Brought to you by

Delinea

Zero Trust Privilege

for dummies®
A Wiley Brand

Explore Zero Trust Privilege use cases

Assess your Zero Trust Privilege maturity level

Create a road map to Zero Trust Privilege

Delinea Special Edition

Lawrence Miller
Tony Goulding

About Delinea

Delinea is a leading provider of privileged access management (PAM) solutions for the modern, hybrid enterprise and makes privileged access more accessible by eliminating complexity, enforcing Zero Trust, and seamlessly defining the boundaries of access. Delinea simplifies security, ensures compliance and reduces risk for thousands of customers, over half the Fortune 100, and the world's largest financial institutions, intelligence agencies and critical infrastructure companies. For more information, go to www.delinea.com

Zero Trust Privilege

Delinea Special Edition

by Lawrence Miller
and Tony Goulding

for dummies®
A Wiley Brand

Zero Trust Privilege For Dummies®, Delinea Special Edition

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

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-88709-6 (pbk); ISBN 978-1-119-88710-2 (ebk)

Publisher's Acknowledgments

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

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: Matt Cox

Production Editor: Mohammed Zafar Ali

Special Help: Andy Smith

Table of Contents

Introduction

Cyber breaches are bigger and worse than ever. Hardly a day goes by without headlines about some new devastating cyber attack. To better protect against data breaches, the use of a Zero Trust model has returned to the spotlight and seen huge growth in adoption. Instead of using the traditional approach of "trust, but verify," the Zero Trust model implements "never trust, always verify" as its guiding principle.

There are many starting points on the path to Zero Trust. However, all roads still lead to privileged access management (PAM) using identity-based access controls as the lowest-hanging fruit. Hackers don't hack in anymore — they log in using weak, default, stolen, or otherwise compromised credentials. So, until organizations start implementing identity-centric security measures, privileged account compromise attacks will continue to provide a perfect camouflage for data breaches.

Under a Zero Trust Privilege strategy, you implement PAM to strictly govern and control just-in-time privileged access by verifying who is requesting access, verifying the context of the request, and limiting admin rights. This "never trust, always verify, enforce least privilege" approach eliminates implicit administrative trust, providing the greatest security.

About This Book

Zero Trust Privilege For Dummies consists of five chapters that explore the basics of Zero Trust and the emergence of Zero Trust Privilege — what it is, why it's needed, and its benefits (Chapter 1); real-world use cases for Zero Trust Privilege in organizations of all sizes and industries (Chapter 2); how to assess your organization's Zero Trust Privilege maturity level (Chapter 3); how to get started with Zero Trust Privilege (Chapter 4); and the myths and realities of Zero Trust (Chapter 5)

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but we assume a few things nonetheless! Mainly, we assume that you're an IT or security executive such as a chief information officer (CIO) or chief information security officer (CISO), a risk and compliance manager, a system or network administrator, or a network or cloud architect within your organization. As such, this book is written primarily for technical readers with some knowledge of basic identity and security concepts and technologies.

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!

TECHNICAL STUFF

You won't find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! Anything marked with this icon explains the jargon beneath the jargon.

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!

Beyond the Book

We can only cover so much in 48 pages, so if you find yourself at the end of this book, thinking, "Where can I learn more?," just go to `www.delinea.com`.

IN THIS CHAPTER

- » Acknowledging the need for a different approach to security
- » Introducing the Zero Trust framework
- » Getting started with identity
- » Looking at the shortcomings of legacy Privileged Access Management
- » Digging deeper into the details of Zero Trust Privilege
- » Recognizing how Zero Trust helps organizations

Chapter 1 Rethinking Your Security with a Zero Trust Approach

In this chapter, we explain why a Zero Trust approach to privileged access management (PAM) is necessary to address the modern threat landscape, the core tenets of Zero Trust Privilege, and its benefits.

Recognizing That Traditional Security Doesn't Work

The traditional perimeter-based approach to security depends on firewalls, virtual private networks (VPNs), and web gateways to separate trusted users (the "good guys") from untrusted users (the “bad guys”). Despite spending an estimated $143 billion on these types of security technologies in 2021, two out of three enterprises are still breached — at the rate of an average of five breaches per organization in a 12-month period! Clearly, the traditional approaches to security aren’t working.

Unfortunately, things won’t get easier in the future. The attack surface is constantly expanding and can no longer be defined by a logical perimeter. Systems and data that resided inside the traditional data center network perimeter in the past are now being moved into the cloud. In fact, more than 90 percent of organizations are moving workloads to the cloud. At the same time, they’re automating processes with DevOps, storing terabytes of additional data in big data lakes, and what used to be deployed on a single server is now operated in hundreds of containers or microservices. This proliferation of compute and associated cloud storage resources enables greater agility, productivity, and opportunity for an organization — as well as for an attacker.

Organizations need to recognize that perimeter-based security, which focuses on securing systems, firewalls, and networks, provides limited protection against identity- and credential-based threats. Until you start implementing identity-centric security measures, account compromise attacks will continue to provide a perfect camouflage for data breaches.

That’s why it’s important to rethink your security strategy and move toward Zero Trust, which assumes that untrusted actors already exist both inside and outside your network. Trust must, therefore, be entirely removed from the equation.

Creating a New Paradigm with Zero Trust

To effectively address today’s dynamic threat landscape, organizations must discard the old model of “trust but verify” (that’s so ‘80s anyway), which relied on well-defined boundaries that are no longer a reality (like the Berlin Wall). The Zero Trust model was created by Forrester Research in 2010. Zero Trust mandates a “never trust, always verify” approach. Zero Trust awareness and adoption is growing worldwide as evidenced by President Biden’s 2021 Executive Order on Improving the Nation’s Cybersecurity calling for advancing toward a Zero Trust Architecture to help modernize federal government cybersecurity.

TECHNICAL STUFF

The original concept of Zero Trust was a data-centric network design that leveraged micro-segmentation to enforce more granular rules and ultimately limit lateral movement by attackers. Since its inception, the concept of Zero Trust and its benefits have evolved significantly. Nowadays, Zero Trust is being used by organizations to drive strategic security initiatives and enable business decision-makers and IT leaders to implement pragmatic prevention, detection, and response measures.

The biggest evolution of the Zero Trust model has been captured by Forrester Research analyst Dr. Chase Cunningham, who published the Zero Trust eXtended (ZTX) Ecosystem report, which extends the original model beyond its network focus to encompass today's ever-expanding attack surface and the following elements and associated processes:

- **Networks:** Segment, isolate, and control the network.
- **Data:** Secure and manage the data, categorize and develop data classification schemas, and encrypt data both at rest and in transit.
- **Workloads:** Apply Zero Trust controls to the entire application stack, covering the app layer through the hypervisor or self-contained components of processing (in other words, containers and virtual machines).
- **Devices:** Isolate, secure, and always control every device on the network.
- **People (also known as identity):** Limit and strictly enforce the access of users and secure those users. It includes authentication, continuous monitoring, and governance of user access and privileges. Oh, and it's the focus of this book!

Realizing That the Path Toward Zero Trust Starts with Identity

Cybercriminals no longer hack into enterprise networks; they simply log in using weak, stolen, or otherwise compromised credentials. Once inside the target network, they expand their attack and move laterally across the network, hunting for privileged accounts and credentials that help them gain access to the organization's most critical infrastructure and sensitive data.

According to a recent study by Delinea among 1,000 IT decision makers, 74 percent of respondents whose organizations have been breached acknowledged that it involved access to a privileged account. This number closely aligns with Forrester Research's estimate "that at least 80 percent of data breaches . . . [involved] compromised privileged credentials, such as passwords, tokens, keys, and certificates."

So, it makes sense to begin your Zero Trust journey where you can get the most bang for your buck: identity and access management (IAM); and more specifically PAM.

Understanding Why Legacy Privileged Access Management Is No Longer Enough

If compromised privileged credentials are the root cause for most breaches, why not simply vault your privileged credentials away? Well, that approach used to work (and Q*bert used to have cutting-edge pseudo-3D graphics).

Legacy PAM has been around for decades. It was designed back in the days when all your privileged access was constrained to systems and resources located inside your network. System administrators used shared superuser account passwords such as "root" or "administrator" that they would routinely check out of a password vault, typically to access a server, database, or network device. In the relatively "controlled" and "safe" network and data center environments of the past, legacy PAM served its purpose.

However, as described earlier in this chapter, today's environment is radically different and far more hostile. Privileged access is no longer limited to only infrastructure, databases, and network devices. It now extends to the cloud, big data projects, and DevOps automation, as well as hundreds of containers or microservices in hybrid cloud environments instantiating what used to be a single server in a "controlled" and "safe" data center.

REMEMBER

Obtaining logon credentials and escalating access privileges are essential objectives in the cyber-attack cycle. For threat actors, access to privileged account passwords provides the keys to the kingdom.

To effectively counter today’s sophisticated cyberthreats against modern IT environments with their nonexistent “perimeters,” a new paradigm for PAM is needed to establish identity as the new perimeter: Zero Trust Privilege.

Tracing the Emergence of Zero Trust Privilege

Zero Trust Privilege redefines legacy PAM for modern IT. With Zero Trust Privilege, the Zero Trust mantra of “never trust, always verify” becomes “never trust, always verify, enforce least privilege” — whether access is requested from inside or outside the network.

With Zero Trust Privilege, users can request elevated rights just-in-time through self-service workflows. Approvers are provided context — such as the user, resource and roles requested, location, and presence of an identity cookie — to make informed grant or deny decisions. Even with elevated rights granted, MFA is critical for identity assurance to stop bad actors (or bots and malware) using legitimate credentials. Ideally, MFA should be risk-aware, using modern machine learning (ML) and user and entity behavior analytics (UEBA) for even greater assurance.

TECHNICAL STUFF

UEBA is a process that applies algorithms and statistical analysis to detect anomalies in user and entity behavior patterns that may indicate a threat or compromise.

Zero Trust Privilege is designed to handle requesters that are not only human but also machines, services, and applications. Especially for DevOps, embedded passwords in code 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.

By implementing least privilege access, organizations minimize their attack surface, improve audit and compliance visibility, and reduce risk, complexity, and costs for the modern, hybrid enterprise.

PAM must now integrate and interoperate with a much broader ecosystem including Infrastructure-as-a-Service (IaaS) providers like Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, as well as DevOps continuous integration (CI)/continuous delivery (CD) pipeline tools such as Chef, Puppet, and Ansible, and Container solutions such as Docker and Kubernetes (see Figure 1-1).

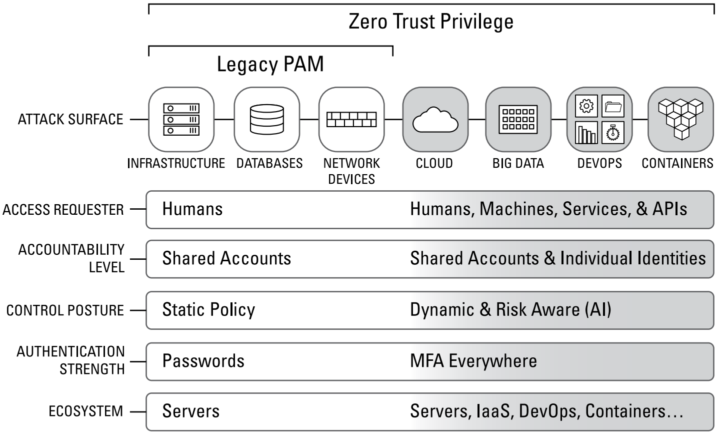

FIGURE 1-1: The shift from legacy PAM to Zero Trust Privilege.

Zero Trust Privilege is built on six tenets discussed in the following sections (see Figure 1-2).

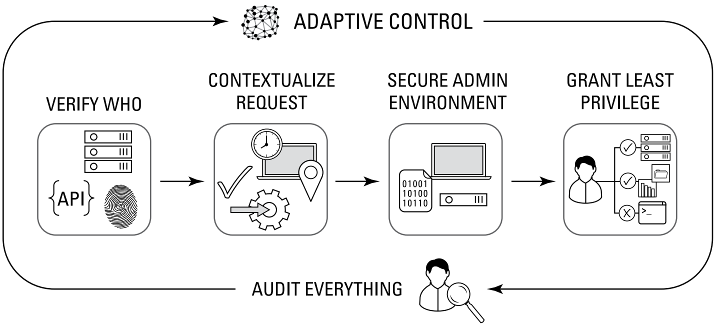

FIGURE 1-2: The six tenets of Zero Trust Privilege.

Verifying who is requesting access

Today, identities include not just people but workloads, services, and machines. Properly "verifying who" means leveraging enterprise directory identities, eliminating local accounts, and decreasing the overall number of accounts and passwords to reduce the attack surface.

Many large organizations use Microsoft Active Directory for directory services. And while Zero Trust Privilege entails utilizing individual identities from an enterprise directory, it doesn't require you to standardize on any particular directory. In fact, you can keep different groups of identities in different directories. The important part is to establish identity for users via enterprise directory identities that are vetted by human resources, meaning these identities are automatically disabled when the person's employment is terminated. The last thing you want is a database administrator (DBA) to leave the organization but still retain his or her privileged access rights. Unfortunately, this is still a common practice as a recent study by Delinea revealed, in which 63 percent of respondents indicated that their companies usually take more than one day to shut off privileged access for employees who leave the company. In an age when insiders are just as much a threat as outsiders, this is unacceptable. Privileged access needs to be revocable instantly.

TIP

A common best practice is to create unique accounts for each administrator to use for administrative tasks that require privileged access. Microsoft suggests creating alternative administrator accounts (commonly referred to as "dash A" accounts because "-A" is frequently appended to the account name) that, unlike the user's regular account, are not published on a business card, LinkedIn, or other public forums.

To verify who, multifactor authentication (MFA) needs to be enforced at all key access control gates, including vault login, password checkout, secret retrieval, server login, and privilege elevation — anytime there is a new request. That doesn't mean though that MFA needs to be invoked every single time. Instead, you want to leverage adaptive/contextual policies that can determine whether additional identity assurance is necessary for that specific access request. Zero Trust Privilege helps mitigate risk by requiring additional proof of identity before granting access, if necessary. MFA is a must-have; passwords are not good enough.

Fortunately, using MFA is as easy as getting a push notification sent to your smartphone and/or touching a Fast IDentity Online (FIDO2) key.

TECHNICAL STUFF

When you're implementing MFA, you should enforce National Institute for Standards and Technology (NIST) Authentication Assurance Level 2 (AAL2), defined in NIST Special Publication (SP) 800-63, at a minimum for admin functions. NIST AAL2 requires "possession and control of two distinct authentication factors": something you know and something you have. A good example is a password combined with a push notification to your smartphone, or a one-time password (OTP) generated by your smartphone. For more sensitive assets, NIST AAL3 is recommended, where possible. NIST AAL3 requires proof of possession of a hardware-based cryptographic token, such as a smart card or FIDO2 key. Those authenticators can then be used in combination with a password or personal identification number (PIN).

Contextualizing the request for access

It makes sense that, for example, a DBA should not have default rights to access all databases. Access should be limited to the databases that the DBA needs to work on in a given day. This way, if the DBA's credentials are compromised, the attack surface is limited. For each request, it's important to know why someone is performing a privileged action. To do this, you must understand the context behind the request for access, and then review and approve the request based on the context provided.

REMEMBER

Least privilege (discussed later in this chapter) and *privilege elevation* go together. Least privilege simply means having minimal rights as your baseline entitlements. You can then request additional elevated rights to perform a certain administrative task and only for the time necessary to perform that task. For example, because you're currently reading this book, you don't need access to your database or cloud management console at this moment — unless you're multitasking! To properly implement least privilege and privilege elevation, the context of the request must be understood to make the appropriate access decision.

The request context typically includes associating the request with a ticket, a user-supplied rationale, as well as what is being requested and for how long. After the request is contextualized, it must then be routed for approval.

TIP

Although just-in-time access request workflows are provided natively by the PAM solution, for larger companies, integration with an enterprise-grade IT service management (ITSM) solution, like ServiceNow, or an identity governance and administration (IGA) platform, like SailPoint Technologies, may be preferred. Access requests can then be initiated from those platforms and, upon approval, fulfilled automatically by the PAM solution.

Securing the admin environment

When connecting to servers with privileged access, you don't want to introduce malware infections during the session. Privileged access must only be permitted from a "clean" source. Zero Trust Privilege means preventing direct access from user workstations that also have access to the Internet and email, which are too easily infected with malware. Internal infrastructure should be isolated from user workstations via a modern cloud jump box. Further, the jump box should be configured as the only trusted device for inbound connectivity.

TIP

Modern cloud jump boxes can serve as distributed connector gateways and are a great way to achieve a secure admin environment for dispersed organizations. In the past, you only had to secure access from inside your network. A properly designed Zero Trust Privilege admin environment not only allows staff to remotely access resources 24/7, but is also well suited for outsourced IT or outsourced development users because it alleviates the need for a VPN and handles all the transport security between the secure client and distributed connector gateways. It also heightens security by not requiring inbound connections, thereby avoiding opening additional firewall ports.

Distributed jump hosts and 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, such as a network Demilitarized Zone (DMZ), IaaS resource, or VPN with private, mutually authenticated connections. These secure connections allow web-based Secure Shell (SSH) or Remote Desktop Protocol (RDP) that works from any location. For outsourced, third-party users, it includes federated inbound authentication, meaning authentication can depend on a partner's directory of authorized employees, providing much higher identity assurance.

Granting least privilege

Least privilege as a concept is more common than you may realize. Think of physical access control at your office: Different levels of users often have different access rights; to enter certain areas, access must be requested and approved. This same concept applies to granting granular role-based access to privileged resources.

Least privilege is critical to limiting lateral movement, which is the primary way attackers get access to sensitive data: They start in one part of the network and move laterally until they find what they're looking for. With least privilege, you effectively stop an attacker's lateral movement by preventing a foothold from becoming a beachhead for further breaches. You'll leave attackers frustrated and singing along with Bono because they "still haven't found what they're looking for."

REMEMBER

Just as no one should have a single key or badge that accesses everything in your office, no one should be allowed to use superuser accounts such as the default root or administrator account on a server — it gives too much access and has no attribution to the actual user. Instead, administrators should be required to log on with an alternative "dash A" administrator account (associated with their unique identity). "Dash A" administrator accounts are still low-privilege accounts: The administrator needs to make a request for additional rights (privilege elevation) to perform privileged tasks. They're also vaulted and their password is managed by the vault so the user can't share the credential with other users or use it directly without oversight of the vault.

Auditing everything

When it comes to privileged access, treat it like the taxman when it comes to the privileged "1 percent" of society: Audit everything!

With a documented record of all privileged access actions performed, audit logs can be used not only in forensic analysis, but also to attribute actions to specific users. A good practice is to integrate audit data with your existing security information and event management (SIEM) system for automated mining so that risky activities can be identified and appropriate personnel alerted. Monitoring (of remote sessions initiated through the vault) and session recording (on both local and remote sessions) is another best practice that can be achieved through gateway- and/or host-based solutions. Host-based solutions ensure that controls cannot be 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 used to search videos for that needle in the haystack.

Providing adaptive control

Zero Trust Privilege controls need to be adaptive to the risk context. For example, even if proper credentials are entered by a user, if the user's behavior deviates from the "norm," then a stronger verification should be required to permit access. Modern ML algorithms are now used to carefully analyze a privileged user's behavior and identify anomalous or unusual (and, therefore, risky) activities and take appropriate action. That might be to deny access and notify the security team or request additional proof of identity via MFA.

Adaptive control requires not only notifying appropriate personnel of risky activity in real time, but also being able to automatically respond by disconnecting sessions, increasing monitoring levels, and/or flagging activity for forensic analysis.

TIP

ML allows companies to pore through millions of events and scan for the "needle in the haystack" on an ongoing and continuous basis, which isn't practical with manual techniques. Even more valuable is performing machine-learning-based analytics inline and in real time, and thus being able to enforce truly adaptive preventive controls and not just after-the-fact detective controls.

Realizing the Benefits of Zero Trust Privilege

In this section, we show you some of the business benefits associated with Zero Trust Privilege so that you can explain to your co-workers why "Zero Trust" is really a good thing for your organization:

- **Breach avoidance:** This is perhaps the most significant and important benefit of Zero Trust Privilege. With 80 percent of breaches involving compromised privileged credentials and as much as one-third of breaches committed by "trusted" insiders, a properly implemented Zero Trust Privilege strategy can help organizations reduce the risk of breach by 50 percent.

- **Compliance:** Stringent data protection regulations and standards (discussed in Chapter 2) impose a complex and confusing array of requirements on organizations of every size, in every industry, around the world. Achieving, auditing, and maintaining compliance is an ongoing and increasingly resource-intensive activity for enterprises. Zero Trust Privilege provides organizations with the visibility they need to ensure continuous compliance.
- **Digital transformation:** According to a February 2019 Forbes article, "Zero Trust Privilege . . . is the force multiplier digital transformation initiatives need to reach their true potential." Zero Trust Privilege enables organizations to accelerate their cloud, DevOps, IoT, and other digital transformation initiatives with confidence.

According to multiple research studies by Forrester, Zero Trust doesn't only reduce an organization's risk exposure; it also leads to an average of $5 million in cost savings related to breaches. In addition, Forrester concluded that Zero Trust allows for newfound business confidence, accelerating partner experiences, empowering mobile workforce models, and securing DevOps environments — which have recently become a focus of many attacks.

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 Zero Trust Privilege Use Case Examples

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

Breach Avoidance

With the realization that compromised credentials are now the number-one attack vector (see Chapter 1), implementing Zero Trust Privilege is clearly an important first step toward significantly reducing an organization's risk exposure.

When a privileged account gets compromised, it allows the cyberattacker to impersonate a legitimate employee or system and carry out malicious activity without being detected as an intruder.

After hackers compromise a privileged account, they can typically roam at will across an IT environment to exfiltrate data, cause damage, and cover their tracks.

Zero Trust Privilege allows you to minimize the risk of a breach by providing security controls throughout the entire cyber-attack life cycle, addressing the common phases of compromise, exploration (for example, via multifactor authentication everywhere, just-enough, just-in-time privilege, access zones, and a secure admin environment), and exfiltration (for example, via host-based auditing and monitoring and machine-learning-based privilege threat analytics).

Because Zero Trust Privilege takes trust out of the equation, there's less of a target for attackers. Even if they get into your network, because privileged accounts are being securely vaulted for break-glass access only and admins are logging in as themselves with least privilege, even if an administrator's account is compromised, there are no associated elevated privileges to leverage for escalation.

Cloud Migration

As organizations increasingly move their workloads and data to the cloud, enforcing a consistent privileged access security model across hybrid environments consisting of public and private cloud resources and on-premises infrastructure is essential. According to a recent report by IDC, worldwide spending on public cloud services and infrastructure grew 21.4 percent year over year in 2020, totaling $312 billion.

Many organizations undertaking cloud migration projects are challenged with extending their existing on-premises security to cloud workloads and ensuring a consistent security "blanket" across the hybrid environment. Zero Trust Privilege provides the keys to reducing risk in the cloud by

- Establishing a single identity infrastructure across on-premises and hybrid cloud environments

- Controlling privileged access, enforcing context-based multifactor authentication (MFA), and managing privilege in your hybrid cloud environment
- Proving regulatory compliance and simplifying root cause analysis and forensic investigation in public cloud provider instances

Compliance

Ever-changing international, federal, state, and local regulations make it increasingly challenging and costly for organizations to achieve and maintain compliance. To reassure customers and the public that sensitive data such as credit card numbers and health records are appropriately protected, organizations in different industries must comply with various government mandates and industry standards, such as the following:

- European Union (EU) General Data Protection Regulation (GDPR)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Plan
- Payment Card Industry (PCI) Data Security Standards (DSS)
- United Arab Emirates National Electronic Security Authority (NESA)
- U.K. Cyber Essentials
- U.S. Federal Identity Credential Access Management (FICAM) Initiative
- U.S. Federal Information Security Management Act (FISMA)
- U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act
- U.S. Health Insurance Portability and Accountability Act (HIPAA)
- U.S. Sarbanes–Oxley (SOX) Act

As a result of this myriad of regulations and standards, it's exponentially harder for modern hybrid enterprises to ensure that they have the proper security controls implemented wherever necessary and to prove their effectiveness, especially in organizations that are manually managing shared privileged accounts. By implementing least-privilege access, Zero Trust Privilege allows organizations to fulfill the most stringent compliance mandates.

IT Modernization/Digital Transformation

Organizations everywhere are modernizing their IT infrastructure and pursuing digital transformation initiatives. As their digital footprints expand to support these initiatives, so does their attack surface. A Zero Trust Privilege strategy is a critical element of any IT modernization or digital transformation project, because it enables the organization to confidently deploy new technologies and capabilities without increasing overall risk to the organization.

IT modernization and digital transformation initiatives take advantage of new and evolving technologies and processes such as behavioral analytics, machine learning (ML), big data, cloud and containers, DevOps continuous integration (CI) and continuous delivery (CD) pipelines, microservices, and more. A Zero Trust Privilege solution must be able to govern and manage access to these technologies and processes not only from humans, but also machines, services, and application programming interfaces (APIs).

Secure Remote Access

With 24/7/365 uptime requirements for practically every organization's network, remote administration is a must for any IT department. Unfortunately, remote access is also a popular attack vector for cybercriminals. The 2013 Target data breach exploited remote access credentials in a heating, ventilation, and air conditioning (HVAC) maintenance system that ultimately led to more than 40 million customer credit and debit card accounts being compromised and $18.5 million in settlement costs alone.

A complete Zero Trust Privilege solution provides your IT administration teams, outsourced IT, and third-party vendors with secure, granular access to critical infrastructure resources regardless of location and without the hassles of a virtual private network (VPN).

Important capabilities in a secure privileged access solution, for both on-site and remote administration, include the ability to

- Grant IT administrators secure, context-aware access to a controlled set of servers, network devices, and Infrastructure-as-a-Service (IaaS) resources.
- Leverage federation technology to support external identity providers (for example, outsourced IT) without needing to add and manage new accounts in Active Directory.
- Control access to specific data center and cloud-based resources without the increased risk of providing full VPN access.
- Secure all administrative access with risk-aware MFA.
- Provide a secure access point for administrators to manage infrastructure using shared accounts or their own Active Directory accounts.
- Enable secure remote access to data center and cloud-based infrastructures for internal users, third-party vendors, and outsourced IT through a cloud service or on-premises deployment.

Secure DevOps

DevOps enables businesses to be more agile and drastically reduce time-to-market for their software applications. However, DevOps processes also create a significant challenge for many organizations because they create a broader attack surface. Prioritizing functional requirements over security requirements while building applications leaves organizations exposed to significant risk.

As companies adopt new technologies, tools, and methodologies to support DevOps, privileged access management becomes increasingly complex. Security and operations teams must manage and audit permissions and credentials for a growing number of user and system accounts in a DevOps environment. Compounding the issue is that traditional methods of securing developer environments involve manual interventions and restrictive controls that significantly restrict the agility of development and operations.

For many teams, implementing secure DevOps practices is just a side job. Their primary focus is on writing infrastructure code, fixing issues with the build servers, helping to diagnose build failures, helping new developers with issues, and getting their environments set up.

Zero Trust Privilege solutions in a DevOps environment help to

- **Establish identity assurance.** Consolidate identities to minimize the attack surface, apply MFA everywhere, and control access through risk-based factors.
- **Limit lateral movement.** Establish access zones, grant access based on use of trusted systems, apply conditional access controls, and minimize VPN access.
- **Grant least, just-in-time privilege.** Grant just enough privilege and move toward just-in-time privilege. In the same way as controlling broad access, automate the request for privilege elevation.
- **Audit everything.** Monitor sessions and analyze the risk of access requests in real time. Receive alerts and notifications on abnormal user access behavior.
- **Automate privileged access management (PAM) technology for agility.** This includes discovery of new systems (including instances in elastic environments) and privileged accounts, PAM software installation, system enrollment, password vaulting, and provisioning default administrative access permissions.

TIP

Zero Trust Privilege reduces risk by managing machine identities and access end-to-end across the entire corporate ecosystem, including DevOps environments and emerging tools and services.

IN THIS CHAPTER

- **Getting to know the Delinea Zero Trust Privilege Maturity Model**
- **Determining where you are and where you want to go with Zero Trust Privilege**

Chapter 3 Assessing Your Current Zero Trust Privilege Maturity

In this chapter, we introduce the Delinea Zero Trust Privilege Maturity Model, which helps organizations better understand and define their ability to discover, protect, secure, manage, and provide privileged access.

Introducing the Zero Trust Privilege Maturity Model

The Delinea Zero Trust Privilege Maturity Model was created to help security professionals assess their organization's ability to prevent the top cause of breaches — privileged access abuse. By using a maturity model for reference, organizations can assess where their Zero Trust Privilege implementation currently stands and where to improve it, working toward a mature level of implementation that allows the organization to maintain a state of Zero Trust Privilege, while dynamically providing necessary access to meet the operational needs of the business.

The model consists of four levels (from lowest to highest): nonexistent, vault-centric, identity-centric, and mature.

Nonexistent

At the most basic level of Zero Trust Privilege maturity (nonexistent), the organization has no technology in place to define, manage, verify, and monitor privileged access. Privileged access accounts consist of static passwords that are not securely stored (for example, in Microsoft Word documents or Microsoft Excel spreadsheets).

Some characteristics of organizations at the nonexistent Zero Trust Privilege level include

- **Identities:** Shared superuser accounts are used for routine privileged access at the user's discretion.
- **Credential management:** Shared static passwords are manually maintained in a spreadsheet or document. They're weak, with limited or no regular password rotation.
- **Multifactor authentication (MFA):** None.
- **Secure admin environment:** None. Server access is permitted directly from local workstations and remote access is through virtual private network (VPN).
- **Session monitoring and auditing:** None.
- **Reporting:** Other than native auditing data, no reporting exists.
- **Just-in-time access request workflow:** None.
- **Least privilege:** None. The superuser admin accounts are the only level of administrative granularity.
- **Least access:** All servers are accessible by the superuser admin accounts.
- **Security configuration management:** If it exists at all, it's limited in scope (for example, local policies on each machine are configured).

Vault-centric

Organizations at the vault-centric level of maturity have password vault technology in place to protect shared, alternative admin, and local admin accounts. Secure admin environments, as well as privileged session management (PSM), may also be in place. You may also have processes in place to support just-in-time access to these privileged accounts.

Some important characteristics of a vault-centric organization include

- **Identities:** The organization uses a checkout model to leverage shared accounts, alternative admin accounts, and local admin accounts.
- **Credential management:** Privileged account passwords are securely vaulted and routinely changed. A checkout facility reveals a password to the user. Alternatively, the vault can establish an Secure Shell (SSH) or Remote Desktop Protocol (RDP) session for a user without revealing the password. Such vault-level activities are audited.
- **MFA:** Vault login, password checkout, and session initiation requires MFA at National Institute of Standards and Technology (NIST) Authentication Assurance Level 2 (AAL2).
- **Secure admin environment:** Distributed jump hosts or privileged admin workstations (PAW) facilitate access to servers, which serve as a "clean source" for admin access.
- **Session monitoring and auditing:** Gateway-based session auditing provides real-time session monitoring, visual session recording, and event logging and reporting.
- **Workflow:** Built-in self-service request workflows enable users to request additional rights to check out passwords, access secrets, and log in to infrastructure resources.
- **Least privilege:** Superuser admin and/or specific-use admin accounts are used via the vault.
- **Least access:** Nothing in place. All servers are accessible by superuser admin accounts that grant unfettered access.
- **Reporting:** The vault provides basic reporting such as "Who has access to vaulted accounts?" and "Who accessed what?" Audit logs from individual hosts require correlation (for example, via a security information and event management [SIEM] tool) with vault logs to determine the exact user performing activities on the host.
- **Security configuration management:** Nothing additional at this level.

Identity-centric

What distinguishes an identity-centric level of maturity is the combination of vaulting and least privilege plus privilege elevation. Instead of routinely using vaulted local privileged accounts, admins use their enterprise IDs with minimum rights. With identity consolidation, local shared and individual privileged accounts are eliminated where possible to reduce the attack surface.

Unified policy management in Active Directory or the privileged access management (PAM) software as a service (SaaS) platform ensures consistent global definition of roles and policies, reducing risk and administrative overhead. Host-level clients enforce these policies, controlling server login and elevation.

These organizations have implemented least privilege through just-in-time temporary assignment of access and privilege elevation and assured identity via MFA.

Specific characteristics of the identity-centric organization include

- **Identities:** Because of identity consolidation, enterprise directory individual and alternative admin accounts are primarily used, with limited use of shared and local accounts. Machine identities are also established for root of trust between PAM and managed servers.
- **Credential management:** Directory-based authentication via short-lived, federated credentials — such as Kerberos, SSH certificates, public key infrastructure (PKI), and Open Authentication (OAuth) tokens — is used.
- **MFA:** At login and at privilege elevation, MFA is required at NIST AAL2 with unified PAM policy enforced on each target server.
- **Secure admin environment:** SAML-based federation is the method of choice especially for third parties. Any remote access is provided by secure web-based remote access without requiring network or virtual private network (VPN) access.
- **Session monitoring and auditing:** Session watch and terminate is provided for supervised or “four eyes” access to sensitive systems.

- **Workflow:** Delegated request and approvals are integrated with IT service management (ITSM) and/or identity governance and administration (IGA) solutions for access as well as privilege elevation.
- **Least privilege:** Privilege elevation with roles and rights is established. Lateral movement between servers is prevented.
- **Least access:** Server zones based on management groups or computer roles are defined to further limit which accounts can access which servers. Access is granted to groups of servers based on role assignments or based on workflow requests.
- **Reporting:** Privileged activity both at the vault and on servers are consolidated along with assigned roles and rights. This provides full visibility into "who can do what," "who approved access," and "what did they do."
- **Security configuration and management:** Methods used in vault-centric levels are used.

Mature

The organization has sufficient PAM maturity to address both vault- and identity-centric levels, while hardening the environment via a number of initiatives, including 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 security information and event management (SIEM) solution; and machine-learning-based behavior monitoring of privileged account usage to detect threats.

Important characteristics of a mature organization include

- **Identities:** In addition to the consolidation of both individual and admin accounts, centralized management of service accounts and application accounts is included.
- **Credential management:** Management of credentials includes auto-managed machine PKI certificates to identify machines.
- **MFA:** Use of MFA includes machine-learning-based adaptive MFA. Sensitive environments align with NIST AAL3 for all MFA, requiring use of a physical second factor.

- **Secure admin environment:** Methods used in both vault-centric and identity-centric levels are used.
- **Session monitoring and auditing:** Host-based session recording is used in conjunction with file and process monitoring. Session auditing streams are integrated with SIEM platforms.
- **Workflow:** Methods used in both vault-centric and identity-centric levels are used.
- **Least privilege:** Fine-grained roles are defined, and role mining and analysis are performed.
- **Least access:** Access is granted only based on a workflow request.
- **Reporting:** Reporting includes detailed privileged user activity captured by each host with identity of the user clearly visible and without requiring any log correlation. Attestation is also possible via integration with IGA solutions.
- **Security configuration and management:** Centralized management via AD Group Policy with local enforcement for Windows and Linux system configurations such as local account control, local group memberships, local SUDOer ("superuser do"), SSH Daemon (SSHD) configuration, and firewall policies.

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

The goal for every organization should be to adopt the identity-centric and mature levels of Zero Trust Privilege best practices described in the preceding sections. To minimize threats — both external and internal — the ideal synergy for an identity-centric Zero Trust approach includes both vaulting and privilege elevation.

The following action items will help you evaluate your organization's current state ("As Is") of security and move toward a higher level ("To Be") of Zero Trust Privilege:

- **Take inventory of your attack surfaces.** You can't protect what you don't know about. So, the first step is to understand where privilege is used within your environment, ideally leveraging PAM discovery tools. Start with the obvious on-premises privileged accounts, but also include service accounts and their credentials, privileged accounts in the cloud, on Infrastructure-as-a-Service (IaaS) hosted systems, and access keys. Then consider (as appropriate) any privileged accounts used as part of your DevOps initiatives, big data, and containers.

- **Assess your security technologies.** It's nearly impossible to implement any Zero Trust Privilege maturity level without security technologies. Having a clear understanding of which technologies are implemented within your organization is a key starting point.
- **Assess your security processes.** The 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 might 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/Linux or data center versus cloud)?
  - What 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/ controls?

  - What process do you follow when you detect abnormal/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.** To properly reduce the threat potential, Zero Trust Privilege technologies and best practices need to be extended to protect the entirety of your organization's environment. To identify potential areas to extend Zero Trust Privilege to, consider the following questions:
  - How are you handling privileged access to cloud workloads?
  - Is your existing PAM solution designed to address modern hybrid cloud scenarios?
  - How will you automate PAM controls into your DevOps pipeline?
  - How are you handling privileged access to container environments?
- **Identify your maturity level and plan to improve.** Assess the level of maturity (discussed earlier in this chapter) that best represents your organization. Keep in mind that your organization may be more mature in one aspect of the model and less mature in another, making it difficult to place your organization firmly in one level of the model.
- **Focus on the goal of Zero Trust Privilege.** The closer you get to Zero Trust — the state at which every access request made requires intelligent scrutiny around granting least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment, with zero access allowed by default — the more mature your implementation will be. Instead of blindly looking to implement a list of technology solutions, the goal is to look for technologies that will specifically advance the state of Zero Trust. The higher your Zero Trust Privilege maturity, the more confident you can be that your organization is protected from external and insider threats and that your security controls are not being subverted. That confidence leads to more agility to transform your business for a new digital generation.

In Chapter 4, we explain how to implement Zero Trust Privilege for your organization at any level of maturity.

IN THIS CHAPTER

- **Getting to a vault-centric Zero Trust Privilege maturity level**
- **Taking the next steps toward an identity-centric solution**
- **Achieving Zero Trust Privilege nirvana**

Chapter 4 Putting Zero Trust Privilege in Action

In this chapter, we describe the steps you can take to get started with Zero Trust Privilege, regardless of where your organization is today on its journey.

Vault-Centric: Discover and Vault

Organizations that are new to Zero Trust Privilege should start with the goal of achieving a vault-centric maturity level. Goals and objectives for a vault-centric organization should include discovery of all machines and privileged accounts, management of and access to admin accounts accomplished via a secure, centralized password vault, and admin sessions routed through a connector gateway with session recording.

Establishing a secure admin environment

When accessing privileged resources, it is vital that you do not introduce infections during your connection session. To achieve this, you need to make sure access is only achieved through a clean source. Thus, access should only be achieved through approved Privilege Admin Consoles (PACs), which can include 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.

The beauty of a properly designed Zero Trust Privilege secure admin environment is that not only does it enable remote staff to access resources 24/7, but it's also perfect for outsourced IT or outsourced development users. Because a Zero Trust Privilege 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, Zero Trust Privilege surgically places the user on a specific resource with least privilege and privilege elevation, preventing them from moving laterally to other servers without explicit approval. In turn, 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 their roles require.

In addition, your IT admins can log in and securely access resources from any location that can reach the Zero Trust Privilege services. For user logins outside the corporate network, you can require multifactor authentication (MFA) for security that is stronger than a username and password.

Discovering and registering all machines

To properly implement a Zero Trust Privilege model, you must have complete visibility of domain-joined and standalone Windows, Linux, and UNIX systems, as well as their associated service accounts. Domain accounts used to launch Windows services and scheduled tasks on infrastructure and systems should also be discovered and managed. For resources not in Active Directory, port scanning can discover additional network devices; Windows, Linux, and UNIX systems; and local accounts.

Discovery must be performed on an ongoing, if not 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

Best practices include avoiding shared, local, and alternative admin accounts to minimize the attack surface of an organization. However, knowing that this approach may not be practical or achievable immediately for organizations, the use of password vaults is considered an essential component of any privileged access management solution. Password vaults keep shared, local, and alternative admin account credentials in an encrypted store and centralize control over access to privileged account credentials, as well as rotate passwords for service, application, and database accounts.

With a password vault, authorized IT personnel, whether internal or outsourced, and third-party vendors can check out passwords for shared accounts for a limited duration. Authorized users can access resources using shared accounts without knowing the passwords, and the vault will not expose the passwords. So, IT admins can use shared accounts without the risk of password sharing or unauthorized access.

In addition, enterprise password vaults can automatically change the password after the checkout expires or simply store the password for future access without changing it.

However, ultimately your objective should be to allow shared privileged account passwords to be checked out for break-glass situations only, otherwise utilizing individual enterprise directory accounts and privilege elevation for normal operating conditions.

Enforcing session auditing and monitoring

Zero Trust Privilege requires a "never trust, always verify, enforce least privilege" approach to security.

Enabling and enforcing session auditing and monitoring is essential for organizations to implement Zero Trust Privilege. Session auditing and monitoring supports root cause and forensic analysis, as well as alignment with many regulatory compliance requirements.

Zero Trust Privilege promotes the usage of supervisory session monitoring and termination, whereby supervisors can watch privileged activity in remote sessions in real time and instantly terminate suspicious sessions. In addition, audit logs provide easy reporting for auditors and support investigations for forensic analysis.

Identity-Centric: Identity Consolidation with Least Access and Privilege

The goals and objectives of an identity-centric organization include reducing the attack surface and aligning with best practices such as Zero Trust and zero standing privileges, by consolidating identities and focusing on implementing least access and least privilege principles. Elevated rights for computers, accounts, and operations are provisioned just-in-time via access requests processed centrally through integrated workflows with IT systems management (ITSM) or identity governance and administration (IGA). MFA is also a best practice in the identity-centric organization for all administrative access.

Establishing alternative admin accounts

Establishing alternative “dash A” admin accounts is a Microsoft best practice adopted by many organizations to disassociate admin-level privileges from their public/business card email addresses. In addition to administrative tasks that require privileged access, these users also 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 typical workday.

REMEMBER

Alternative “dash A” admin accounts should be associated with the user but should be a distinctly separate account from their other end-user account. Their passwords must be vaulted and frequently rotated with high complexity. No admin roles or rights should be preassigned to the admin account. Instead, access request and approval should be used to enforce least privilege and privilege elevation on the account. Login sessions should be initiated by the vault so as not to reveal the account password. Subsequently, the privileged access management (PAM) solution should rotate the password.

Consolidating identities

Managing user identities and their associated roles and entitlements is challenging, but necessary. The objective here is straightforward: Unify identity across all business platforms (Windows, UNIX, and Linux) to reduce silos and overall complexity and provide admins with a single, fully accountable identity.

This aspect of PAM is often neglected. As one of the inaugural capabilities in the PAM macrocosm it’s now considered “table stakes” for any viable PAM solution. It’s not ignored per se; it’s just not leveraged to maximize risk reduction and not given the attention it deserves.

Multi-directory brokering allows a Zero Trust Privilege solution to act as a bridge from non-domain-joined machines back to your enterprise directory. This capability allows you to leverage the many benefits that a directory service offers with regards to identity management, federated authentication, and true role-based privilege management that spans all your platforms. At a basic level, this means eliminating as many local privileged accounts as possible, consolidating identities across UNIX, Linux, and Windows in your global enterprise directory, thereby avoiding the huge administrative effort as well as the security risks of managing identity silos (for example, `/etc/passwd`) 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 (anonymous) account, thereby ensuring better accountability from all your OS and application log and auditing systems.

TIP

Consolidate UNIX and Linux identities under a single unique ID in Active Directory or other enterprise directory for centralized identity, role, and privilege management, as well as federated authentication. By doing so, you can increase IT productivity, lower IT maintenance costs, and reduce your attack surface.

Minimizing break-glass

Ideally, you would remove all shared accounts across your heterogenous environment. However, this may not always be possible. In such cases, you would vault away any remaining super user and application accounts on servers and network devices, both on-premises and in the cloud. As outlined in the vault-centric best practices, modern password vaults allow for authorized users to access resources using shared accounts without knowing the passwords. At the same time, this approach provides controlled, emergency access to privileged account passwords. This so-called break-glass checkout of passwords can, for example, be achieved via a native mobile app enrolled in the Zero Trust Privilege solution. For extra validation, the secured password checkout requires a personal identification number (PIN) or fingerprint scan, and the checkout automatically times out based on per-resource policy.

Enforcing just enough privilege

A key element of Zero Trust is to grant users only the privilege they need to do their jobs. Least privilege access should be enforced at the host level for both login and privilege elevation, to avoid legitimate users working around a vault/proxy and to ensure protection from bad actors directly accessing the system.

It should control access to both privileged accounts and privilege elevation based on roles across infrastructures.

By controlling not only the level of rights a user has on a system, but also what system(s) that user has access to, you can control lateral movement throughout the network. Temporary and scoped assignment of entitlements for what a user can do and which machines she can access is also managed through privilege elevation policy.

Enforcing just-in-time privileged access

Extending the concept of just enough privilege (discussed in the previous section), just-in-time privilege grants users just enough (least) privilege for only as long as they need to perform a specific job function. Governing access through just-in-time and just enough privilege allows access to be temporary and time-bound with request and approval workflows.

Enforcing multifactor authentication

MFA mitigates password risk by requiring a minimum of two factors for authentication: 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). Although less common, MFA can also be based on something the user has *done* — such as normal behavior or the location from which the user normally operates.

By requiring a second authentication factor in security policies, attackers are unable to misuse accounts without possessing the second factor needed to complete the authentication process. This ensures the entity attempting to gain access to critical resources — whether human user or "headless" — 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 possession and control of two different authentication factors.

MFA for privileged access provides flexibility to choose from a comprehensive range of second factor authentication methods. These methods include, but are not limited to, the following:

- Push notification to a smartphone or smart watch
- 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, short message system (SMS)/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

Mature: Hardening of Environments with High Assurance

Within a mature organization, goals and objectives include a focus on hardening the environment and establishing higher levels of assurance around privileged requests. Integration with security information and event management (SIEM) and use of host-based auditing is established to ensure compliance. Credential management expands to include application and service accounts.

Vaulting secrets

In a mature Zero Trust Privilege organization, vaulting extends beyond shared, local, and admin passwords to include digital certificates, encryption keys, and other secrets, such as those typically used by developers in a DevOps context — for example, Secure Shell (SSH) keys, IP addresses, application programming interface (API) keys, and Amazon Web Services (AWS) Identity and Access Management (IAM) credentials.

TIP

Prevent cyber attacks that target application passwords or secrets and streamline operations by eliminating hard-coded, plain text account passwords from scripts and applications.

Centralizing the management of service and application accounts

Management of all privileged credentials, including service and application accounts, should be centralized in an enterprise directory service such as Active Directory. A centralized directory helps to eliminate silos that could lead to compromised credentials. For DevOps purposes, OAuth-compliant servers or services can be configured with a confidential client account within the Zero Trust Privilege solution in order to request access to PAM services, or to obtain OAuth tokens for federated application-to-application authentication.

Enforcing host-based session, file, and process auditing

To harden your session auditing, recording, and reporting capabilities, take a host-enforced approach that ultimately results in better control over privileged access in your environment. By extending vault/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 exactly 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."

The Zero Trust Privilege solution should also alert in real time through SIEM integrations (discussed later in this chapter) and provide out-of-the-box reports for major regulations, such as Sarbanes–Oxley (SOX) and the Payment Card Industry Data Security Standards (PCI DSS), to meet compliance needs.

TIP

Implement host-based auditing to ensure that privileged session recording cannot be bypassed. Audit all privileged session activity at the process level in forensic detail for security review, corrective action for compliance reporting, and to avoid spoofing.

Applying machine-learning-based command monitoring and alerting

Monitoring and alerting at the mature level leverages machine learning to recognize and alert on anomalous behavior through user and entity behavioral analysis (UEBA). Artificial intelligence (AI) automates and orchestrates specific security actions when suspicious behavior is detected, such as increasing logging levels (for example, verbose), disconnecting active sessions, and temporarily blocking new sessions from a specific IP address or account.

Integrating with security information and event management

Integrating Zero Trust Privilege with your existing SIEM enables real-time correlation and analysis of events across your entire digital footprint including on-premises as well as public and private clouds. Privileged access audit logs are an incredibly valuable resource in risk identification and correlation.

Enforcing multifactor authentication

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 a 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.

IN THIS CHAPTER

- Extending Zero Trust beyond the network and evolving into a framework
- Enabling Zero Trust for organizations large and small
- Implementing Zero Trust one step at a time
- Preventing privileged access abuse first and foremost
- Moving beyond password vaults
- Taking Zero Trust to the cloud
- Reducing credential-based breaches and empowering new business models

Chapter 5
Ten Myths about Zero Trust Debunked

In this chapter, we debunk some common myths about Zero Trust. If Big Foot or the Loch Ness Monster are one of the myths holding you back, sorry, but we can't help you!

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, the Zero Trust Extended Ecosystem spans the entire digital ecosystem and includes the following:

- Data security
- Network security

- Identity and access
- Workloads
- Devices

TIP

Read Chapter 1 to learn more about the extended Zero Trust framework.

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

Although the Zero Trust model created by Forrester Research nearly a decade ago was initially focused primarily on network segmentation and least privilege, it has now evolved into a complete framework with practical guidance for implementing a complete Zero Trust strategy for any organization.

In addition, Zero Trust has evolved from being a concept to a security framework that is being used by a growing number of businesses and government agencies. According to IDG's 2021 Security Priorities Study, Zero Trust technologies see steady adoption from 24% (2019) to 35% (2020) and 46% (2021). NIST has also published its Zero Trust Architecture (SP-800-207) prescribing general deployment models and use cases to improve an enterprise's overall information technology security posture.

Myth #3: Zero Trust Is Only for Large Organizations

Google was one of the first organizations to adopt the Zero Trust security model in its BeyondCorp initiative. Although Google is certainly a large target for cybercriminals, the reality is that no organization is safe from credential-based cyber-attacks. With credential stuffing attacks on the rise, almost every organization is a potential victim as attackers attempt to gain unauthorized access to systems and networks. According to the 2021 Verizon Data Breach Investigations Report, 61 percent of breaches involved credential data. Ninety-five percent of small to midsize business (SMB) organizations suffered credential-stuffing attacks and had between 637 and 3.3 billion malicious login attempts through the year. These basic web application attacks were largely against cloud-based servers that were hacked via the use of stolen credentials or brute-force attacks. For any organization, large or small, Zero Trust is vital in countering credential-based attacks.

Obviously, SMBs don't have access to the same financial and cybersecurity resources as large enterprises, but you don't have to be Google to adopt a Zero Trust strategy.

TIP

Company size and budget should not deter you from adopting a Zero Trust strategy. "Zero Trust" doesn't mean "zero sum" when it comes to your security budget. You can implement Zero Trust incrementally along with your other security projects to ensure a robust cybersecurity posture for your organization.

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

Although Google did it, when it comes to implementing Zero Trust, rip and replace is more the exception (that is, Google) than the rule (practically everybody else). The reality is that implementing a Zero Trust architecture is really an augmentation of your current security controls. Zero Trust is a journey to be taken one step at a time — unless you're Google and you can afford a teleporter.

TIP

Use the Zero Trust maturity model discussed in Chapter 3 as a strategic road map to plan your organization's journey to Zero Trust.

Myth #5: Zero Trust Implementations Take Years

You don't have to boil the ocean to get started with a Zero Trust strategy for your organization. An effective Zero Trust strategy can be implemented in phases as your resources and priorities permit. Start with Zero Trust Privilege and expand your Zero Trust initiative from there.

TIP

Use the blueprint provided in Chapter 4 as a step-by-step action plan on how to implement Zero Trust Privilege in your organization.

REMEMBER

Technology is constantly evolving, so Zero Trust — like so many other IT strategies and initiatives — is more of a journey than a destination.

Myth #6: Zero Trust Is Simply Not Affordable

This one simply isn't true! Zero Trust doesn't require a "rip and replace" implementation and should be done incrementally (see the previous two myths). Zero Trust can be organized into logical phases, each with a variety of technology options to meet your security requirements — and your budget requirements. Leveraging existing investments in, for example, incumbent on-premises identity and access management (IAM) technologies such as Active Directory is certainly possible.

Myth #7: The Path to Zero Trust Starts with Data Integrity

Ultimately, cybercriminals are after your data — whether to steal it or to ransom it. So, it makes sense to start on the path to Zero Trust by ensuring the integrity of your data, right? Wrong.

Think about it this way. What is your bank's first line of defense for protecting your money? Is it to verify that the cash it receives and disburses isn't counterfeit or to ensure an accurate account balance? Those are certainly important controls to ensure the integrity of your account, but probably not their first line of defense. Their first line of defense is to verify that you — and only you, can withdraw the money in your account. In other words, verifying the identity of the account owner — not ensuring the integrity of the cash (data) in the account — is the first step.

According to Forrester Research, 80 percent of today's breaches are caused by the abuse of privileged credentials. It only really takes one compromised privileged credential to potentially impact millions — whether it's millions of individuals or millions of dollars. Until organizations start implementing identity-centric security measures, cyber-attacks will continue to take advantage of compromised account credentials to breach data. Thus, the path to Zero Trust should always start with identity.

REMEMBER

Privileged access management (PAM) should be a top priority on your organization's list of security projects.

Myth #8: Zero Trust Privilege Can Be Achieved through a Password Vault Alone

A password vault is an essential component of Zero Trust Privilege and an ideal first step in a PAM maturity initiative, but it's only one component and one step. As discussed in Chapters 3 and 4, a vault-centric organization is still in the early stages of Zero Trust Privilege.

Building off a vault foundation, Zero Trust Privilege includes components such as multifactor authentication (MFA), identity consolidation, just enough, just-in-time privilege, PAM, privileged session monitoring, secure remote access, advanced analytics, and automation and orchestration.

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

Hybrid environments, consisting of on-premises and multi-cloud resources, are the norm today, which is why Zero Trust Privilege is essential. Legacy PAM solutions (discussed in Chapter 1) were designed to protect on-premises environments with a well-defined perimeter and are, thus, ineffective in today's borderless cyberworld.

REMEMBER

You can extend Zero Trust Privilege to your cloud environments. The rules haven't changed; only the location of your data has.

Myth #10: Zero Trust Privilege Benefits Are Limited to Minimizing Risks

As Zero Trust was conceived as a response to the new threat landscape, many people believe that its benefits are primarily focused on minimizing an organization's risk exposure.

Certainly, during the initial rollout of Zero Trust Privilege, risk exposure reduction can be dramatic — 50 percent or more in many cases, according to Forrester Research. Organizations implementing Zero Trust Privilege have also experienced an average of $5 million in cost savings related to breaches.

But it's not all material benefits that organizations can gain. According to Forrester, Zero Trust Privilege also contributes to newfound business confidence, whereby organizations have shown twice the confidence accelerating new partner experiences, felt 66 percent more confident in adopting mobile workforce models, and gained 44 percent more confidence in securing their DevOps environments.

Delinea™

Defining the boundaries of access

www.delinea.com

Eliminate breaches due to compromised credentials

A Zero Trust Privilege 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'll learn how to assess your organization's current Zero Trust Privilege 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 Zero Trust framework
- Accelerate your journey to the cloud
- Simplify compliance audits
- Enable secure remote access
- Enforce just enough and just-in-time privilege
- Enable multifactor 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.

for dummies®
A Wiley Brand

ISBN: 978-1-119-88709-6
Not For Resale

9 781119 887096