IBM Security Verify Privilege Server Suite On-Premises

Minimize your attack surface and control privileged access to on-premises and cloud-hosted infrastructure

Digital transformation is changing the enterprise landscape, creating increased complexity as organizations leverage emerging technologies such as the cloud, big data, DevOps, containers, microservices, and more.

This complexity brings new challenges and requirements for identity and access management, making it essential to centralize and orchestrate these exponentially increasing and fragmented identities across a hybrid enterprise infrastructure.

Today's modern enterprise

IT organizations are increasingly deploying and managing hybrid environments that combine cloud-based and data center infrastructure while working to mitigate the risk of insider and cyberthreats, all while meeting PCI DSS, SOX, FISMA, HIPPA, MAS, or other industry mandates and government regulations. Modern enterprises require a purpose-built, privileged access management (PAM) solution with a common platform that enables centralized control and visibility over privileged access and simplified compliance

Highlights

- Enable fine-grained access control to Windows, Linux, and UNIX systems with centralized policy management
- Reduce the risk of a breach and associated damage resulting from broad and unmanaged privilege
- Enforce zero standing privileges and reduce lateral movement.
- Detect suspicious user activity and alert in real-time to stop breaches in progress.
- Monitor and control privileged sessions with full video and metadata capture

to protect against new and evolving identity-based threats and attack surfaces.

Privileged identities are a critical focus

Underlying the foundation of digital transformation are privileged identities, meant to assure that only authorized individuals, machines, or services access the right resources at the right times and for the right reasons. But, in the wrong hands, your entire business can be at risk. Protecting them is, therefore, paramount.

Establishing a proper mechanism to do this efficiently and securely has become the Achilles Heel, limiting many digital transformation projects' successes. Technology debt accrues with complex infrastructures and PAM solutions with one foot in the past, having stood still as your business needs have evolved.

You invest in modern infrastructures and application development tools. Shouldn't you invest in modern PAM to protect it?

Legacy security technology— including firewalls, virtual private networks (VPNs), and antivirus software —has proven to be necessary, but insufficient protection against today's data breaches. Organizations must look beyond these network-centric security solutions and on to PAM to stop data breaches.

A modern PAM solution founded on zero trust principles takes an identity-centric approach to protect your IT infrastructure, wherever it is. Gone are the old PAM assumptions, protecting infrastructure that lives exclusively in a walled-garden datacenter.

IBM Security Verify Privilege Server Suite enables digital transformation at scale, modernizing how organizations secure privileged accessacross hybrid multicloud environments. It allows

humans and machines to seamlessly authenticate, enforcing least privilege with just-in-time privilege elevation, increasing accountability, and reducing administrative access risk.

Why Place Your Trust in Verify Privilege Server Suite?

Verify Privilege ’s history demonstrates a deep understanding of PAM, starting with the core mission to centralize and orchestrate fragmented identities across enterprise infrastructure.

Expertise in infrastructure management evolved into a thoroughly modern PAM approach and focus on identity-centric solutions based on zero trust principles. We believe that PAM solutions must meet the needs of both infrastructure and security teams sharing a single platform; they are made of the same connective tissue and therefore function and grow together.

Verify Privilege Server Suite comprises three core services that work synergistically to fully protect your Windows, Linux, and UNIX estates against identity-based attacks.

Privilege Authentication Service

Privilege Authentication Service extends Active Directory (AD) benefits to Linux and UNIX by natively joining them to AD, turning the host system into an AD client. It secures access to these systems consistently, using the same authentication and Group Policy services currently deployed for your Windows systems. Changes to user access and permission in AD (e.g., via just-in-time access request workflow) is immediately reflected and enforced at the AD client. This overcomes inherent AD propagation delays that can disrupt time-critical activities (such as a breach investigation).

With AD for cross-platform management, you can now consolidate identities--eliminating many local privileged accounts (especially on *NIX) and giving administrators a single AD account with which to access any AD-joined system, reducing your attack surface. If you must use local accounts, you can use AD to centrally manage their lifecycle with Local Account and Group Management.

Manage all this complexity and chaos with roles and zones technology. Zones extend the flat AD container model, so you can logically group systems in a parent-child hierarchical model that aligns with your preferred governance approach. Granting access to computers in a zone is as simple as adding a user to that zone.

The same infrastructure that helps you get human user access under control can be applied to better secure your DevOps environment. LeverageVault Service to store application/service passwords and secrets. The result is that instead of sensitive data being exposed in code and configuration files, applications can obtain it at run-time via API or CLI calls to further reduce your risk. Moreover, eliminate per-application service accounts required to authenticate to the vault – each of which represents a vector of attack. Leverage unique Delegated Machine Credentials and capitalize on the machine's enrollment in the platform and resulting mutual trust. Thus, only a single machine identity is required for access to vault services with:

- AD bridging
- Brokered authentication
- Group policy for Linux
- Linux smart card loginfor workstations
- RBAC and zones
- MFA at system login
- Local account and group management
- Approval workflows for login

Privilege Elevation Service

Assigning just enough privilege based on a job function increases security and accountability. Having users log in as themselves and elevate privilege based on their role within the organization minimizes your attack surface by reducing shared accounts and vaulted credentials. Instead of standing privileges, self-service workflow allows admins to request temporary roles to complete legitimate helpdesk-driven tasks for just-in-time access.

Privilege Elevation Service acts as a policy enforcement point to control privilege elevation on Windows, Linux, and UNIX systems. It consumes policy that the Authentication Service centrally defines and maintains in AD and enforces what system- level commands and applications users can execute. Privilege Elevation Service offers:

- Least privilege enforcement
- MFA at privilege elevation
- Approval workflows for privilege elevation
- Zones for RBAC policy
- Delegated Machine Credentials

Audit & Monitoring Service

Gain full accountability and visibility into all privileged activity and tie everything back to the individual by recording and managing a holistic view across Windows, Linux, and UNIX servers. Out-of-box reports assist with PCI and SOX compliance and incident response investigations.

With host-based auditing on each system, Verify Server Suite helps ensure that cyber- attackers can’t bypass session recordings. You can combat spoofing with advanced monitoring capabilities that combine

application and file change monitoring at the shell and process levels, with video recording, metadata capture, and time-indexed command auditing. Detect spoof video recordings with commands hidden inside aliases and shell scripts. Audit and Monitoring Service features include:

- Host-based audit and monitoring
- Gateway-based audit and monitoring
- Linux and UNIX advanced monitoring at the shell and process levels

For data privacy, prevent visibility to sensitive data in audit logs. Audit & Monitoring Service obfuscates the data at source (i.e., on the host system) ensuring it never leaves the host system. Thus, data privacy can be ensured whether events are viewed locally or forwarded to other systems (e.g., Splunk and IBM Security QRadar).

If you need a modern PAM solution to govern and control access to on-premises and private cloud IT infrastructure, centrally managed from AD — take a closer look at Verify Privilege Server Suite.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Security Verify Privilege Server Suite and other PAM solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security/privileged-access-management