Safeguard for Privileged Sessions

Reduce risk by controlling, monitoring and recording privileged access

Introduction

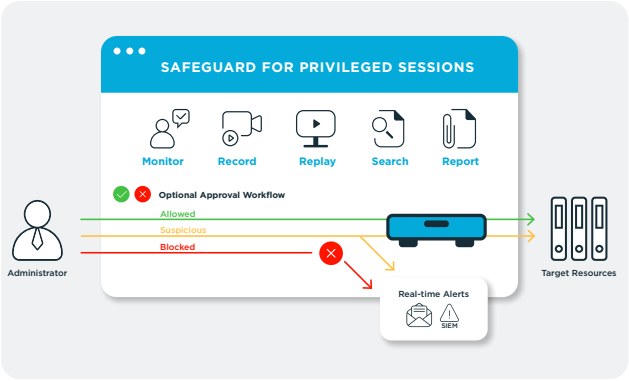
Granting uncontrolled privileged access to internal administrators, third-party vendors, contractors and service providers can create significant risk. This opens the door to attackers who hijack privileged accounts and to rogue administrators. The unfortunate – and expensive – impact of this type of risk has been shown over and over again by recent, highly-publicized incidents. To achieve true security and compliance, you must do more than simply control privileged user accounts. You must monitor and record what they do with privileged access.

With One Identity Safeguard for Privileged Sessions, you can control, monitor and record privileged sessions of administrators, remote vendors and other high-risk users. The recorded sessions' content is indexed to make searching for events simple and it also helps automate reporting so you can easily meet your auditing and compliance requirements.

Safeguard for Privileged Sessions also serves as a proxy, inspecting the protocol traffic on the application level. This inspection makes an effective shield against attacks by rejecting all traffic that violates the protocol. In transparent mode, minimal changes to your network are required and users do not have to change their current workflow or client applications, which makes implementation a breeze. However, workflow rules can be configured to be more stringent, including requiring prior user authorization, limiting access to specific resources and receiving alerts if connections exceed preset time limits. Safeguard can also monitor sessions in real time and execute various actions: if a risky command or application appears, One Identity Safeguard can send you an alert or immediately terminate the session.

Benefits

- **Mitigate the risk of a security breach** by controlling access to sensitive IT assets
- **Easily meet compliance requirements** for monitoring privileged access
- **Get value faster** with simple deployment and management
- **Keep admins happy** by enabling the use of familiar tools to administer systems
- **Maximize productivity** with a small learning curve and elegant UI design
- **Reduce efforts of audit reports** with quick access to all the information you need
- **Track access** to any type of systems thanks to a host-independent, agentless design
- **Accelerate incident response** through fast, full-text search in recorded sessions



Record and monitor all privileged access

With full-text search, real-time alerting and blocking, Safeguard reduces your risk while making it easier to meet compliance requirements.

Features

Full session audit, recording and replay

All session activity – down to the individual keystroke, mouse movement and windows viewed – is captured, indexed and stored in tamper-proof audit trails that can be viewed like a video and searched like a database. Security teams can search for specific events across sessions and play the recording starting from the exact location the search criteria identified. Audit trails are encrypted, time stamped and cryptographically signed for forensics and compliance purposes.

Real-time alerting & blocking

Monitors traffic in real time and executes various actions if a certain pattern appears in the command line or on screen. Predefined patterns could be a risky command or text in a textoriented protocol or a suspicious window title in a graphical connection. In the case of detecting a suspicious user action, Safeguard can log the event, send an alert or immediately terminate the session.

Two modes of operations

Choose which mode suits your needs.

- **Workflow Engine** – A workflow engine that supports time restrictions, multiple approvers, reviewers, emergency access and expiration of policy. It also includes the ability to input reason codes and/or integrate directly with ticketing systems. A password request can be automatically approved or require any level of approvals.
- **Instant On** - Deploy in transparent mode so that no changes to user workflows are necessary. It can act as a proxy gateway operating like a router in the network – invisible to the user and to the server. Admins can continue to use familiar client applications and can access target servers and systems without any disruption to their daily routine.

Proxy access

Since users have no direct access to resources, the enterprise is protected against unauthorized and unfettered access to sensitive data and systems. Safeguard for Privileged Sessions can proxy and record to many target resources, including UNIX/Linux, Windows, network devices, firewalls, routers and more.

Command and application control

Safeguard for Privileged Sessions supports both black listing and white listing of commands and windows titles. Work the way you want Even when workflow is enabled, administrators can choose their client, tooling and preferences when accessing privileged sessions.

This creates a frictionless solution that gives administrators the access they need while **meeting compliance and security regulations**.

Full-text search

With its Optical Character Recognition (OCR) engine, auditors can do full-text searches for both commands and any text seen by the user in the content of the sessions. It can even list file operations and extract transferred files for review. The ability to search session content and metadata accelerates and simplifies forensics and IT troubleshooting.

ONE IDENTITY by Quest

Auto-login

With the password injection functionality, access can be configured for auto login, which enhances security and compliance by never exposing the password to the user. Wide protocol support Full support for SSH, Telnet, RDP, HTTP(s), ICA and VNC protocols. In addition, security teams can decide which network services (e.g. file transfer, shell access, etc.) within the protocols they want to enable/disable for administrators.

Instant off

By acting as a virtual firewall, One Identity Safeguard increases protection of your servers by terminating questionable or malicious accesses nearly instantly. In addition, to avoid accidental misconfiguration and other human errors, the solution supports the four eyes authorization principle under which the monitoring admin can terminate the session at any time.

Drop in deployment

With a rapid appliance-based deployment and simplified traffic rerouting, One Identity Safeguard can have you recording sessions in a matter of days without disrupting your users.

Analytics ready

Collect all the information you need to analyze privileged users and behavior and detect internal and external threats.

Secure access to legacy systems

Use smartcard, 2FA or other strong authentication methods to gain secure access to systems. Because Safeguard acts as a proxy gateway to the system, it enables strong authentication to targets that cannot or do not support those methods automatically.

The One Identity approach to Privileged Access Management

The One Identity portfolio includes the industry's most comprehensive set of Privileged Access Management solutions. You can build on the powerful session management functionality of Safeguard for Privileged Sessions with our privileged password safe and privileged analytics solutions. Our product offering includes solutions for granular delegation of the UNIX root account and the Active Directory administrator account, add-ons to make open source sudo enterprise ready; and keystroke logging for UNIX root activities – all tightly integrated with the industry's leading Active Directory bridge 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.

ONE IDENTITY by Quest