



# Modernizing security: Proactive PAM solutions for today

A new approach to privileged access management

 **ONE IDENTITY**  
by Quest

## Introduction

In every enterprise IT environment, privileged accounts are instrumental in empowering administrators to manage the system effectively. However, the inherent risks associated with granting privileged access, as underscored in many of today's headlines, raise significant concerns for any organization, regardless of size or industry.

### Navigating the perils of privilege

While privileged accounts are indispensable for administrators to efficiently manage an IT environment, they also introduce substantial compliance and security risks. The “all or nothing” nature of privileged accounts means that even basic tasks such as password resets require full administrative rights. This leaves vulnerabilities open to intentional or accidental exploitation. Managing privileged accounts is inherently complex due to shared access among numerous individuals and systems.

### The evolution of PAM solutions

In the past, the complexity of a privileged access management (PAM) solution meant compiling a comprehensive list of privileged accounts and identifying associated individuals and systems. This meticulous process allowed organizations to pinpoint areas of vulnerability to internal or external security breaches and prioritize addressing those areas. Many solutions required creating an exhaustive inventory of scripts and applications using privileged credentials, serving as a foundational step in the implementation process.

Investing in software solutions was crucial, particularly when native tools fell short of providing individual accountability and enforcing the principle of least privileged access. In cases where native tools lacked the ability to enforce accountability and least privileged access, establishing a process for periodic certification was recommended to ensure that users with access to privileged accounts underwent regular auditing, reporting and certification.

### David vs. Goliath: The pressure smaller organizations face

Addressing privileged access as a serious security risk demands a thoughtful, practical and balanced approach. While there may be no silver bullet for IT security, adopting a robust PAM strategy empowers your organization to evaluate its current security posture, identify gaps and effectively mitigate the risks associated with privileged access. It's crucial to acknowledge that existing PAM solutions are often tailored for the large enterprise market, presenting challenges for smaller organizations in terms of comprehension and implementation due to their feature-rich complexity. The ongoing shift of business services to the cloud underscores the necessity for simplicity in service consumption and operation.

Smaller organizations are particularly susceptible to widespread direct access to administrator or root privileges within their environments, often with minimal monitoring of privilege use. With increased reliance on internet connectivity and cloud-based services, the risk of security breaches, reputational damage and regulatory scrutiny multiplies. Consequently, these organizations are under pressure to address privileged access issues promptly, both to mitigate the risk of security breaches and to avoid regulatory violations. The consequences of either scenario could be catastrophic for these smaller organizations.

## A new approach to PAM: One Identity Cloud PAM Essentials

It's time for a simplified, SaaS-based PAM solution that prioritizes security, manageability and compliance to protect your most critical assets.

One Identity Cloud PAM Essentials<sup>SM</sup> provides advanced security features in a user-friendly and cost-effective package to ensure robust privilege access management for organizations of any size.

PAM Essentials provides privileged sessions and access controls, helping mitigate heightened risks associated with unauthorized users. With quick deployment and simplified management, it eliminates the complexities of traditional on-premises PAM solutions and the need for additional infrastructure investments. PAM Essentials aids in meeting compliance and industry-specific standards and enables organizations to meet cyber insurance requirements.

In addition to its core features, PAM Essentials offers advanced capabilities such as federation. This feature focuses on limiting access to a federation of web applications, enabling organizations to enforce session recording for all privileged user access to federated web applications and exercise control over privileged access to SaaS apps. With PAM Essentials, your organization can unlock:

- Full visibility into user activities
- User-centric, security-first design
- Scalable SaaS-based architecture
- Cost-effectiveness through rapid deployment and no need for additional IT infrastructure

## Seamless connection from cloud to on-premises

A seamless connection between the cloud and on-premises is of paramount importance in today's interconnected IT landscape. The integration is facilitated by a network agent to proxy connection, ensuring a smooth and efficient merging of cloud-based services with on-premises systems.

This connectivity guarantees a **cohesive and uninterrupted flow of data and operations**, enabling organizations to leverage the benefits of both cloud and on-premises environments.

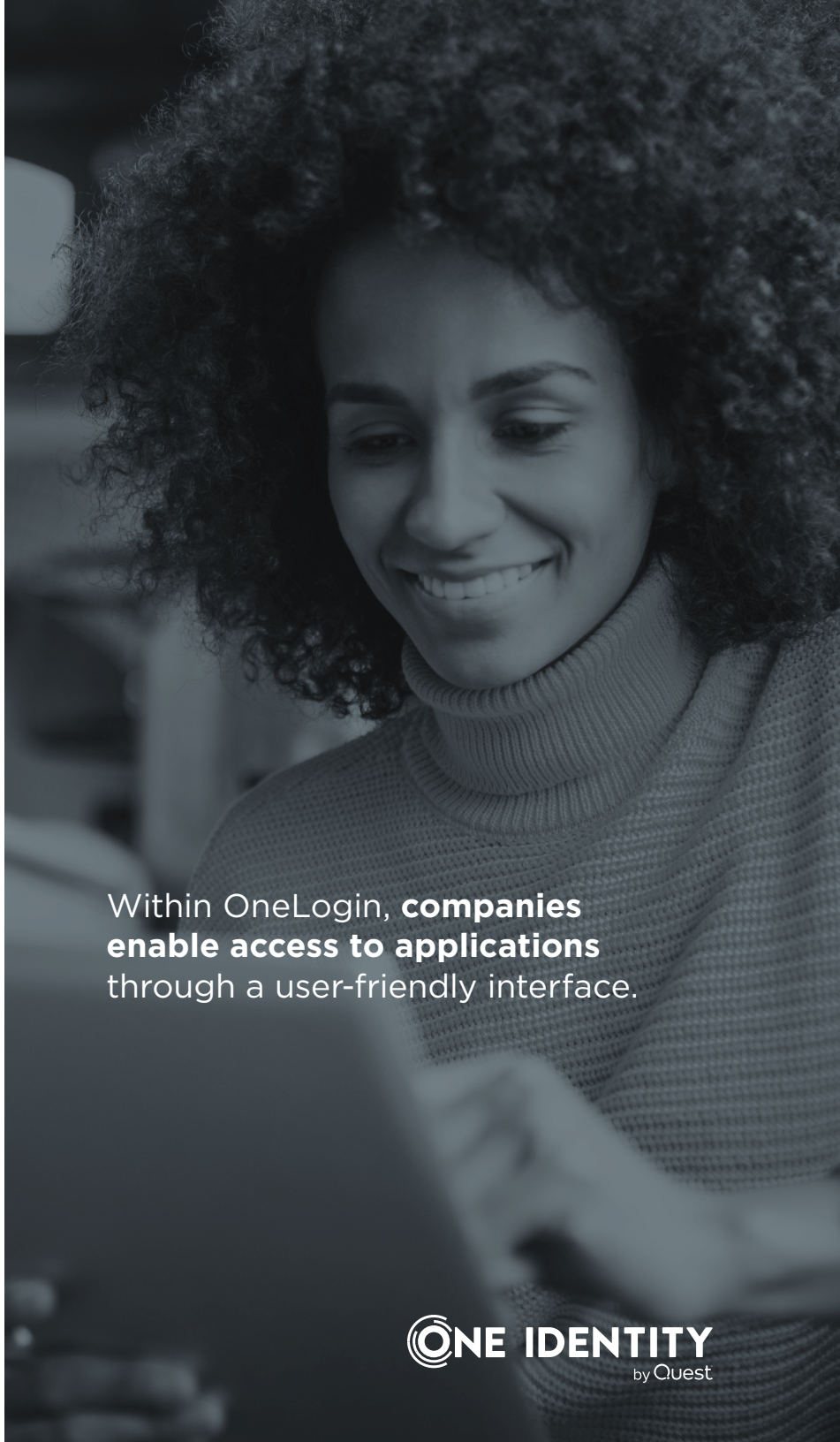
The simplicity of this connection is crucial, streamlining processes and minimizing complexities, allowing businesses to concentrate on their core operations without disruptions. Acting as a reliable bridge, the network agent ensures that data exchanges between the cloud and on-premises systems happen seamlessly, thereby enhancing overall operational efficiency and agility. Adopting this approach, PAM Essentials simplifies the management, scaling and security concerns associated with this complexity.

## Building on the capabilities of OneLogin

Within OneLogin, companies enable access to applications through a user-friendly interface. However, privileged users require more than just application access; they also need remote access to servers and systems. Therefore, in addition to providing straightforward access to applications, PAM Essentials controls administrative accounts by keeping them secure with password rotation while allowing users access into systems without the release of credentials. With this approach, users can seamlessly access not only application tiles but also privileged systems, streamlining workflows for enhanced efficiency.

## PAM Essentials key features

- 1. Security, manageability and compliance:** PAM Essentials prioritizes security, manageability and compliance. It offers comprehensive privilege sessions and access controls to mitigate the heightened risks associated with unauthorized users.
- 2. Quick deployment and simplified management:** Eliminate the complexities of traditional on-premises PAM solutions. With quick deployment and simplified management, organizations can efficiently enhance their security posture without the need for additional infrastructure investments.
- 3. Federation control:** Enable your organization to limit access to federation web applications, enforcing session recording for all privileged user access to federated web applications. Provide control over privileged access to Software as a Service (SaaS) applications.
- 4. Compliance and industry standards:** Effortlessly meet compliance and industry-specific standards. Ensure adherence to cybersecurity regulations and facilitate compliance with cyber insurance requirements.
- 5. Full visibility into user activities:** Follow a simplified PAM approach to gain full visibility into user activities. This offers a clear view of access controls and helps identify potential security risks in real time.
- 6. User-centric and security-first design:** Adopt a user-centric and security-first design. Ensure robust protection without compromising user experience, striking a perfect balance between usability and security.
- 7. Cost-effective and rapid deployment:** The solution is cost-effective and rapid to deploy. It does not require additional IT infrastructure, making it a practical choice for organizations seeking efficient and budget-friendly PAM solutions.
- 8. Scalable SaaS-based architecture:** With a SaaS-based architecture, PAM Essentials scales to meet evolving business needs. This scalability ensures that the solution can grow seamlessly alongside the organization's digital transformation journey.

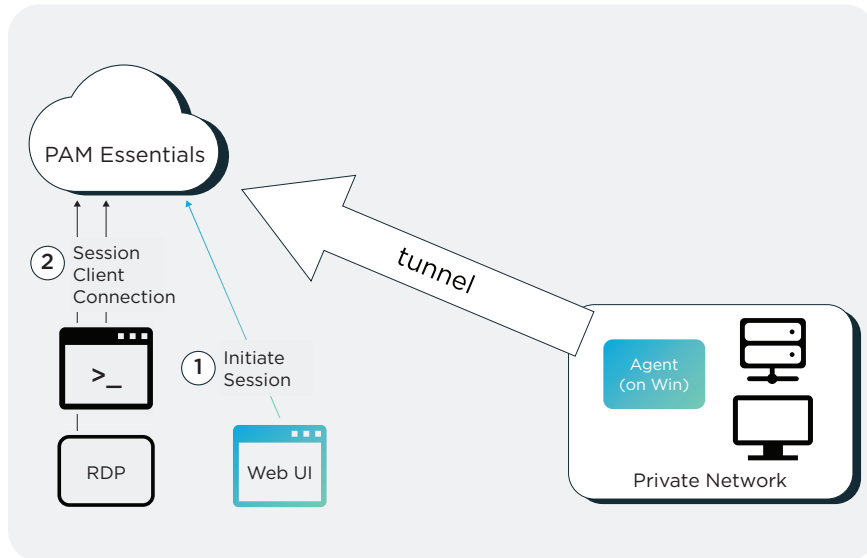


Within OneLogin, **companies enable access to applications** through a user-friendly interface.

## Architecture

In PAM Essentials, the protocol gateway functions as a firewall, filtering incoming traffic by inspecting headers, validating RDP and SSH connections from the public Internet. Following the gateway is the session proxy, tasked with retrieving credentials, injecting them and recording sessions. Subsequently, traffic is directed to the tunnel manager, which interfaces with network agents. In the backend, there's a vault, auditing service and various APIs for thorough tracking. It's also noted that all traffic regardless of source passes through the public internet before making it to the protocol gateway.

This is illustrated in the model below.



## Conclusion

As cyberattacks continue to become more sophisticated in both technique and scale, the security of privileged accounts is paramount. One Identity Cloud PAM Essentials stands out as a robust, user-friendly and cost-effective solution that addresses the challenges of privileged access management.

By prioritizing security, manageability and compliance, **this SaaS-based PAM solution empowers organizations to secure their digital assets** while adapting to the dynamic nature of modern business environments.

*\*One Identity Cloud PAM Essentials is natively integrated with OneLogin which may be used alongside any identity provider solution.*

## About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (ADMgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale - managing more than 500 million identities for more than 11,000 organizations worldwide. For more information, visit [www.oneidentity.com](http://www.oneidentity.com).

If you have any questions regarding your potential use of this material, contact:

**One Identity LLC**  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656