IBM Security Privilege Manager

Block malware-based attacks with least privilege and application control.

Highlights

- Control endpoint application privilege escalation
- Enforce least privilege policies on endpoints
- Stop malware at the endpoint

Implementing a least privilege cybersecurity strategy is a foundational step for your organization. A large number of cybersecurity breaches involve compromised endpoints. It is the most common entry point for threats into organizations. Once hackers gain privileges on one machine, they can quickly move throughout your network – and cover their tracks!

Adopting a least privilege method can be done through controlling privileges of each user or by controlling privileges of all applications on the network. Privilege management through application control is the strongest level of security, because it ensures that your users NEVER operate as administrators. It is the most scalable and sustainable method as your organization grows and individuals come and go, change roles, and continually explore applications.

IBM Security Privilege Manager prevents malware from exploiting local credentials to install on endpoints, the most vulnerable part of your attack surface. It allows organizations to take a proactive approach to endpoint security and avoid spending time and resources on reactive detection and remediation.

With Privilege Manager you can easily remove local administrative rights from endpoints and enforce the principle of least privilege through application control policies that are seamless for users and reduce the workload of your desktop support team.

Even if local accounts have not been granted elevated privileges in the domain or the operating system, if they can manipulate the configuration of an application or access information the application provides, they are a vulnerability in your attack surface that allows threat agents to get inside

your organization.

Application control further reduces the attack surface by restricting the applications allowed to run, the devices allowed to connect, and the actions a system can perform. By focusing first on removing privileged credentials you tighten your attack surface, which applies to all attacks, even the most evasive.

With IBM Security Privilege Manager, you can adopt a multi-layered approach that covers your privilege security needs from endpoints to credentials, ensuring that you have protection at every step of an attacker's chain.

Why IBM?

IBM's Privileged Access Management products are powered by Thycotic's technology, branded as IBM Security Secret Server and IBM Security Privilege Manager. This partnership combines Thycotic's proven technology with the legacy, support, services and integrations of IBM Security.

For more information

To learn more about IBM Security Privilege Manager, please contact your IBM representative or IBM Business Partner, or visit: https://www.ibm.com/us-en/marketplace/privilege-manager.

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

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