Safeguard from One Identity (OI)

Securely store, manage and analyze privileged access

Accounts with privileged rights are the preferred target of hackers. It is essential for companies to manage privileged access effectively and securely, as they are at the core of IT security and compliance. One Identity Safeguard enables companies to minimize damage caused by data loss or misuse and provides a secure method for protecting privileged accounts and sustainably improving IT security.

A must-have: differentiated approach for privileged access

The differentiation of privileged accesses and accounts is not standard in most companies. According to the "all or nothing" principle, many users often have enormous rights that they do not need to perform their daily tasks. Since privileged accounts can be used to bypass standard controls and authorization levels, a person with a privileged account often has unlimited access and can cause significant damage to networks, servers, applications and data, either intentionally or unintentionally. This risk increases when the identity management is outsourced to external IT service providers with remote access to the company network. Without differentiation in privileged access, it is not possible to analyze and track violations and misconduct and determine appropriate consequences and measures to optimize the security.

More security and transparency thanks to multiple control mechanisms

Managing privileged accounts is about the interplay of processes, policies, and technology to ensure that privileged users with administrative rights are doing the right thing. Similar to the separation of powers of the judiciary, legislature and executive, Safeguard helps to install multiple control mechanisms in a corporate IT landscape. To this end, Safeguard not only supports a differentiated approach of access needs by administrators, it also identifies particularly risky users and compares activities based on automated workflows with applicable guidelines. In this way, the authorizations and access rights of privileged users can not only be limited, but the traceability of all activities is always also ensured. All in all, this adds an extra layer of security for privileged access, while at the same time creating all the conditions for system administrators to perform their tasks efficiently and in compliance with policies.

Product characteristics & features

- Individual security concepts for privileged passwords and sessions
- Policy-based approval control

- Identification of users at risk
- Biometric analysis of user behavior
- Real-time warnings and blocking
- Systematic command and application control via white/black list
- Support of numerous protocols (SSH, Telnet, RDP, HTTP(s), ICA and VNC)
- Drop-in deployment
- REST-based API for simplified integration of applications and systems

Your benefits at a glance

- Simplified management of privileged accounts and sessions
- Improved protection for sensitive data and corporate information
- Identification of privileged users with high risk, risky behavior and unusual events
- Mitigation of potential damage caused by security breaches
- Efficient generation of monitoring reports
- Fulfillment of compliance requirements
- Rapid payback through simplified deployment and management

„Since privileged accounts are a preferred target of hackers, the management and administration of these accounts is of particular importance for the overall IT security in a company. That is why the Safeguard runs on a hardened instance to which not everyone has access. The application offers the best possible protection for all privileged accounts by combining a session management and monitoring with comprehensive analysis options. This enables the early detection of conspicuous activities and threats plus the initiation of appropriate protective measures.“

Gerald Appel (Team Lead One Identity)