EBOOK

ONE IDENTITY

by Quest

Realize Your Vision with Next-Gen Privileged Access Management

Seven organizations boost security, efficiency and agility with One Identity Safeguard.

Save time and focus on driving growth with **flexible, automated tools** for managing privileged access

Hackers often target the accounts of IT administrators and other privileged users to gain access to systems and data without detection. To increase insight and control over privileged users' actions, global banks, cloud service providers and organizations across all industries use One Identity Safeguard for privileged access management (PAM).

With Safeguard, organizations can manage privileged access to diverse platforms with centralized, easy-to-use tools that work seamlessly with existing security measures and simplify the automation of workflows such as:

- Privileged access requests and authorizations
- Unique session-password generation
- Session recordings
- Monitoring privileged sessions for unusual behavior

On the following pages, read how seven organizations increase security, efficiency and agility by protecting privileged access with One Identity Safeguard.

"It's important to know when privileged accounts are being used and how they're being used, which is why Safeguard is extremely important for Investors Bank."

Damiano Tulipani,
Vice President of Cybersecurity,
Investors Bank

Investors Bank improves accountability to drive security

Ensures privileged accounts are properly managed and attested with the next-generation PAM solution, One Identity Safeguard.

With One Identity Safeguard, Investors Bank ...

Provides a critical layer of protection for customers' accounts and sensitive corporate data so that it can continue to build on its 90-year history of delivering competitive banking services to the residents of New Jersey and New York.

Improves security and compliance

- Increases visibility and control over privileged accounts.
- Grants and removes access automatically based on users' current roles in the HR system.
- Generates new system passwords whenever privileged access is granted.
- Records privileged sessions to ensure traceability.

Saves time and money

- Gives business users the access they need, quicker.
- Speeds the efficiency of IT, HR and audit staffers by automating — and granting clear insight into — provisioning and deprovisioning workflows.
- Improves ROI with a "fast and simple" implementation.
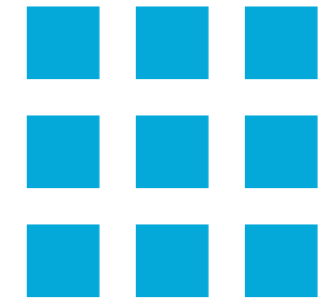
Boosts agility

- Simplifies change and growth with highly flexible and scalable privileged access controls.
- Delivers the insights IT staff need to rapidly pivot and mitigate emerging threats.

PROSEGUR

Customer Profile
Company: Prosegur
Industry: Security
Country: Spain
Employees: 160,000

To learn more, read the
Prosegur case study.

"We can see what's going on in our environment at any point in time. Now that privileged access is under control with One Identity Safeguard, we can accelerate our RPA program."

**Prasanna Kumar,
IT Architect,
Prosegur**

Securing privileged access for robotic process automation (RPA)

Prosegur uses RPA to transform its business while reducing the risk from privileged access using One Identity Safeguard.

With One Identity Safeguard, Prosegur ...

Increases its efficiency in delivering physical security-protection services for customers including banks, armored-vehicle transport companies and individuals with home-alarm systems by automating time-consuming administrative workflows.

Improves security and compliance

- Controls and records developers' access to the RPA solution.
- Protects the credentials of privileged users.
- Monitors privileged users' accounts and flags unusual behavior.
- Checks the access history of a digital workflow before granting access.
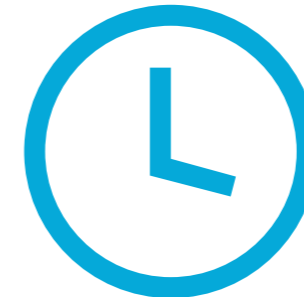
Saves time and money

- Saves 350,000 hours over two years by automating and governing administrative workflows.
- Sets up user accounts one week faster.
- Makes requested password changes one day faster.
- Speeds the creation of detailed audit trails for regulators.

Boosts agility

- Increases technology choice because developers can easily connect applications — such as Blue Prism RPA — with Safeguard through its highly flexible API.
- Frees up staff in 14 business areas to focus on value-added tasks.

"I hear compliments about how much they love Safeguard…. [It] cuts their session request time in half."

Director of Information Security

Healthcare company protects critical systems with Safeguard

Increasing accountability — and efficiency by over 66%.

With One Identity Safeguard, the healthcare company …
Meets strict laws governing patients' data privacy and enables IT staff to focus on developing solutions that can help improve patient outcomes.

Improves security and compliance

- Ensures accountability for all system access.

- Facilitates reliable PAM sessions that start and stop as required.

- Accelerates issue detection and audits with session recordings.

- Enforces strong passwords for production and non-production systems.
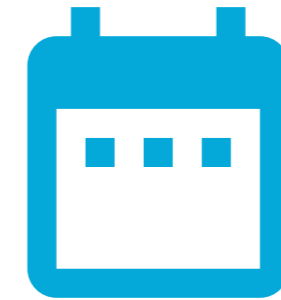
Saves time and money

- Halves session-request times for privileged users.

- Boosts efficiency by granting session approvals 66% faster, so they take less than one minute.

- Minimizes IT staff training requirements.

- Expedites the remediation of any PAM issue.

- Simplifies backup and failover configurations.

Boosts agility

- Enables approvals, anytime and anywhere, via mobile devices.

- Scales to instantly support access to 200 additional servers during peak cycles.

- Shifts the time IT staff previously spent struggling with manual PAM workflows and waiting for slow system-access approvals to time for developing innovative solutions.

Customer Profile

Company: 3DS OUTSCALE

Industry: Cloud Service Provider

Country: France

Employees: 125

To learn more, read the
3DS OUTSCALE case study.

"I no longer feel as though we can't do anything until incidents occur. With Safeguard, we can act straightaway before any damage is done."

Edouard Camoin,
Chief Information Security Officer,
3DS OUTSCALE

Tightening control of privileged access without additional overhead

3DS OUTSCALE strengthens security by automating monitoring, recording and privileged password control with One Identity Safeguard.

With One Identity Safeguard, 3DS OUTSCALE …

Drives growth by demonstrating to global customers that it can protect their hosted cloud-service infrastructures — including compute, GPU, storage and networking — from internal security threats.

Improves security and compliance

- Accelerates security-issue detection, issue tracing and auditing.

- Generates unique passwords for each session, which eliminates the use of generic passwords and password sharing.

- Increases effectiveness of security-awareness training with recorded, indexed sessions.

- Prevents errors that previously occurred from manual monitoring workflows.

Saves time and money

- Recoups 2,000 hours a year by accelerating security investigations and the creation of audit reports.

- Speeds adoption by ensuring administrators can continue to use their familiar client applications to access systems.
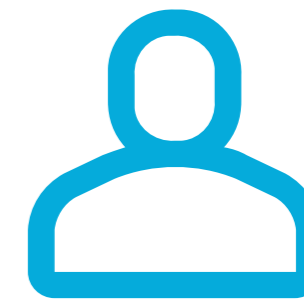
Boosts agility

- Supports varying levels of privileged access for administrators, based on their roles and responsibilities.

- Ensures internal access controls can scale with rapid corporate growth.

Customer Profile
Company: Aquila Heywood
Industry: Software
Country: United Kingdom
Employees: 163

To learn more, read the
Aquila Heywood case study.

"We were attracted by Safeguard coming as an appliance. It was more than a piece of PAM software…. Everything was pre-installed and ready for use."

Adam Livingstone,
Senior Technical Consultant for the Hosting Support Team,
Aquila Heywood

Centralized control simplifies management, boosts security

Aquila Heywood saves two days of full-time work each week on PAM processes while ensuring compliance in a more security-conscious world.

With One Identity Safeguard, Aquila Heywood …
Improves its ability to provide highly competitive, managed IT services for pension providers across the European Union that deliver mission-critical availability and security compliance.

Improves security and compliance

- Meets GDPR requirements.
- Streamlines privileged session recordings, replays and audits.
- Stores passwords in one central location and automatically rotates them.
- Ensures expert implementation.

Saves time and money

- Saves privileged access managers 16 hours each week.
- Speeds deployment with a ready-to-use, easy-to-learn PAM appliance.
- Gives support desk and product specialists faster system access.

Boosts agility

- Simplifies security changes needed to meet increasing data protection and privacy requirements.
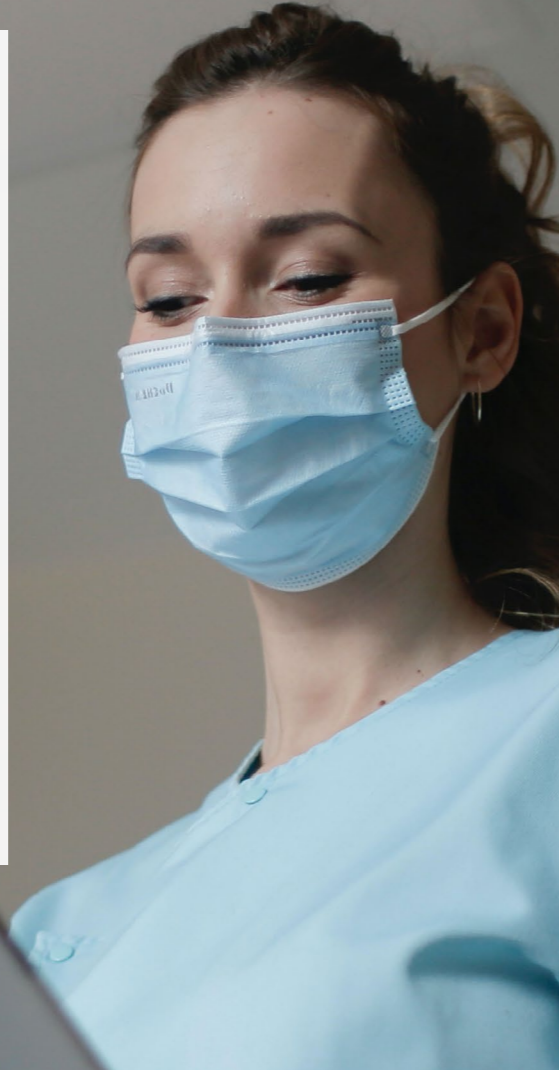- Frees up time that IT staff need to complete a critical data center refresh.

"Safeguard helps us protect sensitive member data and be compliant in managing access to our critical systems and information. It also saves us a lot of time and is truly easy to use."

**John Paul O'Leary,
Systems Operation Team Leader,
Laya Healthcare**

Better care outcomes with powerful identity management

Laya Healthcare enables faster patient services with increased security in managing privileged user access and efficient regulatory compliance.

With One Identity Safeguard, Laya Healthcare ...

Ensures privileged users who work at its offices and customers' hospitals and clinics gain quick access to the information they need to deliver effective patient care and support, while also meeting GDPR and other security requirements.

Improves security and compliance

- Accelerates threat detection because session traffic is automatically analyzed for unusual behavior.
- Centralizes PAM data, including passwords, in one security-hardened appliance.
- Simplifies GDPR compliance.
- Streamlines audits, including the generation of required reports.
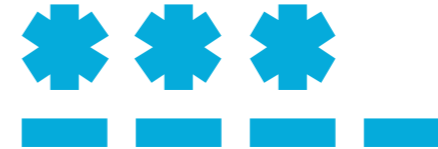
Saves time and money

- Boosts employees' efficiency in meeting patients' requirements by speeding access-request approvals by as much as 30 minutes.
- Replaces complex privileged-password change processes with a single-click procedure.
- Simplifies lifecycle management and the creation of automated workflows.
- Minimizes learning curves and disruptions to administrative processes.

Boosts agility

- Facilitates anytime, anywhere session approvals via mobile devices.
- Ensures IT staff can rapidly pivot privileged access policies and settings to support evolving requirements.

"Safeguard for Privileged Sessions is a reliable and straightforward solution, which integrated seamlessly into our existing identity management system and is able to support our needs for both Linux and Windows server access."

**Matt Magleby,
Senior Computer Scientist,
Adobe**

Internal and external security compliance

Adobe meets increasing security requirements of global cloud service customers and boosts efficiency with flexible privileged access management.

With One Identity Safeguard, Adobe ...

Protects access to tens of thousands of systems supporting its Adobe Experience Cloud users that include Fortune 100 companies in pharmaceuticals, telecommunications and other industries.

Improves security and compliance

- Cuts complexity and risk by consolidating PAM for Windows and Linux systems.

- Facilitates multifactor authentication (MFA) by integrating seamlessly with the third-party service, Okta.

- Enables long-term session storage and advanced privileged session analysis using Adobe's existing third-party solution, Splunk.

- Meets requirements for ISO 27001 and SOC 2 compliance.
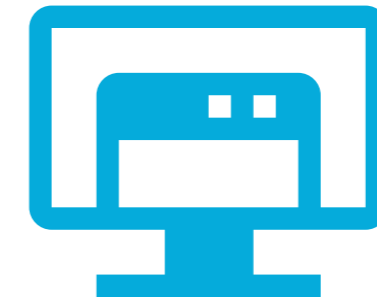
Saves time and money

- Facilitates one mobile login process that combines automated privileged-session requests and MFA.

- Gives global IT staff one solution to manage privileged RDP and SSH sessions that involve Active Directory and LDAP identity-management solutions.

- Speeds deployment and adoption by minimizing changes to administrators' workflows and tools.

- Reduces support tickets involving privileged access.
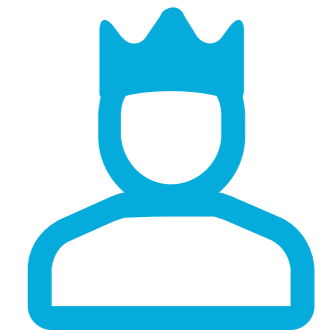
Boosts agility

- Supports Adobe's rapid increase in privileged users.

- Boosts customer responsiveness because IT staff can quickly customize privileged access to meet new requirements.

ONE IDENTITY

by Quest

Realize Your Vision with Next-Gen Privileged Access Management.

ONEIDENTITY.COM