from which they normally operate.

By requiring a second authentication factor in security policies, attackers can't misuse accounts without possessing the second factor needed to complete the authentication process. This ensures the entity attempting to gain access to critical resources is who they say they are and can effectively stop bots and malware in their tracks.


REMEMBER

The National Institute of Standards and Technology (NIST) Authenticator Assurance Level (AAL) 2 requires possessing and controlling two authentication factors. MFA for privileged access provides flexibility in choosing from a comprehensive range of second-factor authentication methods. These methods include, but aren't limited to, the following:

- Push notification to a smartphone or smartwatch
- One-time passcode servers via Remote Authentication Dial-In User Service (RADIUS) integration to take advantage of RSA SecurID, Duo Security, or Symantec Validation and ID Protection (VIP) Service
- Generating one-time passwords (OTP) delivered via email, text messages, or to a mobile app
- Interactive phone call with security questions

- Existing Open Authentication (OAuth)–based software or hardware tokens
- Fast ID Online (FIDO) Universal Second Factor (U2F) security keys
- Universal Serial Bus (USB) public key infrastructure (PKI) keys
- Smart cards

MFA in the mature organization extends to all users — privileged or otherwise — and is context-based, meaning users may be prompted to log on with an additional factor (such as an OTP sent to a smartphone) under certain conditions, such as logging in from an unknown IP address or device, logging in after a period of inactivity, or logging in from a different geographic region. Mature organizations also implement MFA for privileged access at NIST Authentication Assurance Level 3 (AAL3), which requires a cryptographic hardware authenticator.

Managing non-human identities

In a mature approach, vaulting extends beyond human identities to include secrets used by non-human identities in the cloud and rapid DevOps workflows. The secrets include digital certificates, encryption keys, SSH keys, IP addresses, API keys, and Amazon Web Services (AWS) Identity and Access Management (IAM) credentials.

TIP

Never retain default credentials within scripts and applications or store them in code repositories like GitHub.

Increasing Oversight

Mature organizations establish higher levels of oversight for all processes that relate to Identity-Centric Zero Trust.

Host-based session recording and auditing

In addition to privileged session monitoring via a PAM vault, host-based auditing and auditing ensure identity security controls are working as expected. By extending vault and proxy-based capabilities with a host-based approach, you can

- Ensure that your privileged access policies are enforced and effective even if the vault is circumvented.
- Capture and collect data in a high-fidelity recording of each privileged session on any server across your on-premises and cloud-based infrastructure.
- Store sessions centrally in an easily searchable SQL Server database for a holistic view of what happened on any system, by any or all users, and at any given time.
- Correlate policy data with privileged activity data for consolidated reporting of "who can do what?" with "what did they do?"

Applying intelligent, contextual detection and response

Mature organizations recognize and alert anomalous privileged behavior. With solutions such as Identity Threat Detection and Response (ITDR), machine learning and artificial intelligence (AI) develop a baseline of expected privileged identity behavior under different circumstances and trigger alerts to incident response teams to review when anomalies occur. It automates and orchestrates specific security actions when suspicious behavior is detected, such as increasing logging levels, disconnecting active sessions, and temporarily blocking sessions from an IP address or account.

Integrating with security information and event management

Contextual alerts can also integrate with Security Information and Event Management (SIEM) solutions for real-time correlation and analysis of events across your entire digital footprint, including on-premises and public and private clouds. Privileged access audit logs are a precious resource in risk identification and correlation.

Identifying misconfigurations

Solutions such as Cloud Identity and Entitlement Management (CIEM) and ITDR support oversight by identifying vulnerabilities such as misconfigurations within your cloud platforms. Such solutions identify misconfigurations by continuously monitoring

identities, groups, group access, roles, stale access, and over-privileging. They provide a structured security view for IT and security teams, enabling them to comply with best practices and address issues based on their severity, category, or compliance framework.

Ongoing governance

Solutions such as Identity and Access Governance (IGA) add oversight to your Zero Trust program. Through automated user access reviews and certification campaigns, you can double check that privileged users have the appropriate level of permissions and avoid access creep.

In addition, you can manage privileged identities throughout their life cycle, as users join, move, and leave the organization. That way, you reduce your risk of orphaned accounts, unmanaged credentials, or standing access that can be leveraged by malicious insiders or threat agents.

Identity-Centric Zero Trust in an intelligent, integrated platform

As attackers get more sophisticated, you need to be ready. The most important thing is to select solutions with modular capabilities and seamless integrations, so you can mature without having to redo any work you're already put in.


TIP

You don't have to go it alone. Partner with an identity security provider with an easy-to-use solution that can be deployed quickly for fast time to value. After you get started and prove the case, you can grow your Zero Trust program, reduce risk, and demonstrate measurable results.

IN THIS CHAPTER

- Extending Zero Trust beyond the network
- Enabling Zero Trust for organizations of all sizes
- Implementing Zero Trust one step at a time
- Preventing privileged access abuse
- Moving beyond password vaults
- Taking Zero Trust to the cloud
- Increasing productivity

Chapter 5
Ten Myths about Zero Trust Debunked

In this chapter, we debunk some common myths about Zero Trust.

Myth #1: Zero Trust Is Solely Focused on Networks

Although networks are perhaps the most well-known and best-understood component of the original Zero Trust model defined by Forrester Research, their Zero Trust Extended Ecosystem spans the entire digital ecosystem. Those with limited IT security budgets should prioritize Identity-Centric Zero Trust, even if it means diverting budget away from network security.

Myth #2: Zero Trust Is All Theory and No Practice

The Zero Trust model has evolved from a concept into a security framework with practical guidance for implementing a complete Zero Trust strategy that's being used by a growing number of businesses and government agencies.

Myth #3: Zero Trust Is Only for Large Organizations

No organization is safe from identity-based attacks. Size and budget shouldn't deter you from adopting a Zero Trust strategy. Zero Trust doesn't mean zero-sum regarding your security budget. You can implement Identity-Centric Zero Trust incrementally along with your other security projects to ensure a robust cybersecurity posture for your organization.

Myth #4: Zero Trust Requires "Rip and Replace"

Implementing a Zero Trust security model is really an augmentation of your current security controls. Integrating Identity-Centric Zero Trust within your overall cybersecurity program and IT stack saves time and money. For example, integrations with identity stores like Active Directory and other identity providers, Identity and Access Management (IAM), Privileged Access Management (PAM), Identity Governance and Administration (IGA), and multi-factor authentication (MFA) solutions streamline governance throughout the entire identity life cycle. In addition, integrations with ticketing and incident response systems make it easier to identify attacks and contain the damage.

The myth is believing you can Frankenstein tools together and be effective. Yes, you can do that, and you can achieve some degree of Zero Trust, but a platform-based approach enhances security, improves productivity, and reduces risk and technical debt.

Myth #5: Zero Trust Implementations Take Years

An effective Zero Trust strategy can be implemented in phases as your resources and priorities permit.


TIP

Begin with aspects of your business that carry the greatest risk. Many organizations start with one team or set of IT resources. To simplify operations, you can apply policies to groups of servers that need similar access controls. You can also isolate critical systems into zones and enforce more stringent security policies tailored to sensitive environments.

The most important thing is to select easy-to-use identity security solutions with modular capabilities so you can grow at your own pace without having to redo any work you're already put in. Technology is constantly evolving, so Zero Trust — like many other cybersecurity strategies and initiatives — is more of a journey than a destination.

Myth #6: Zero Trust Isn't Affordable

Identity-Centric Zero Trust can be organized into logical phases, each with various technology options to meet your security and budget requirements. Leveraging existing investments in, for example, incumbent IAM and PAM solutions ensure you get a jump start with rapid time to value.

Myth #7: Zero Trust Is Just Another Buzzword

In reality, Zero Trust is a well-defined security model with concrete principles and practical implementations that organizations of all sizes can leverage to reduce risk and improve security posture.

Myth #8: Zero Trust Privilege Can Be Achieved through PAM Alone

Implementing a PAM solution is an important security measure and an essential component of Identity-Centric Zero Trust, but it only takes you so far.

Building from a vault foundation, Identity-Centric Zero Trust also includes other capabilities of PAM such as capabilities like just-enough, just-in-time privilege policies, privileged session monitoring, secure remote access, advanced analytics, and automation and orchestration. In addition, it includes identity security solutions that are adjacent to PAM, such as MFA, identity federation, IGA, and Identity Threat Detection and Response (ITDR).

Myth #9: Zero Trust Is Limited to On-Premises Resources

Hybrid environments are the norm today, which is why Identity-Centric Zero Trust is essential. Legacy identity security solutions were designed to protect on-premises environments with a well-defined perimeter, not today's porous environment. You must extend Zero Trust to your cloud environments. The rules haven't changed; only the location of your data has.

Myth #10: Zero Trust Limits Productivity

Many organizations worry that implementing a Zero Trust model causes friction in the organization as frustrated users can't get access to the resources they need to do their job. In fact, Identity-Centric Zero Trust enables the opposite: seamless policies that work in the background, automatically evaluating risk and elevating privileges when necessary. When supported by modern solutions, Identity-Centric Zero Trust saves time for IT operations, security analysts, incident responders, compliance teams, and business users.

Securing identities at every interaction

delinea.com

Eliminate breaches due to compromised credentials

An Identity-Centric Zero Trust strategy creates a "never trust, always verify, enforce least privilege" security posture that enables organizations to significantly reduce or eliminate the number-one attack vector for data breaches today: weak or compromised privileged access credentials. In this book, you discover how to assess your organization's current Zero Trust maturity level and plot your road map on the journey to Zero Trust, extending across your entire digital footprint from the data center to the public cloud and the Internet of Things.

Inside...

- Explore the extended maturity framework
- Accelerate your journey to the cloud
- Simplify compliance audits
- Enable secure remote access
- Enforce just enough and just-in-time privilege
- Enable multi-factor authentication everywhere

Delinea

Lawrence Miller is the coauthor of *CISSP For Dummies* and has written more than 150 *For Dummies* books on numerous technology and security topics.

Tony Goulding has more than 25 years of global information security experience and is a frequent speaker on cybersecurity and risk management strategies.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-29089-5
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.