BALASYS

One Identity Safeguard

Securely store, manage, record and analyze privileged access

BENEFITS

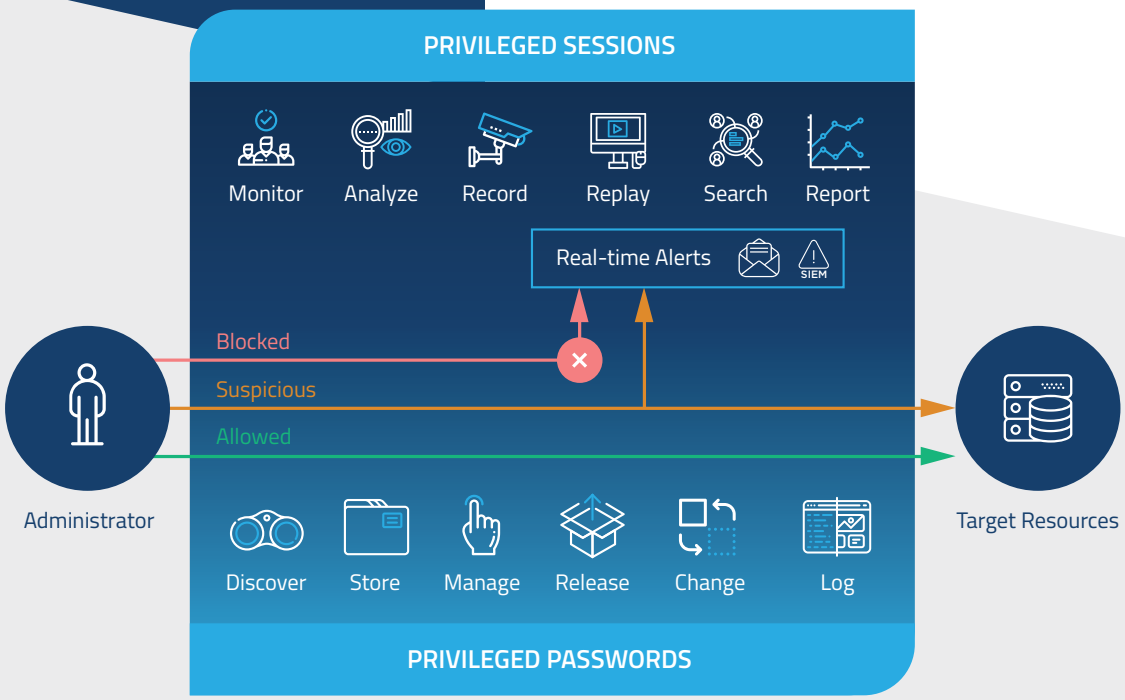
- Mitigate the potential damage of a security breaches
- Meet compliance requirements
- Quick ROI with simplified deployment and management
- Efficient audit-report creation
- Identify high-risk privileged users, risky behaviors and unusual events
- Simplifies privileged account management

INTRODUCTION

Hackers continually evolve the methods they use to gain access to your systems and data. Ultimately, they want to get to your privileged accounts. In nearly every recent high-profile breach, privileged accounts have been compromised to gain access to critical systems and data. You can limit the damage from a breach by deploying solutions that provide a secure, efficient and compliant way to access to privileged accounts.

For IT managers, these all-access accounts are a challenge to manage for a number of reasons, including the sheer number of the privileged accounts and the number of people that need access to them. On top of these challenges, traditional privileged access management (PAM) solutions involve complex architectures, lengthy deployment times and onerous management requirements.

Yes, PAM can be a huge challenge, but it doesn't have to be. One Identity Safeguard is an integrated solution that combines a secure hardened password safe and a session management and monitoring solution with threat detection and analytics. It securely stores, manages, records and analyzes privileged access.



Secure privileged access without sacrifice

Take the stress out of protecting your privileged accounts by securely storing, managing, recording and analyzing privileged access while satisfying your admins and auditors with One Identity Safeguard.

Safeguard for Privileged Sessions

With One Identity Safeguard for Privileged Sessions, you can control, monitor and record privileged sessions of administrators, remote vendors and other high-risk users. Content of the recorded sessions is indexed, which makes finding session events easy later and helps simplify and automate reporting, both functionalities easing your audit and compliance requirements. In addition, Safeguard for Privileged Sessions serves as a proxy, and inspects the protocol traffic on the application level and can reject any traffic that violates the protocol – thus making it an effective shield against attacks.

Safeguard for Privileged Passwords

One Identity Safeguard for Privileged Passwords automates, controls and secures the process of granting privileged credentials with role-based access management and automated workflows. The user centered design of Safeguard for Privileged Passwords means a reduced learning curve. Plus, the solution enables you to manage passwords from anywhere and using nearly any device. The result is a solution that secures your enterprise and gives your privileged users a new level of freedom and functionality.

Safeguard for Privileged Analytics

With One Identity Safeguard for Privileged Analytics, you can put user-behavior analytics to work for you and know which privileged users present the most risk, discover previously unknown internal and external threats, and find and stop suspicious activities. Safeguard for Privileged Analytics ranks the potential risk level of threats so you can prioritize your response – take immediate action on the most imminent threats – and ultimately prevent data breaches.

FEATURES

Policy-based release control

Using a secure web browser with support for mobile devices, you can request access and provide approval for privileged passwords and sessions. Requests can be approved automatically or require dual/multiple approvals based on your organization's policy. So whether your policies consider the requestor's identity and level of access, the time and day of the request attempt, and the specific resource requested – or all of these — you can configure One Identity Safeguard to meet your customized needs. Plus, you can input reason codes and/ or integrate with ticketing systems.

Full-session audit, recording and replay

All session activity – down to the 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 occurred. Audit trails are encrypted, time-stamped and cryptographically signed for forensics and compliance purposes.

Change control

Supports configurable, granular change control of shared credentials, including time-and last-use-based, and manual or forced change.

User behavioral biometrics

Each user has an idiosyncratic pattern of behavior, even when performing identical actions, such as typing or moving a mouse. The algorithms built into Safeguard for Privileged Analytics inspect these behavioral characteristics (captured by Safeguard for Privileged Sessions). Keystroke dynamics and mouse movement analysis help identify breaches and also serve as a continuous, biometric authentication.

Approval anywhere

Leveraging One Identity Starling Two-Factor Authentication, you can approve or deny requests from anywhere – and with nearly any device -- without being on the VPN.

Favorites

Quickly access the passwords that you use most often right from the login screen. You can group several password requests into a single favorite so you can get access to all the accounts you need with a single click.

Discovery

Quickly discover privileged accounts or systems on your network with host-, directory- and network-discovery options.

Real-time alerting and blocking

Safeguard for Privileged Sessions 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 text-oriented 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.

Identify risky users

Safeguard evaluates entitlement grants against risk-classification rules to identify high-risk accounts. Proactive notifications are sent when changes to entitlement grants move a user's profile into a high-risk status. This eliminates risk from unnecessary or dormant entitlements before someone can abuse or exploit them.

Command and application control

Safeguard for Privileged Sessions supports both black listing and white listing of commands and windows titles.

Instant on

Safeguard for Privileged Sessions can be deployed in transparent mode requiring no changes to user workflows. Acting as a proxy gateway, Safeguard can operate like a router in the network – invisible to the user and to the server. Admins can keep using the client applications they are familiar with, and can access target servers and systems without any disruption to their daily routine.

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.

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.

Drop-in deployment

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

RESTful API

Safeguard uses a modernized API based on REST to connect with other applications and systems. Every function is exposed through the API to enable quick and easy integration regardless of what want to do or which language your applications are written.

One Identity Hybrid Subscription

Expand the capabilities of Safeguard with the One Identity Hybrid Subscription, which offers immediate access to cloud delivered features and services. These include all-you-can-eat Starling Two-Factor Authentication to protect Safeguard access and Starling Identity Analytics & Risk Intelligence for Safeguard so that you can pre-emptively detect risk users and entitlements. A single subscription enables all One Identity solution deployments

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 capabilities of One Identity Safeguard with 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 helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats.

ONE IDENTITY™

Balasys IT Ltd. | Alíz Street 4. H-1117 Budapest | Phone: +36 1 646 4740 | sales@balasys.hu