IBM Security Verify Privilege

Powerful privileged access management available on-premises and in the cloud

Privileged access is the route to an organization's most valuable information. As a result, implementing privileged access management (PAM) has become a top priority. IBM Security Verify Privilege is a fully-featured PAM solution available both on-premises and in the cloud, ready to empower your security and IT ops team to secure and manage all types of privileged accounts quickly and easily. With Verify Privilege you can:
`

- Establish a Secure Vault - Store privileged credentials in an encrypted, centralized vault.
- Discover Privileges - Identify all service, application, administrator, and root accounts.
- Protect Passwords - Automate password changing, ensure password complexity, and rotate credentials.
- Meet Compliance - Proactive compliance through auditing, reporting, and alerts.
- Control Sessions - Implement session launching, proxies, monitoring, and recording.
- Monitor Activity – Keep track of suspicious and irregular activity patterns with the Analytics add-on
- Deploy a Single Agent – Discover application usage with admin rights, even on non-domain machines.

Highlights

- Vault, Audit & Control Privileged Access
- Identify and track suspicious behavior
- Manage local groups and accounts while maintaining a least privilege model
- Automate secrets management with consistent, centralized, and auditable processes
- Easily deploy in distributed environments
- Take control of service accounts

- Define Flexible Policies – Creating allowed, trusted and denied trusted applications and processes.
- Manage & Remove Local Admin Rights – Determine which accounts are members of any local group, including system administrators.
- Elevate Applications – Allow trusted applications to run, block or sandbox others, all while maintaining a least privilege model.
- Improve Productivity – People automatically access apps and systems they need; helpdesk tickets decrease.
- Automate secrets management - Provide DevOps teams the speed and agility needed to stay productive without sacrificing security
- Control Service Account Governance - Secure, provision, and decommission accounts to harden your attack surface

Verify Privilege is fast to deploy, easy to use, and scalable for the enterprise. It integrates with the larger IBM Security portfolio for key use cases, such as identity governance, threat detection and response systems, single sign-on and multi-factor authentication. IBM Support is available 24x7. Deployment guidance, strategy consulting, and managed PAM Services are also available. Interested in testing out the product firsthand? Start your free 30-day trial here.

On-premises? In the cloud? No need to compromise

IBM Security Verify Privilege deployed on- premises allows for total control over your end-to-end security systems and infrastructure. You can deploy software within your on-premises data center or your own virtual private cloud instance. You'll be able to meet legal and regulatory obligations that require all data and systems to reside on-

premises. Verify Privilege in the cloud is a software-as-a-service model which lets you sign up and start right away. There are no hardware or infrastructure costs and no provisioning, patching, or maintenance overhead. Experience elastic scalability as you grow, with controls and redundancy with 99.9% uptime SLA.

Detect anomalies in privileged account behavior so you can take action before a cyber threat becomes a cyber catastrophe.

Verify Privilege includes a SaaS service that helps identify and track anomalous behavior. The solution delivers privileged behavior analytics (PBA) by importing and analyzing all secret and user history from Verify Privilege. The analytics add-on connects seamlessly to existing security and IT software, and can automatically take administrative action, send alert notifications in Slack, or open a ticket in ServiceNow.

Swift and Effective Incident Response

PBA imports all secret and user history from Verify Privilege. When risk scores pass acceptable thresholds, you’re instantly alerted so you can protect privileged accounts by immediately rotating passwords, requiring additional authentication, or increasing session monitoring. PBA connects seamlessly to your security and IT software. It can automatically take action in Verify Privilege, send alert notifications in Slack or open a ticket in ServiceNow.

At-a-glance dashboard and actionable reports help you cut through the noise to see what's most important

- Detailed snapshot of privileged account activity
- Real-time behavior pattern recognition
- Threat scoring to prioritize issues
- Map view of privileged users and related accounts
- Configurable alerts
- Controls to manually increase sensitivity for specific users or accounts

Remote session management at enterprise scale: Monitor, record and control privileged sessions

As IT groups scale their efforts across larger networks, new cloud services, various connection protocols, numerous privileged users, different business groups and customer environments, they need to closely monitor privileged accounts across sessions.
Verify Privilege provides remote connection management capabilities to give a unified environment to manage and interact with multiple remote sessions for both Remote Desktop Protocol (RDP) and SSH. Credentials, session recording, multi- factor authentication and secrets access workflows can now be accessed in a single location to improve productivity, strengthen security and tighten compliance.

Maximize Productivity

- Support use of specific protocols, tools and user interfaces for multiple sessions.
- Launch new sessions in a separate tab for better visibility.
- Quickly switch between sessions.
- Available for Windows and MacOS

Secure Credentials

- Inject credentials automatically into sessions from IBM Security Verify Privilege.
- Minimize privilege escalation and third-party privileged account misuse.
- Reduce improper access due to administrative errors.

Centralize Control

- Tight integration with Verify Privilege Vault provides secure access to privileged credentials.
- Support for workflow actions are accessible in a single location.
- Improve accountability and oversight over privileged users

Monitor and Audit

- Capture every action taken in your audit log to prove regulatory compliance and enable session recording.
- Meet regulations including SOX, HIPAA, ICS CERT, GLBA, PCI DSS,FDCC, FISMA, among others

Protect the secrets that DevOps teams and RPA tools need to access applications, services, and IT resources

Rapid, iterative DevOps workflows often expose many security vulnerabilities directly tied to privilege management.

Every container, server, and application can have privileged access, dramatically expanding the attack surface for intruders looking for an entry point. It’s difficult to balance high-speed, dynamic DevOps

practices and RPA deployments with necessary security policies. IBM's Verify Privilege automates secrets management to provide DevOps teams the speed and agility needed to stay productive without sacrificing security. It addresses all scenarios where secrets are exchanged between machines, including databases and applications for software and infrastructure deployment, testing, orchestration, configuration, and Robotic Process Automation.

Enable greater agility, ease of use, and reduced overhead

- Manage secrets at the speed and scale of DevOps pipelines and RPA deployments.
- Adopt DevOps and RPA principles securely without the infrastructure burden of provisioning on-premises vault instances.
- Eliminate the risk of disparate vault instances and decrease cost of ownership with a SaaS solution.
- Issue X.509 and SSH certificates, enabling automated certificate signing and distribution.

Get started rapidly

- Cloud-based solution with REST API and command-line interface helps you get started fast.
- Connect to any platform in your DevOps pipeline or RPA deployment, and take advantage of infinite scalability

Maximize productivity of development, security, and operations teams

- Automate the deprovisioning of secrets when they are no longer needed.
- Minimize privileged account sprawl.
- Allow flexibility with a platform-agnostic solution.
- Eliminate the need to build and maintain your own infrastructure.

De-risk operations within dynamic, elastic environments

- Harden attack surface by controlling privileged access.
- Eliminate the need to hard-code secrets within code and scripts.
- Provide centralized, unified, auditable management and enforcement of secrets access.
- Remove standing access to critical infrastructure with dynamic secrets

Enforce least privilege security and control application rights on endpoints

Verify Privilege also focuses on endpoint privilege management and application control. Removing local administrative privileges is the most effective way to protect endpoints from attack with immediate, measurable benefits. Implementing and enforcing a least privileged security posture takes planning, collaboration, and tools that make life easy for security, IT, desktop support, and users. Not every least privilege solution gives you the flexibility and control you need to be successful. IBM Security Verify Privilege empowers you to implement a least privilege security posture and application control on endpoints.

Assess your IT security risk with any of these free discovery tool

Privileged accounts: how many, where and why?

When it comes to privileged account credentials, what you don't know can hurt you. Not knowing how many privileged accounts exist, how they're being used, or where they’re located is a major

vulnerability. IBM offers a free privileged account discovery tool which gives you a comprehensive view of all the Windows privileged accounts in your environment. It generates a report to help you assess the security of your privileged passwords and highlight potential risks. *Download the free Windows privileged account discovery tool today.*

See which IT systems and users have higher privileges than they need.

Adhering to a least privilege policy is particularly important for remote workers connecting through diverse workstations. If users have local administrator rights and unintentionally download malicious software, they invite cyber criminals into your entire network. Register to immediately download the Least Privilege Discovery tool. A quick scan of your environment indicates which accounts may be overprivileged, and therefore vulnerable to insider threats and malware attacks. Knowing this information will help you improve least privilege in your environment by restricting applications allowed to run, devices allowed to connect, and the actions a system can perform. *Register for the Least Privilege Discovery Tool*

Quickly identify the riskiest applications running in your environment.

Hackers are targeting applications on endpoints to easily access core systems. That is why having a better understanding of what's running and installed on your endpoints is so important. These tools helps identify what operating system and potential security risks are running on your endpoints. The executive summary report will

provide insight into operating systems, vulnerable computers and risky applications. Save hours of effort by discovering vulnerable applications and associated risks in minutes. *Register for the Endpoint Application Discovery Tool*

Take Control of Service Account Governance

Secure, provision, and decommission accounts to harden your attack surface.

Service accounts abound in every organization. Failure to manage them leads to significant risk. These specialized non-human accounts are used by applications or other services to access data and network resources for specific tasks. Because of their “set it and forget it” operation and limited human interaction, service accounts often fly under IT’s radar and rarely get inventoried and controlled. This lack of governance makes service accounts the ideal target for cyber criminals. Thycotic’s Account Lifecycle Manager enables service account governance by automating the lifecycle of service accounts, from workflow-based provisioning to account decommissioning.

Establish Workflow

- Admins define workflows for provisioning process
- Approvals can be required for each type of account request
- Bi-directional integration with ServiceNow embeds service account governance in IT workflow

Delegate Ownership

- Role-based permissions govern user access, setup, and request workflow

- Out-of-the-box roles include System Admin, Account Owner, Requesters and Approvers
- Create additional roles to support specific business needs
- Separation of duties (SOD) allowed through an approval process created by the admin

Provision Accounts

- Manage and control service accounts with automated provisioning
- Admins can create templates that specify how an account will be created

Enforce Governance

- Create accountability and ownership over service accounts
- Easily audit accounts for compliance through account searches and reporting and logging

Decommission Accounts

- Decommissioning of service accounts enabled without disruptions
- Control service account sprawl and harden your attack surface

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.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

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 Offering Name, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security/offeringname