One Identity Safeguard On Demand

SaaS-delivery to securely store, manage, record and analyze privileged access

Cloud without Compromise

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. But you can limit the damage with an on-demand solution that provides a secure, efficient and compliant way to manage privileged accounts.

For IT managers, these all-access admin 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 On Demand is a SaaS-delivered solution that combines a secure password safe and a session management and monitoring solution with threat detection and analytics all managed and delivered from the cloud.
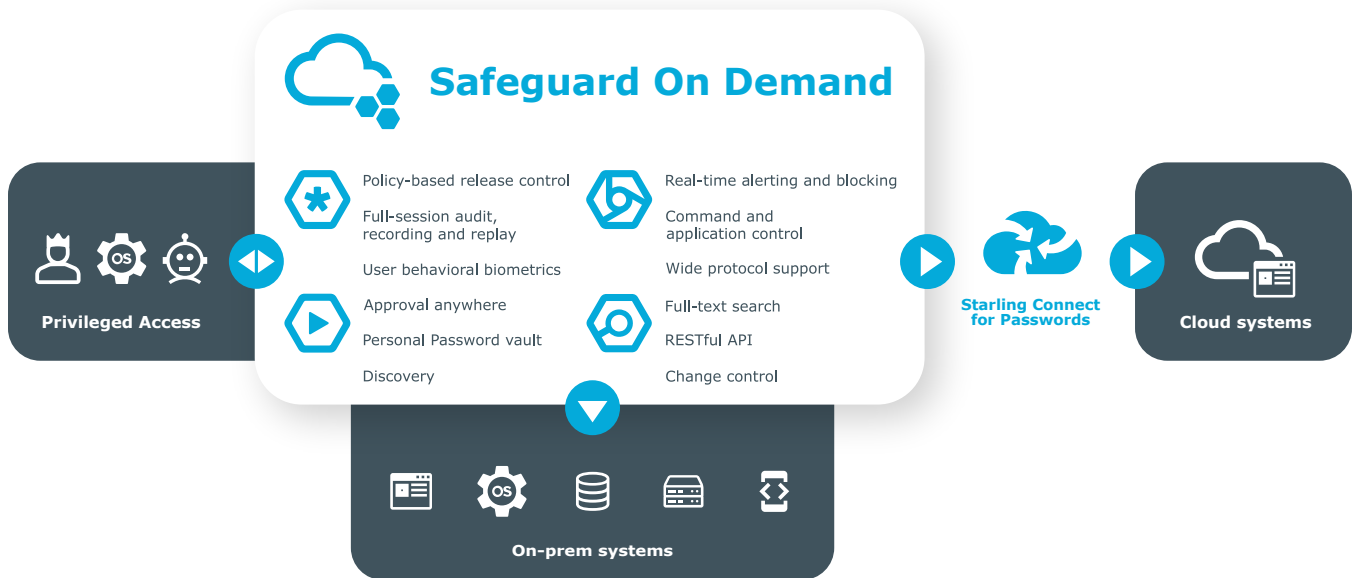
Safeguard On Demand automates, controls and secures the provisioning of privileged credentials with role-based access management and automated workflows. The user-centered design of Safeguard On Demand means a reduced learning curve. Plus, it gives you the flexibility and convenience to manage passwords from anywhere and using nearly

Benefits

- **Mitigate the potential damage** of security breaches
- **Meet compliance requirements**
- **Realize quick ROI** with simplified deployment and management
- **Get efficient audit**-report creation
- **Identify and stop risky behaviors** and unusual events
- **Simplify** privileged account management

any device. The result is a solution that secures your enterprise and gives your privileged users a new level of freedom and functionality.

Safeguard On Demand also enables you to 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 On Demand 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 On Demand

Privileged Access

- Policy-based release control
- Full-session audit, recording and replay
- User behavioral biometrics
- Approval anywhere
- Personal Password vault
- Discovery

- Real-time alerting and blocking
- Command and application control
- Wide protocol support
- Full-text search
- RESTful API
- Change control

On-prem systems

Starling Connect for Passwords

Cloud systems

Safeguard On Demand also includes privileged analytics, so you can discover previously unknown internal and external threats, and find and stop suspicious activities. Safeguard On Demand 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 On Demand 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.

Instant on

Safeguard On Demand operates in transparent mode requiring no changes to user workflows. Acting as a proxy gateway, Safeguard On Demand 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.

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 On Demand inspect these behavioral characteristics. Keystroke dynamics and mouse movement analysis help identify breaches and also serve as a continuous, biometric authentication.

Approval anywhere

Leveraging One Identity Cloud Assistant, you can approve or deny requests from anywhere —and with nearly any device.

ONE IDENTITY
by Quest

Personal Password Vault

All your organizations employees can store and generate random passwords for non-federated business accounts in a free personal password vault. This enables your organization to use a sanctioned tool with the ability to securely share and recover passwords providing much needed security and visibility into business accounts.

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 On Demand 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 On Demand can log the event, send an alert or immediately terminate the session.

Command and application control

Safeguard On Demand supports both black listing and white listing of commands and windows titles.

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.

RESTful API

Safeguard On Demand 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 you want to do or the language in which your applications are written.

Change control

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

ISO 27001 Certified

One Identity, a Quest Company and a leading global identity security company, and its cloud infrastructure and processes have achieved ISO/IEC 27001 certification; the international standard outlining best practices for information security management systems.

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 On Demand with solutions for granular delegation of the UNIX root account and the Active Directory administrator account; addons 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