

# Conversational Server Access Security

By Derek A. Smith (CCISO, CISSP)



**In this  
book, you  
will learn:**

- Why privileged access sits at the center of cyberattacks today
- Which common privileged threat vectors are creating the most risk to your servers
- How to practically establish a privileged access strategy that includes PAM

**2nd  
Edition**

Sponsored by  
**Delinea**

## Sponsored by Delinea

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies.

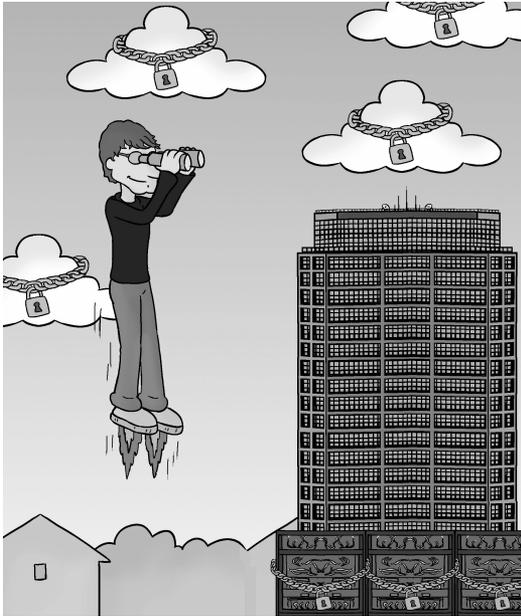
# Delinea™

For more details visit  
[delinea.com](https://delinea.com)

# Conversational Server Access Security (2<sup>nd</sup> Edition)

By Derek A. Smith

© 2023 Conversational Geek



ConversationalGeek®

# Conversational Server Access Security

Published by Conversational Geek® Inc.

[www.conversationalgeek.com](http://www.conversationalgeek.com)

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

## Trademarks

Conversational Geek, the Conversational Geek logo, and J. the Geek are trademarks of Conversational Geek®. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

## Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

## Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at [ConversationalGeek.com](http://ConversationalGeek.com)

## Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Derek A. Smith
Project/Copy Editor:	Pete Roythorne
Content Reviewer(s):	Katherine Vondrak Tony Goulding Barbara Hoffman

## Note from the Author

Thank you for choosing to download this eBook on Server Access Security! Protecting your business from the ever-evolving threat of cybercriminals can seem overwhelming, especially when running your organization demands so much of your attention.

Today, organizations like yours continue to embrace cloud infrastructure – and the speed of this change has been turbo-charged by the pandemic. One of the most challenging side-effects of this is that companies' attack surfaces have increased vastly, and the traditional perimeter no longer exists.

The bad guys know your most critical data resides on servers located on-premises and in the cloud. So, protecting access to those servers has never been more important. But, at the same time, it has never been harder to achieve.

I'm assuming that if you're reading this book, you may already realize quite a lot of this. So, over the next 20-plus pages, I'm going to take a look at how things have changed and provide you with critical insights and recommendations that will help you protect access to your data assets.

Hopefully, this will help make your journey, whether on premise or in the cloud, as secure as it possibly can be.

Derek A. Smith

# Protecting Your Servers in the Age of the Cloud



*“How are we going to secure all this?”*

Today, organizations like yours are reinventing themselves and adjusting business imperatives to support growth. To accomplish this, they are rapidly embracing cloud infrastructure. With this migration to the cloud, your extended enterprise, resulting from cloud transformation and a shift to hybrid cloud infrastructure, increases the risk of cyberattacks because your attack surface is also vastly increasing. Cybercriminals know that your most critical resources and data reside on servers located on-premises and in the cloud. As more organizations moved to the cloud for digitization and

business continuity, cybercriminals quickly took advantage of the inherent complexities in securing cloud environments.

Tactics such as privilege escalation on servers and lateral movement between servers are often employed by these cyber attackers and bots to infiltrate and extract valuable data. According to the MITRE ATT&CK framework, a globally recognized and widely adopted resource for understanding adversary tactics and techniques, lateral movement is indeed a key tactic that is frequently exploited. Therefore, securing access to servers and only granting appropriate privileges becomes a critical aspect of any robust privileged access management (PAM) strategy.



Your Privileged Access Management journey is unique to your organization, but it's vital, as it enables you to reduce your risk of security breaches to servers by minimizing your attack surface.

As IT environments evolve, it's rare for your infrastructure only to be on-premises or in the cloud. In fact, it expands across on-premises and one or multiple clouds. Even after the pandemic, much of your staff still likely remote, adding to the distributed nature of where the infrastructure is and where access is needed. This continues to challenge your IT operations teams to ensure security across this infrastructure. It has become harder to distinguish who is friend or foe by simply examining what's "inside" vs. what's "outside" your perimeter. Why? Because your modern perimeter is now spread across multiple locations and vendors.

Your IT teams are still responsible for SLAs on server maintenance, break-fix, and meeting compliance requirements. They have/had good processes and controls on-prem, but the cloud is different. Your existing security tools and processes may not be designed to accommodate this hybrid cloud model.

In order to safeguard your organization from potential cyber threats, it is essential to allocate a substantial portion of your security strategy and budget to the protection of your servers. Regardless of their location, servers can become prime targets for cybercriminals aiming to infiltrate and acquire sensitive data such as financial records, intellectual property, and more. Failing to prioritize the security of your servers could lead to severe consequences, including widespread data loss, ransomware attacks, and other detrimental outcomes. By dedicating a meaningful and significant part of your security strategy and budget to fortifying your servers, you can effectively mitigate the risks associated with compromised data, safeguard valuable resources such as time, money, and user productivity, and ultimately safeguard your organization's reputation.

Relying solely on native operating system security controls is an ineffective approach that exposes you to significant risks. In today's digital landscape, information holds immense value, and hackers are constantly seeking to exploit vulnerabilities. When your servers lack proper security measures, they become susceptible to various threats, and the consequences of data breaches can be devastating for your entire organization. Neglecting to secure your servers puts you on a perilous path, risking the compromise of sensitive information. Fortunately, this guide is designed to equip you with valuable information and practical tips that will empower you to make well-informed decisions and enhance your security posture. By understanding the necessary steps to secure access to your servers effectively, you can proactively mitigate the dangers associated with inadequate protection.

First, some numbers you should know! I love throwing numbers at you because they really make a point, scare the heck out of you, and stick with you long after you put down this eBook.

2022 was a watermark year for high-profile cyber-attacks, encompassing some of the most daring and costly breaches in data history, with many of these breaches being identity- and credential-based. Most notable among these was the Uber breach (despite MFA protections) due to unencrypted admin privileges and the Okta attack through a third-party identity compromise.

In both cases, the protections in place could not account for human error and the lack of comprehensive security across all identity surfaces. The pattern that emerged was a concerted targeting of identities and identity systems by malicious actors.

The following stats from the 2023 Verizon Data Breach Investigations Report help to establish the pattern of identities being the focus of recent attacks:

- 49% of all breaches involve credentials, whether they be stolen via social engineering or hacked using brute force.
- In social engineering attacks, credentials were the data target in 76% of attacks.
- 74% of all breaches include the human element, with people being involved either via *Error*, *Privilege Misuse*, *Use of Stolen Credentials* or *Social Engineering*.
- 83% of breaches involved external actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

- The three primary ways in which attackers accessed an organization were stolen credentials, phishing and exploitation of vulnerabilities.



According to the Identity Theft Resource Center's 2022 Data Breach Report (released in January of 2023), there were **1,774 data breaches last year**, with 392,180,551 victims.

But here is what is even more vital for you to understand: the potential for misuse or abuse of privilege by insiders, malware, and external threat actors presents considerable cyber risk that is inadequately managed across many organizations.

## How Cyberattacks Impact Your Organization

So, you have seen the stats and know how devastating cyberattacks can be to your bottom line. But maybe you are not sure about how they can impact your organization. The problems caused by cyberattacks can range from minor disruptions in operations to significant financial losses. Regardless of the type of cyberattack, every consequence has monetary or other costs. These attacks may continue to impact your business for weeks, if not months, after the actual event. Here are some of the key areas where your business may suffer:

- Financial losses
- Loss of productivity
- Operational disruption

- Reputation damage
- Decline in stock value
- Loss of intellectual property
- Loss or compromise of customer data
- Legal liability
- Business continuity problems
- Regulatory fines
- Sanctions
- Employee morale
- Cyber insurance denial or premium raise

These attacks are costly, too, the threat of being attacked is genuine, and the stakes are very high. Reaching an all-time high, the cost of a data breach averaged USD \$4.35 million in 2022, and in data breaches where stolen or compromised credentials are involved, the average cost was \$4.5 million.<sup>1</sup>. Besides the direct financial loss, a security breach can also result in negative publicity for your company, damaging your brand and your reputation.

---

<sup>1</sup> IBM Security, *Cost of a Data Breach* (2022)



Cyberattacks can damage your business's reputation and erode the trust your customers have for you. This, in turn, could potentially lead to a loss of customers and a loss of sales.

Even if you are a small business, you are not immune to the devastation of a cyber breach. While Marriott International, Target, Yahoo, and other big-name companies have been at the center of substantial data-breach scandals, small businesses have also suffered, with 43% of cyberattacks aimed at SMBs<sup>2</sup>.

The genuine threat of a cyberattack has caused organizations to spend between 6% and 14% of their overall IT budget on cybersecurity<sup>3</sup>.

Your credentials are hot commodities for hackers, with stolen credentials being the top threat variety in breaches<sup>4</sup>. Once a credential is compromised, privileged access management solutions become most beneficial because you can use them to do such things as rotating your credentials to stop the breach or limit your privileges so that even if compromised, access can be prevented or limited for the compromised credential. In situations such as these, PAM becomes vital, as it enables you to reduce the risk of breaches by minimizing the attack surface.

While workstation PAM can protect the initial point of entry (typically a phished user and compromised workstation), server PAM is critical to protect the servers and prevent lateral

---

<sup>2</sup> Accenture, *Cost of Cybercrime Study* (2022)

<sup>3</sup> Deloitte, *Reshaping the Cybersecurity Landscape* (2021)

<sup>4</sup> Verizon, *Data Breach Investigations Report* (2023)

movement. Privileges are typically in the form of group memberships or device-level permissions that allow the execution of privileged commands. Even if a user is not explicitly given access to a server or workstation, that user's domain or group-level permissions often allow access whenever that person needs or wants it.

The reason our industry has failed miserably at addressing standing privilege is that we struggle to answer three simple questions:

1. What admin credentials exist and have standing access (visibility)?
2. How do you eliminate them (to reduce your attack surface)?
3. How do you protect those you can't eliminate (e.g., "root", "local administrator")?

I will address how to deal with standing privileges later in this guide. For now, let's check out some of the ways cybercriminals can get to your servers and privileged accounts.

## **Common Privileged Threat Vectors**

You have seen the stats, know the threats your privileged user accounts pose to your organization, and know how costly they can be, you must afford them extra attention. You should now be thinking about how you can get ahead of the game so that your organizations won't be among the statistics. Well, , when it comes to securing server access, it's understand the various threat vectors that lead to server breaches so you can take proactive steps to avoid becoming a statistic..



An attack vector is a potential pathway into your sensitive server resources that could facilitate a data breach if exploited.

Here's a comprehensive overview of the common problem areas associated with server access:

- **Over-provisioning your privileges:** Over-provisioning privileges on servers can result in a larger attack surface, making it easier for unauthorized users to gain access to sensitive data. By carefully managing user privileges on servers, organizations can reduce the risk of unauthorized access and limit the potential damage caused by compromised accounts.
- **Protecting a large and complicated DevOps toolchain:** this is crucial for maintaining robust server security. DevOps toolchains encompass a wide range of interconnected tools and processes, making them attractive targets for cyber attackers seeking to exploit vulnerabilities and gain unauthorized access to servers.
- **Lack of awareness of privileged accounts:** Unmanaged privileged accounts on servers can create significant security vulnerabilities. It is crucial to identify and monitor all privileged accounts on servers, ensuring that they are properly managed, regularly audited, and granted only to authorized individuals. This helps prevent unauthorized access and enhances server security.

- **Hardcoded and embedded credentials:** Servers often contain hardcoded or embedded credentials, such as default usernames and passwords. These credentials can be easily exploited by attackers to gain unauthorized access. It is essential to regularly review server configurations, remove any hardcoded credentials, and enforce strong password policies to prevent unauthorized entry.
- **DevOps vulnerabilities:** In the DevOps environment, servers can be exposed to vulnerabilities if plaintext credentials and sensitive data are embedded within code or configuration files. Implementing secure coding practices, such as properly encrypting sensitive data, utilizing secure credential management systems, and conducting regular code reviews, helps mitigate these vulnerabilities and ensures robust server security.
- **Shared admin accounts:** Sharing privileged credentials across IT teams increases the difficulty of tracking activities and maintaining accountability. It is essential to enforce the use of individualized accounts for server access, ensuring that each user has a unique identity. This practice enhances server security by enabling better auditing, monitoring, and control over privileged activities.
- **Inadequate enterprise password management practices:** Weak password management practices on servers can expose organizations to various risks, including credential theft and unauthorized access. Implementing strong password policies, enforcing

password rotation, and using password management tools can help improve server security by reducing the risk of compromised credentials.

- **Reliance on unsupported tools like sudo:** Depending solely on unsupported tools like sudo for server administration can introduce security vulnerabilities. Upgrading to more robust privilege management solutions that offer centralized management, strong access controls, and comprehensive logging and monitoring capabilities strengthens server security and reduces the risk of unauthorized access.
- **Third-party vendor/remote access:** Granting remote access to servers, whether by employees or third-party vendors, requires careful management to prevent unauthorized access and data breaches. Implementing secure remote access protocols, such as multi-factor authentication and encrypted VPN connections, along with strict access controls and regular monitoring, helps ensure that only authorized individuals can access servers remotely, minimizing the risk of security incidents.
- **Workstation security:** Workstation security is a critical aspect of overall server access security. Neglecting to secure workstations can create entry points for attackers to exploit and gain unauthorized access to servers. It is essential to implement robust security measures such as endpoint protection, strong authentication mechanisms, regular patching and updates, and user awareness training to mitigate the

risk of workstation-related vulnerabilities compromising server security.

- **Managing API Keys in software repositories like GitHub:** API keys play a crucial role in authenticating and authorizing access to server resources. However, if not properly managed, API keys stored in software repositories like GitHub can be exposed to unauthorized individuals. It is essential to follow best practices for API key management, including encrypting and securely storing keys, implementing access controls to limit their exposure, and regularly reviewing and rotating keys to prevent unauthorized access and potential data breaches.
- **Focusing on server-related vulnerabilities:** Servers are high-value targets for attackers due to the sensitive data and resources they store. To enhance server access security, it is important to prioritize vulnerability management. This includes regularly scanning servers for known vulnerabilities, promptly applying security patches and updates, implementing strong access controls, configuring proper network segmentation, and conducting regular security audits and assessments. Additionally, employing intrusion detection and prevention systems, robust logging and monitoring mechanisms, and implementing secure coding practices for server applications can significantly reduce the risk of successful attacks on servers.

By addressing these common problems, you can bolster your server access security and reduce the risk of unauthorized access and data breaches. By focusing on server-related

vulnerabilities, you can strengthen your overall server access security posture. Taking a holistic approach to security, encompassing both servers and the workstations accessing them, ensures a comprehensive defense against potential threats, minimizing the risk of unauthorized access, data breaches, and reputational damage.

With privileged threat vectors gaining increased attention, organizations are now placing a stronger emphasis on enhancing server access security. However, despite this growing awareness, many organizations still have significant gaps to address in their privileged security controls. Blind spots, backdoors, and careless practices related to server access abound. The application of cyber risk insurance further amplifies the urgency to maximize server security, reduce the attack surface, and meet compliance requirements.

The integration of cyber risk insurance into the equation adds additional pressure on organizations to fortify their server access security measures. Insurance providers now closely evaluate the effectiveness of security practices and controls implemented by businesses when assessing risk profiles and determining insurance premiums. Inadequate server access security increases the likelihood of successful cyberattacks, leading to potential insurance claims. Therefore, organizations must take proactive steps to bolster server access security and demonstrate robust privileged security practices to insurers.

To meet this challenge head-on, organizations must adopt comprehensive security strategies that specifically focus on server access. These strategies should encompass robust privileged access management protocols, continuous monitoring mechanisms, and adherence to industry best practices for securing server access. By implementing strong server access security controls, organizations can effectively minimize the risk of unauthorized access, prevent server data breaches, and meet the stringent requirements set by cyber risk insurance providers.

In order to delve deeper into the realm of server access security and discover the strategies and insights that will empower you to protect your critical server assets, we invite you to continue reading. By doing so, you will gain valuable knowledge and actionable guidance to navigate the evolving landscape of cybersecurity, safeguard your servers, and fortify your organization against potential security threats.



Privileged access management, security awareness training, an identity-centric security strategy, MFA, strict cloud permissions, and a robust patch management strategy are all efforts you can use to advance your data security.

## How Organizations are Addressing Server Security Challenges

As organizations navigate their cloud roadmap, they are undergoing innovation, modernization, and re-engineering efforts. Amid these transformations, it becomes crucial to prioritize certain key areas. One fundamental shift for many organizations is rethinking their approach to security, as the traditional network perimeter has dissolved due to the adoption of hybrid cloud solutions. In this context, the conveyance and assertion of privileges and entitlements through identities and accounts take center stage, highlighting the critical importance of privilege management.

To advance data security in this evolving landscape, organizations are focusing on several critical measures. These include privileged access management, security awareness training, implementing an identity-centric security strategy, multi-factor authentication (MFA), enforcing strict cloud

permissions, and establishing a robust patch management strategy.

While some vendors argue that identity is the new perimeter, organizations must go beyond mere identity verification and ensure proper authorization levels. This is where privilege management becomes paramount. In fact, privilege itself emerges as the new perimeter, as organizations recognize the need to implement best practices such as Zero Trust. By adopting identity-centric security approaches grounded in the principle of least privilege and eliminating implicit trust in users, organizations can effectively adapt to the changing landscape and bolster their server security.

Having explored the challenges that can arise from inadequate server security and privileged account management, let us now shift our focus to the ways organizations are addressing these concerns. The annual Security and Risk Management Summit by Gartner has consistently identified Privileged Access Management (PAM) as the most significant security project for Chief Information Security Officers (CISOs) to prioritize. This recognition highlights the critical role of PAM in mitigating security risks. Now, let's delve into the actions being taken to address these challenges and explore the measures organizations are implementing in response to evolving security landscapes.

## **Server Security within the Context of Privileged Access Management (PAM)**

Server security is of paramount importance in today's threat landscape, and organizations are increasingly focusing on privileged access management (PAM) as a crucial aspect of their security strategy. PAM involves implementing comprehensive controls and processes to safeguard privileged accounts and mitigate the risk of unauthorized access to critical server resources.

## What is PAM?

Privileged Access Management (PAM) is a set of practices and technologies designed to manage and secure privileged accounts, such as administrator and root accounts, which have extensive access and control over server systems. PAM encompasses various security measures to ensure that privileged access is granted only to authorized individuals, and that activities performed with privileged accounts are closely monitored and controlled.

Within PAM, two important components are Privilege Elevation and Delegation Management (PEDM) and Privileged Account and Session Management (PASM).

PEDM focuses on controlling and monitoring the elevation of privileges for specific tasks or time periods. It ensures that users are granted elevated privileges only when necessary and for the required duration. By implementing PEDM, organizations can enforce a least privilege approach, reducing the risk of unauthorized access and minimizing the potential impact of privilege misuse.

On the other hand, PASM is concerned with managing privileged accounts and sessions comprehensively. It involves controlling and monitoring privileged access to critical systems and resources. PASM solutions provide secure mechanisms to authenticate privileged users, enforce strong access controls, and log privileged activities for auditing and compliance purposes. By implementing PASM, organizations can effectively protect sensitive data, detect malicious activities, and ensure accountability.

Both PEDM and PASM are integral parts of a robust PAM framework. They contribute to the overall security posture by reducing the attack surface, preventing unauthorized privilege escalation, and enabling organizations to enforce strong access controls for privileged accounts and sessions. By leveraging

PEDM and PASM within their PAM strategy, organizations can enhance server security, maintain compliance with regulatory requirements, and safeguard critical assets from unauthorized access and misuse.

## Key Elements of Server Security within PAM

- **Privileged Account Discovery and Inventory:** Organizations need to identify and maintain an inventory of privileged accounts across their server infrastructure. This involves conducting regular audits and assessments to ensure all privileged accounts are accounted for and properly managed.
- **Access Control and Authorization:** Granular access controls should be implemented to restrict privileged access to authorized individuals and specific tasks. Role-based access control (RBAC) can be used to define and manage the permissions and privileges associated with different roles within the organization.
- **Just-in-Time Privilege:** Adopting a just-in-time approach to privilege access ensures that privileged accounts are only granted access when needed and for a limited duration. This reduces the attack surface and minimizes the exposure of privileged credentials.
- **Multi-Factor Authentication (MFA):** Implementing MFA adds an extra layer of security by requiring multiple forms of authentication, such as a password combined with a unique token or biometric verification, for privileged account logins.
- **Session Monitoring and Recording:** Monitoring and recording privileged sessions on servers provide

visibility into the activities performed by privileged users. This enables the detection of suspicious behavior, facilitates auditing and compliance efforts, and supports forensic investigations in the event of a security incident.

- **Privilege Elevation and Delegation:** Implementing secure privilege elevation mechanisms allows users to obtain temporary elevated privileges for specific tasks, reducing the need for continuous privileged access while maintaining necessary functionality.
- **Continuous Monitoring and Threat Detection:** Implementing robust monitoring solutions enables real-time monitoring of privileged activities and the detection of anomalous behavior or potential security threats. Security information and event management (SIEM) tools can aid in aggregating and analyzing privileged access logs for proactive threat detection.
- **Regular Reviews and Audits:** Conducting regular reviews and audits of privileged access controls, user permissions, and activity logs helps identify and address any gaps or vulnerabilities in server security. This helps ensure that privileged access remains aligned with business requirements and compliance standards.

By focusing on these key elements of server security within the context of PAM, you can establish a strong foundation for protecting your servers against unauthorized access, insider threats, and data breaches. Implementing robust privileged access management practices helps maintain the integrity and

confidentiality of critical server resources, reducing the risk of security incidents and safeguarding sensitive data.



MFA is increasingly crucial in server access security, not only for initial login but also for privilege elevation and other privileged events. MFA provides an additional layer of identity verification, ensuring legitimate ownership of credentials and enabling informed decisions on access permissions. Cyber insurance providers often require MFA implementation to mitigate the risk of unauthorized access to privileged resources. By enforcing MFA for privilege elevation and other privileged operations, organizations enhance server security, adhere to the principle of least privilege, and demonstrate their commitment to robust security practices.

It is challenging to manage JIT without an automated solution. Adopting just-in-time as part of your privilege management approach means you can implement a true least privilege model enterprise-wide.

## **Methodologies for Server Access Security Leveraging PAM Capabilities**

When it comes to server access security, leveraging the capabilities of Privileged Access Management (PAM) enables organizations to implement robust methodologies that align with modern security principles. Several methodologies stand out in the context of PAM, including Zero Trust, Just-in-Time (JIT) access, Just Enough Access (JEA), and more. Let's explore

these methodologies and their significance in server access security:

- **Zero Trust:** The Zero Trust approach assumes that no user or device should be inherently trusted, even if they are within the organization's network perimeter. This methodology advocates for strict authentication, authorization, and continuous monitoring of all users and their access requests. By integrating PAM capabilities, organizations can enforce Zero Trust principles by ensuring that privileged access is granted on a need-to-know basis, with strong authentication and strict access controls in place.
- **Just-in-Time (JIT) Access:** JIT access is a methodology that grants temporary and precisely timed access to privileged accounts, reducing the attack surface and minimizing the exposure of privileged credentials. By leveraging PAM capabilities, organizations can establish JIT access mechanisms, ensuring that privileged access is only granted for the required duration when specific tasks need to be performed. This methodology enhances security by reducing the window of opportunity for unauthorized access and limiting the potential for privilege misuse.
- **Just Enough Access (JEA):** JEA is a methodology that limits the permissions granted to users during privileged sessions, allowing them to perform only the necessary tasks and actions required to fulfill their responsibilities. PAM capabilities enable organizations to implement fine-grained access controls, defining the specific privileges and commands that users can

execute during privileged sessions. JEA minimizes the risk of accidental or intentional misuse of privileges and helps organizations maintain a least privilege approach, reducing the potential impact of security incidents.

- **Privilege Escalation Protection:** PAM capabilities play a vital role in protecting against unauthorized privilege escalation attempts. By implementing robust access controls, monitoring mechanisms, and regular reviews, organizations can prevent unauthorized users from gaining elevated privileges on servers. This methodology ensures that only authorized individuals with a legitimate need can escalate privileges, reducing the risk of unauthorized access and potential malicious activities.
- **Continuous Monitoring and Analytics:** PAM capabilities provide organizations with the ability to continuously monitor privileged activities and leverage analytics to detect anomalous behaviors or potential security threats. By analyzing privileged access logs and session recordings, organizations can proactively identify suspicious activities, such as unusual access patterns or privileged commands, and respond promptly to mitigate potential risks.
- **Compliance and Audit Readiness:** PAM methodologies align with compliance requirements and facilitate audit readiness. By implementing strong access controls, session monitoring, and regular reviews of privileged access, organizations can demonstrate compliance with regulations and industry standards. PAM

capabilities provide the necessary tools and functionalities to generate audit reports, track privileged activities, and ensure accountability, which is essential for regulatory compliance.

- **Zero Standing Privilege:** Zero Standing Privilege is a principle that advocates for minimizing standing privileges granted to users, especially for privileged accounts. Instead of providing continuous access, organizations should enforce just-in-time access, granting privileges only when necessary and revoking them promptly afterward. This approach reduces the potential attack surface and limits the exposure of privileged credentials.
- **Fine-Grained Access Control:** Fine-grained access control is the practice of implementing highly granular permissions and restrictions for privileged accounts. It involves defining precise sets of privileges and commands that users can access based on their roles and responsibilities. By leveraging PAM capabilities, organizations can establish fine-grained access controls, ensuring that privileged users have access to only the specific resources and actions required to perform their duties, minimizing the risk of privilege abuse.
- **Temporary Privilege Access:** Temporary privilege access is a methodology that provides time-limited elevated privileges to users when needed. By leveraging PAM capabilities, organizations can implement mechanisms to grant temporary elevated privileges for specific tasks or time periods. This

approach reduces the prolonged exposure of privileged credentials, limiting the opportunity for attackers to exploit them. It ensures that users have access to the necessary privileges when required, without continuously maintaining elevated access rights.

These practices can help you adhere to the principle of least privilege, minimize the potential impact of security incidents, and ensure that privileged access is granted only when necessary and for limited periods. Ultimately, these practices enhance the overall security posture of server access and strengthen the protection of critical resources.



Why PAM? Controlling and monitoring privileged user access to your most critical data and server systems is the best way to prevent attacks. PAM can help your organization protect against accidental or deliberate misuse of privileged access by streamlining the authorization and monitoring of your privileged users.

## Centralized PAM: Harnessing the Power of a Unified SaaS Platform for Optimal Cybersecurity

A unified Privileged Access Management (PAM) platform provides central control, an essential feature if you want to have effective cybersecurity management. With the increasing complexity of technology environments, the sprawl of digital assets, and the sophistication of cyber threats, having a single, centralized PAM system brings numerous benefits.

The most defining features of a unified Privileged Access Management (PAM) platform center around three core elements: *comprehensive visibility*, *simplified administration*, and *consistent policy enforcement*. These pillars are what set a robust PAM platform apart, making it a vital tool for effective security management.

At the cornerstone of such a platform is comprehensive visibility. This feature isn't just an additional benefit, but rather forms the fundamental basis of the PAM solution. By tirelessly monitoring privileged activities across an entire organization's infrastructure, such a system offers unparalleled detection capabilities. The quick identification and response to potential threats substantially diminish potential security breaches' impact. Thus, it's not merely about visibility, but about transforming that visibility into actionable intelligence.

The second element that underscores the significance of a PAM platform is simplified administration. Such a platform transcends the clutter and inefficiency associated with managing different systems from various vendors. Here, the need for navigating through multiple interfaces, complex configurations, and vendor-specific quirks is eliminated. Instead, it provides a singular, streamlined administrative experience that enhances efficiency, significantly reduces the risk of misconfigurations, and simplifies the complexity of the security infrastructure. This is not merely a convenience, but a crucial feature that reduces vulnerabilities at the root.

The last but equally essential aspect is the provision for consistent policy enforcement. An effective PAM platform doesn't just manage access policies, it enforces them uniformly across the organization. Where there can be discrepancies, loopholes, or overlaps in policies with different systems, a unified platform eradicates these potential security risks. It ensures all access is governed by the same rules, effectively reducing the attack surface. Hence, it's not just about

managing access, it's about maintaining control with unwavering consistency.

A high-performing PAM platform emphasizes these three elements as its most significant aspects, providing a comprehensive, simplified, and consistent security solution. The 'bolting' approach, using various products from different vendors, often leads to inefficiencies and potential security gaps. Integration between disparate systems can be challenging and time-consuming, often leading to suboptimal results. A single PAM platform, in contrast, provides seamless integration and functionality, designed to work together out of the box, eliminating the challenges associated with the bolt-on approach.

A centralized Software-as-a-Service (SaaS) PAM platform goes a step further, providing all the benefits of a unified platform while also offering the advantages of cloud-based solutions. These can include scalability to meet changing demand, automatic updates for always staying current with the latest features and security updates, and reduced maintenance requirements compared to on-premises solutions.

In addition, a SaaS PAM platform can offer improved accessibility for remote or distributed teams. As more organizations adopt hybrid or fully remote work models, this kind of flexibility becomes increasingly valuable. All these features can enhance the agility and resilience of your organization's security infrastructure.

A single, centralized PAM platform, particularly when delivered as a SaaS solution, offers significant advantages over a bolted-on multi-vendor approach. It provides enhanced visibility, consistency, and efficiency while simplifying administration and improving accessibility, all of which contribute to a more robust and effective cybersecurity posture.

## "Cyber insurance and the Cost-Benefit Impact of a PAM Solution"

In today's digital age, Cyber insurance has become a necessity for businesses of all sizes. As a matter of fact, according to the Gartner report, *Reduce Risk Through a Just-in-Time Approach to Privileged Access Management*, "By the year 2025, 75% of cyber insurance providers will mandate the use of JIT PAM principles."

Cyber insurance helps protect organizations from the financial implications of cyber threats such as data breaches, network damage, and business interruption. However, the premiums for such insurance can be significant, and insurers carefully evaluate an organization's cybersecurity posture when determining these costs. Implementing a Privileged Access Management (PAM) solution can play a critical role in this regard.

Insurance providers consider a variety of factors when pricing a policy, including the robustness of a company's cybersecurity infrastructure and the effectiveness of its risk management strategies. A well-implemented PAM solution indicates a strong security posture and a proactive approach to managing cyber risks.

A PAM solution demonstrates to insurance providers that your organization has a system to control, monitor, and manage privileged access, significantly reducing the risk of unauthorized access and data breaches. By effectively implementing the principle of least privilege, minimizing the attack surface, and providing comprehensive audit trails, a PAM solution can drastically lower the chances of a successful cyberattack, which is a key consideration for insurers.

Furthermore, a centralized PAM platform provides insurers with the visibility they require. It allows for easy demonstration of compliance with best practices and regulatory standards, which is a critical factor that insurance providers consider. Not only can this result in lower premiums for you, but it can also simplify the process of acquiring or renewing a policy.

Additionally, the proactive threat detection and mitigation capabilities of PAM solutions can be beneficial in an insurance claim scenario. Should a cyber incident occur, your effective PAM solution can provide valuable forensic data, enabling you to prove you took all reasonable steps to protect your systems, which can help with successful insurance claims.

Finally, a robust PAM solution can favorably impact your cyber insurance negotiations. By demonstrating strong cybersecurity practices and risk management, you can potentially reduce your cyber insurance premiums and simplify the policy acquisition or renewal process. In this way, investing in a PAM solution not only strengthens your cybersecurity but can also lead to tangible financial benefits.



### **How to secure your server infrastructure**

- Step 1:** Discover all servers and local privileged accounts
- Step 2:** Bring servers under centralized PAM management
- Step 3:** Consolidate identities and vault the rest
- Step 4:** Enforce least privilege and MFA at the server
- Step 5:** Manage and record privileged sessions

## Strategies and Recommendations for Securing Your Servers

Having discussed the importance and challenges of securing access to servers and examined various protection methods, it is now time to delve into recommended approaches for addressing these challenges. As your organization seeks to proactively protect its distributed server infrastructure, it is crucial to evaluate your business needs and available options, and determine the optimal solution based on best practices. Your server security process should be ongoing, with continuous evaluation and adjustments to enhance security as your business and threat landscape evolve.

It is important to note that there is no single "silver bullet" technical solution that can magically mitigate privileged access risks. Instead, a holistic approach that combines multiple technologies is necessary to safeguard against numerous entry points that attackers may exploit. To achieve comprehensive protection, it is crucial to bring together the right tools for each aspect of the job.

One recommended approach is to adopt a unified threat management (UTM) solution that covers all aspects of your threat landscape. A UTM solution integrates various security functionalities such as firewall, intrusion detection/prevention, antivirus, data loss prevention, and secure web gateways into a cohesive system. This unified approach provides a centralized and streamlined security management experience, enabling efficient monitoring, detection, and response to potential threats.

Additionally, implementing a robust Privileged Access Management (PAM) solution is vital for securing privileged accounts and minimizing the risk of unauthorized access. PAM solutions provide capabilities such as privileged account discovery, access control, session monitoring, and just-in-time access. By implementing PAM, organizations can enforce least

privilege, control privileged access, and detect suspicious activities related to privileged accounts.

Furthermore, it is crucial to prioritize regular patch management and vulnerability assessments for your server infrastructure. Keeping servers up to date with the latest security patches helps protect against known vulnerabilities and reduces the likelihood of successful attacks. Conducting regular vulnerability assessments enables you to proactively identify and address potential weaknesses in your server environment.

Additionally, security awareness training for employees is essential to cultivate a security-conscious culture within your organization. Training should cover topics such as secure password practices, social engineering awareness, and the importance of reporting suspicious activities. By empowering employees with security knowledge, organizations can effectively mitigate the risks posed by human error and insider threats.

Lastly, ongoing monitoring and incident response capabilities are critical for detecting and responding to security incidents in a timely manner. Implementing security information and event management (SIEM) solutions, along with intrusion detection systems (IDS) and intrusion prevention systems (IPS), enables continuous monitoring of server activities, detection of anomalous behavior, and quick response to potential threats.

In summary, securing your servers requires a multifaceted approach. By combining these strategies and continuously adapting your security measures, you can significantly enhance the security of your servers and mitigate risks effectively.

## **Putting the Right Tools in Place**

PAM technology controls elevated (privileged) access and permissions for users, accounts, processes, and systems. So

overall, the best solution is to use PAM/PEDM tools to help reduce risks associated with external attacks, insider threats, and third-party access. While PAM solutions help automate the granting and revoking of privileged access, successful implementation depends on a careful approach that considers the following questions:

- Who (or what kind of user) is appropriate for each type of privileged access in my environment?
- What kind of access is appropriate for my enterprise?
- Where are the boundaries of the access?
- When is the access appropriate for my users?
- Why is access necessary in the first place?

Once you have answered these questions, you can use five key elements to start on the path to successfully secure your privileged access.

## **1. Establish a solid privileged account discovery process**

To prune unnecessary accounts and precisely define which accounts and users have access to vital assets, it is crucial to track every instance of privileged access, be it on-premises or cloud-based. This encompasses both conventional and non-conventional accounts leveraged by individuals - including personal, shared, and administrative accounts such as local administrator and root - as well as by software.

With systems, applications, and accounts undergoing continual updates, the establishment of a persistent discovery process is vital. This process also proves instrumental in identifying unsanctioned "rogue" or "shadow IT" servers. Such elements could pose a potential risk or indicate an ongoing attack, hence

their early detection is of paramount importance for preemptive action and risk mitigation.

Integration of discovery tools from PAM vendors with supplementary controls can further enhance this process. It is advisable, at the very least, to utilize an IT Service Management (ITSM), Security Information and Event Management (SIEM), Identity Governance and Administration (IGA), authentication, DevOps tools, and ticketing systems. This approach creates a layered security architecture that fortifies the privileged access landscape while providing a broad overview of potential vulnerabilities and security threats.

## **2. Develop an automated privileged account password policy**

Establishing a clear and comprehensive password policy is an integral component of managing privileged accounts. Such a policy needs to be easily understandable and agreeable to everyone who uses and manages these accounts. The development of a privileged account password protection policy that encompasses both human and non-human accounts is fundamental to prevent unauthorized access and demonstrate regulatory compliance.

However, just having a policy isn't enough. It's equally important to complement this with automated password management. Privileged Access Management (PAM) controls streamline this process while offering robust security. They not only facilitate the automatic randomization, management, and vaulting of passwords but also empower the automatic and simultaneous updating of all privileged account passwords.

Crucial to this mechanism is the ability of a PAM vault to rotate passwords on a schedule. Regular and automated password rotation significantly minimizes the window of opportunity for

attackers and keystroke loggers, thus bolstering overall security.

Equally significant is the creation of unique passwords for each account. By ensuring that no two accounts share the same password, the threat surface is considerably reduced. This diminishes the potential damage from a single compromised password and adds an additional layer of security, making the password management system not only efficient and reliable but also far more resilient to breaches.

### **3. Implement least privilege**

To mitigate the risk of adversaries infiltrating critical systems or accessing sensitive data, it's crucial to bestow users with only the bare minimum privileges required for their roles. This is where the implementation of the principle of least privilege comes in, ensuring that access rights are limited strictly to what is necessary for specific tasks.

When individual accounts necessitate the capability to execute privileged tasks, Privileged Access Management (PAM) solutions can facilitate the process. These tools enable access that is precisely confined to the scope and duration required to accomplish the given activity, subsequently revoking that access once the task is completed.

A critical aspect of this implementation, however, is preventing lateral movement between servers. Even with minimal privileges, users with access to multiple servers can become a potential risk if an attacker compromises their account. It's therefore essential to eliminate full local administrator access to servers, thus limiting the potential for lateral movement and further fortifying the security infrastructure.



To minimize risk, you should enforce two key principles:

- 1. Separation of duties** – No employee can perform all privileged actions for a given system or application.
- 2. Least privilege** – Employees are granted only the bare minimum privileges needed to perform their jobs.

#### **4. Monitor accounts with analytics**

Privileged user behavior analytics solutions can help you gain insight into privileged activity with a behavioral baseline based on machine learning algorithms that consider user activity, account behavior, access behavior, credential sensitivity, and similar user behavior. Your PAM should allow you to analyze user behavior and produce a risk score that PAM can then use to govern access.

#### **5. Choose the right solution**

Numerous PAM technology providers have varying features and deployment options. Before choosing, it's important to define your use cases for privileged access in your environment and preferred solution capabilities, such as service account management, discovery functions, asset and vulnerability management, analytics, file integrity monitoring, SSH key management, and more.

Professional security assessments can help you successfully deploy your selected solution by identifying what your privileged accounts are protecting and objectively detailing current security policies, controls, and processes. Leverage a vendor partner to help you test and evaluate potential solutions and help you implement your PAM solution.

I recommend opting for a single, trusted vendor offering a comprehensive, SaaS-based PAM solution. This type of platform provides the advantage of a holistic approach to privileged access management, combining all necessary components into a seamless, cloud-based service.

With the heritage of building secure technology that businesses can rely on, such a vendor will ensure a high degree of trust and dependability. A SaaS PAM platform also offers the benefits of regular updates, easy scalability, and lower upfront costs, making it an attractive option for organizations of all sizes.

Ultimately, a modern, SaaS PAM platform can enhance your security posture by providing advanced, integrated solutions that adapt to the dynamic nature of cybersecurity threats.

## **How to Reduce the Risk of Cyberattacks**

Finally, I want to provide you with some quick tips you can use as part of your server security program, along with the PAM solution you choose.

- Be familiar with your industry's compliance regulations and best practice frameworks like Zero Trust.
- For strong PAM maturity, adopt a credential vault that works seamlessly with your chosen Server PAM solution. but remember it's only one piece of securing access across your organization.
- Ensure that you can discover and see all the local and server privileged accounts across your environment, no matter where they are (on-premises or in the cloud) or what OS they utilize.

- Understand the security measures you adopt across your servers. Remove excessive privileges from user accounts, enforcing a least privilege model. Eliminate as many local privileged accounts as possible. Vault your remaining local privileged credentials, strictly control access to them, and rotate them regularly.
- Make managing access to resources across your hybrid cloud easier for your team by:
  - Using individual (not shared) enterprise credentials to provide access – whether AD, LDAP, or a cloud identity provider – and even better if you can work with a vendor that can help bridge multiple directories if required in your environment to ensure one consistent set of identities for authentication and authorization.
  - Removing standing privileges wherever possible.
- Establishing robust processes for consistent privileged access, including user self-service workflows and third-party integrations. It's crucial to institute comprehensive processes that consistently provide the appropriate access level for necessary activities, irrespective of the server's operating system or location. Self-service workflows allow users to request and receive elevated access when needed, enhancing efficiency while retaining tight access control. Additionally, third-party workflows, such as ServiceNow, can streamline access management and add an extra layer of auditability, fostering greater transparency, efficiency, and security.

- Ensuring your PAM solution can integrate with enterprise governance tools that adjust privileges when users are onboarded, offboarded, or when their role changes.
- Implementing additional security as necessary – like MFA at server login and server elevation.
- Enforce a least privilege policy – but provide as little friction for users as possible by:
  - Providing password-less access using enterprise credentials – this allows IT staff to access systems using their normal account and not have to track multiple credentials or constantly go into the vault.
  - Enabling adaptive authentication that uses context and/or historical behavior to determine the risk to better detect and alert on anomalous activities. For example, if low – permit single sign-on for minimum user friction. If medium – ask for additional proof of identity via MFA. If high, deny access, disable the account, and alert IT security.
  - Using a browser-based portal that enforces RBAC and eliminates the need for local SSH or RDP clients or a VPN for secure remote login to servers – whether on-premises or in multiple VPCs and multiple clouds. Record all remote privileged sessions for future reporting and investigations as needed.

As more servers and workloads are moved to the cloud – different teams may be responsible for on-premises servers vs.

servers hosted within public cloud provider environments – it's critical to collaborate and utilize the same technologies and processes to consistently manage access to resources.

# The Big Takeaways

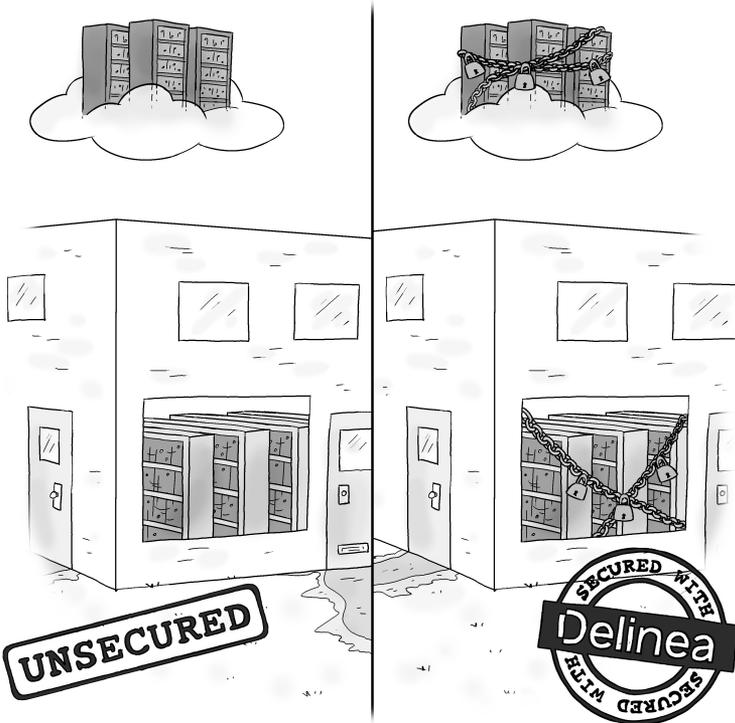
More and more companies are adopting the public cloud quickly because they need their speed and agility to be competitive and innovative in today's fast-paced business landscape. The problem is that many of these companies fail to adopt a holistic approach to security for both their in-cloud and on-premises servers, opening them up to undue risk.

The demonstrated focus on privileged credentials in cyberattacks makes it clear that organizations also must have mitigating controls in place that ensure privileged access remains under control and that the use of privileged credentials is only accessible to sanctioned users within the organization.

The use of a PAM solution helps establish the needed controls around privileged access to effectively protect servers – and the valuable data they contain – from threat actors. Through controls such as removing standing privileged access, securing access to privileged credentials within a vault, and using Just in Time privileged access, PAM creates a hostile environment for threat actors where no accessible credentials have the needed levels of privilege needed to assist in carrying out malicious threat actions.

I hope this guide has provided you with ideas that can help make your choice for the best server and privilege access solutions easier.

# Maintaining Server Access Security with Delinea



Protecting your business from the ever-evolving threat of cybercriminals may seem overwhelming, especially when simply running your organization demands so much of your attention. Fortunately, maintaining your server access security can be seamless with Delinea's Server PAM solutions.

If you are unfamiliar with Delinea, they are a cybersecurity provider created in 2021 via a merger between two cybersecurity industry leaders, Thycotic and Centrify. What

makes them unique is that Delinea believes in building secure solutions by design. They understand the user and focus on building tools that make security seamless for the modern, hybrid enterprise. Their solutions empower organizations to secure critical data, devices, code, and cloud infrastructure to help reduce risk, ensure compliance, and make security easy to manage. Their intuitive user interface removes complexity and clearly defines access boundaries for thousands of organizations worldwide.

## **Your Server Security Challenges Answered**

Delinea's answer to your server security challenges is their Server PAM Solution. This modern PAM solution is purpose-built to address challenges across multiple fronts – risk, cost, productivity, and compliance.

Delinea's Server PAM secures and consolidates identity access to improve productivity; manages privileges and protects against cybersecurity. It controls privileged access to servers in both on-premises and cloud/multi-cloud environments and allows humans and machines to seamlessly authenticate with passwordless login, enforcing least privilege with just-in-time privilege elevation, preventing lateral movement, increasing accountability, and reducing administrative access risk.

Server PAM protects servers by:

### **Centrally managing identities**

Server PAM centrally manages and simplifies login, execution, and multifactor authentication (MFA) policies in Active Directory (AD) or from cloud identity providers. All this can be done using a single enterprise identity for user login, eliminating local privileged accounts and the risk they pose to your business.

## **Minimizing cyber risk with best practices**

Server PAM removes implicit trust for privileged access by aligning with regulations and best practices such as Zero Trust and zero standing privileges to protect against ransomware and data breach attacks. Privileged activity on each server is captured and tied to an individual for full accountability.

## **Following least privilege guidelines**

Server PAM provides role-based access control (RBAC) at the host level for fine-grained control and privilege elevation. System administrators can request access and elevated privileges through built-in self-service workflows.

## **Enforcing adaptive MFA**

Server PAM uses Multi-Factor Authentication policies enforced at login and application execution across Windows and Linux to provide stronger identity assurance and cyber risk insurance demands. Multi-Factor Authentication ensures the user is legitimate, blocking bots and malware and preventing lateral movement.

## **Improving security and compliance**

Server PAM captures all privileged activity on the server for full accountability, access granular audit logs, reports, and visual session recordings to aid compliance and incident response.

## **A Server-first Approach to PAM**

Delinea's Server PAM solution can solve all your server access problems mentioned throughout this guide. As a modern enterprise embracing a cloud-first strategy, your organization requires a similar cloud-first approach to PAM. Legacy PAM designed a decade ago for the data center can't adapt to a multi-cloud distributed IT infrastructure. Delinea recognized industry trends and invested to get ahead of the curve. They

were the first vendor to offer PAM-as-a-Service, and while other vendors play catch-up, retrofitting legacy technology and focusing their efforts on a subset of PAM, Delinea continues to innovate with comprehensive PAM solutions that cover all the bases enabling privileged access security at scale.

Delinea's Server PAM Solution will provide you with the technology you need to manage access to your infrastructure on your journey to the cloud.

# Improve your server access security!

## FREE Server PAM Resources from Delinea

Secure your on-premises & multi-cloud server environment with modern PAM.

Reduce the risks of security breaches & ransomware attacks while ensuring compliance.



### 5 Reasons to Turn to Multi-Factor Authentication Everywhere Infographic

Combat data breaches, weak passwords, and phishing attacks with MFA.



### Zero Trust Privilege for Dummies eBook

"Trust but verify" is now replaced with "never trust, always verify."



### Advanced Active Directory Bridging Whitepaper

Centralize identity, authentication, and access management for Linux and Unix servers within Active Directory.



### Critical Controls for Modern Cloud Security Whitepaper

Privileged Access Management (PAM) mitigates risks across the cloud attack surface.



### How to Apply Zero Standing Privilege Consistently Across Windows and \*NIX Systems Solution Brief

Secure access to modern hybrid cloud infrastructures that include Windows, Linux, and Unix servers.

**Delinea**

Download now: [delinea.com/resources](https://delinea.com/resources)

With organizations rapidly adopting cloud infrastructure, the perimeter as we knew it no longer exists. This makes it harder to secure access to your systems as you cannot distinguish who is friend or foe by simply examining what's "inside" vs. what's "outside" your perimeter.

With your servers sitting at the center of your infrastructure, securing all privileged access to them has become a core part of a mature cybersecurity strategy.

This eBook will provide you with information and tips to help increase your server access security.



### About Derek A. Smith

With over 30 years in the security industry, Derek A. Smith is a former government agent, cybersecurity SME, holds a variety of certifications (CISSP, CEH, CCISO, Security+, etc.), eight college degrees, is a published author, conference speaker, cybersecurity analyst for several international and local television news stations, government program manager, and more.



ConversationalGeek®

For more content on topics geeks love visit

[conversationalgeek.com](https://conversationalgeek.com)