Why managing (and securing) Privileged Accounts should be your top priority:

## The Case for a Least Privilege Strategy

# YOUR GUIDE TO PRIVILEGED ACCOUNT MANAGEMENT AND SECURITY SOLUTIONS

**This guide will help you understand and develop a plan of action around:**

- Why securing your Privileged Accounts is so critical now
- Challenges with protecting your Privileged Accounts
- Benefits you gain with an automated Privileged Account Management (PAM) solution from Thycotic

## WHY MANAGING AND SECURING PRIVILEGED ACCOUNTS IS SO IMPORTANT

The recent increase in sophisticated, targeted security threats by both external attackers and malicious insiders, along with the growing complexity and distributed nature of IT environments, have made it extremely challenging for organizations to protect their sensitive information. These challenges are driving the need for a new layer of security that complements traditional threat protection by securing access to privileged accounts and preventing the exploitation of organizations' critical systems and data.

### Growing complexity and openness of IT environments increases risk

To support business priorities and the evolving needs of their customers, enterprises are investing in new technologies and architectures that are rapidly increasing the complexity and openness of the IT infrastructure, including virtualization, cloud computing, mobility, big data and social networking. An IT infrastructure typically consists of many servers, databases, network devices and applications, and is often distributed across multiple geographic regions. Furthermore, many enterprises are outsourcing aspects of their infrastructure to cloud service providers and remote vendors, increasing their reliance on third parties to manage and protect their sensitive information.

While these modern technologies offer organizations many benefits, they also increase the security risk by expanding the attack surface of the organization and increasing the complexity of security management. This is particularly true for an often overlooked area of vulnerability---privileged account credentials used throughout the enterprise.

> 63% of confirmed data breaches involved leveraging weak/default/ stolen passwords.
>
> **- 2016 Verizon Data Breach Investigations Report**

## YOUR PRIVILEGED ACCOUNTS ARE WIDESPREAD AND HIGHLY VULNERABLE TO ATTACK

Privileged accounts represent one of the most vulnerable aspects of an organization's IT infrastructure. Privileged accounts are those accounts within an organization that give the user high levels of access, or "privileged" access, to IT systems, applications and data. Privileged accounts are used by systems administrators to deploy and maintain IT systems and they exist in nearly every connected device, server, database, and application. Additionally, privileged accounts extend beyond an organization's traditional IT infrastructure to include employee-managed corporate social media accounts, which can be misused to cause significant reputational damage and other harm to an enterprise.

With the increasing complexity of IT infrastructures, the number of privileged accounts has grown exponentially. We believe that organizations typically have two to three times more privileged accounts than employees. As a result, hijacking privileged accounts gives attackers the ability to access and download an organization's most sensitive data, distribute malware, bypass existing security controls, and erase audit trails to hide their activity.

## CHALLENGES IN HOW TO PROTECT YOUR PRIVILEGED ACCOUNTS

The increasing sophistication, scale and frequency of advanced cyberattacks challenge traditional cybersecurity methods and create a need for a comprehensive approach to securing privileged accounts from use by attackers. Such an approach must address a range of challenges specific to the nature and use of privileged accounts.

- **Traditional security solutions typically have limited ability to protect privileged credentials and critical assets from cyberattacks.** Organizations continue to struggle to protect privileged credentials and critical assets despite significant investment in traditional perimeter, or identity-focused security solutions. They attempt to solve these vulnerabilities by using a combination of disparate traditional security solutions that do not address the unique requirements of securing privileged accounts.

- **Most organizations do not have sufficient visibility and lack automated tools to help in the management of privileged accounts. Traditional approaches to identifying and** managing privileged accounts typically involve manual, time-consuming tasks performed on an infrequent or ad hoc basis. These approaches do not ensure that organizations identify their complete inventory of privileged accounts, or manage their privileged credentials securely. Manual approaches often result in the use of common passwords used across multiple systems, unauthorized sharing of credentials, default passwords remaining in place and other behaviors that compromise security and leave IT systems susceptible to attack. Thus, these approaches do not provide a current, accurate and global picture of an organization's security and compliance posture, decreasing security effectiveness and increasing IT risks and operational costs.

- **Many organizations lack the ability to monitor and audit all privileged account activity.** Traditional information systems do not provide sufficient detail in the use of privileged activities. Worse yet, they allow privileged account users to change security settings or delete system audit logs to hide wrongdoing. Without monitoring and recording privileged account activities, organizations are unable to track and audit privileged activity. This leaves them at risk of failing compliance audits, and unable to hold privileged users accountable for their actions.

> Two out of three organizations still rely on manual methods to manage privileged accounts.
>
> **- Failure to Secure: The 2016 State of Privileged**

## BENEFITS OF THYCOTIC PRIVILEGED ACCOUNT MANAGEMENT AND SECURITY SOLUTIONS

Thycotic privileged account security software solutions provide proactive protection against cyberattacks with the following key benefits:

**Comprehensive platform for proactive protection of privileged credentials and target assets from cyberattacks.**

Our comprehensive solutions for privileged account security enables you to proactively protect against and automatically detect and respond to in-progress cyberattacks before they strike vital systems and compromise sensitive data. Thycotic solutions enhance the effectiveness of traditional security defenses by introducing a new security layer that prevents the misuse of privileged accounts which exist in virtually every piece of technology in the organization---including security products.

**Automatic identification and understanding of the scope of privileged account risk.**

Thycotic solutions automatically detects privileged accounts across the enterprise and helps you visualize the resulting compliance gaps and security vulnerabilities. This automated process reduces the time-consuming and error-prone task of manually tracking and updating privileged credentials, thereby decreasing IT risk and operational costs. This enhanced visibility significantly improves the security posture of our customers, and facilitates adherence to rigorous audit and compliance standards.

**Continuous monitoring, recording and secure storage of privileged account activity.**

Thycotic solutions help you monitor, collect and record individual privileged session activity. They also provide highly secure storage of privileged session recordings and robust search capabilities allowing organizations to meet their audit and compliance requirements. Session recordings also provide a full forensics record of privileged activity to facilitate a more rapid and precise response to malicious activity.

**A Privileged Account Management (PAM) security solution that has been architected across products to optimize security.**

Thycotic's privileged password Vault for example, a secure repository for privileged credentials, offers multiple layers of security including robust segregation of duties, a secure proprietary communications protocol and military-grade encryption.

**Scalable and flexible PAM security platform that enables modular deployment.**

Thycotic solutions are scalable and flexible to enable deployments in large-scale distributed environments.

> 50% of organizations do not audit privileged account activity.
>
> **- Failure to Secure: The 2016 State of Privileged Account Management Report**

> From the KuppingerCole perspective, Thycotic Secret Server is a clear pick when selecting a Privileged Account Management solution. It is of particular interest when competitive pricing, rapid deployment, and short time to value are required, while also supporting a variety of complex and specialized enterprise use cases.
>
> **- KuppingerCole Report**

## SUMMARY

Given the risks and costs associated with unknown and unsecured privileged accounts, it is a must that IT professionals make protecting these accounts from hackers and malicious insiders a top priority. You can start by visiting our website at www.thycotic.com. There you will find an assortment of innovative free tools and automated solutions that deliver simple, easy to use and affordable solutions to protect your privileged accounts and improve the security of your IT infrastructure.

## FREE RESOURCES

Free Privileged Account Discovery Tool for Windows
thycotic.com/free-windows-discovery/

Free Privileged Account Discovery Tool for UNIX
thycotic.com/free-unix-discovery/

Free Privileged Account Password Vulnerability Benchmark
thycotic.com/password-vulnerability-benchmark/