KuppingerCole Report

EXECUTIVE VIEW

by Paul Fisher | October 2019

One Identity Safeguard Suite

Privileged Access Management (PAM) has evolved into a set of crucial technologies that addresses some of the most urgent areas of cybersecurity today against a backdrop of digital transformation. One Identity Safeguard Suite is a PAM solution that uses a modular approach across password management, session management and privilege account analytics.

by **Paul Fisher**
pf@kuppingercole.com
October 2019

Content

Related Research

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 72330

Leadership Compass: Access Management and Federation - 71147

Leadership Compass: Access Governance & Intelligence - 71145

1 Introduction

In the age of digital transformation, the requirements for IT are constantly evolving. To remain relevant, organizations must reinvent themselves by being agile and more innovative. Emerging technology such as the digital workplace, DevOps, containers, security automation and the Internet of Things (IOT) continue to expand the attack surface of organizations as well as introduce new digital risks. To stay competitive and compliant, organizations must actively seek newer ways of assessing and managing security risks without disrupting the business. Security leaders, therefore, have an urgent need to constantly improve upon the security posture of the organization by identifying and implementing appropriate controls to prevent such threats. Controlling access to privilege accounts is a key area of securing the new IT landscape.

Privileged Access Management (PAM) solutions are critical cybersecurity controls that address the security risks associated with the use of privileged access in organizations and companies. Traditionally, there are primarily two types of privileged users:

1. Privileged Business Users - those who need access to sensitive data and information assets such as HR records, payroll details, financial information or intellectual property, and social media accounts.
2. Privileged IT Users – those who need access to the IT infrastructure supporting the business. Such permissions are usually granted to IT admins who need access to system accounts, software accounts or operational accounts.

In recent years the picture has become more complicated with many more non-traditional users requiring and getting privileged access to IT and business data. Some will be employees working on special projects, others may be developers building applications or third-party contractual workers.

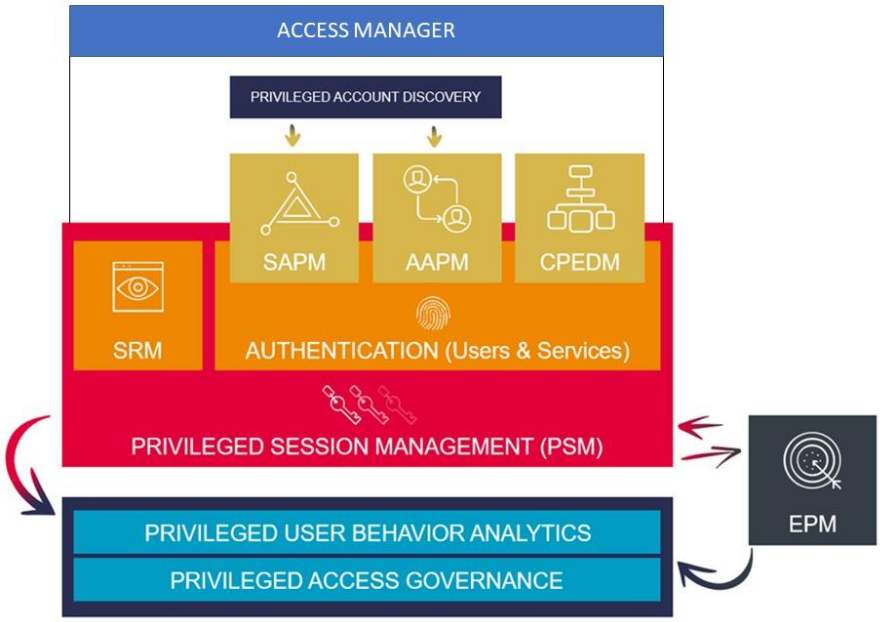
If not managed, privilege accounts provide users with unrestricted and often unmonitored access across the organization's IT assets, which not only violates basic security principles such as least privilege but also severely limits the ability to establish individual accountability for privileged activities. Privileged accounts pose a significant threat to the overall security posture of an organization because of their heightened level of access to sensitive data and critical operations.

Security leaders therefore need stronger emphasis on identifying and managing these accounts to prevent the security risks emanating from their misuse.

Existing Identity Governance and Administration (IGA) tools are purposely designed to deal with the management of standard users' identity and access and do not offer the capabilities to manage privileged access scenarios such as the use of shared accounts, monitoring of privileged activities and controlled elevation of access privileges, and ultimately perform governance actions on privileged users and elevated access. Privileged Access Management solutions address these challenges by offering specialized techniques and unique process controls, thereby significantly enhancing the protection of an organization's digital assets.

In recent years, PAM solutions have become more sophisticated making them robust security management tools in themselves. While credential vaulting, password rotation, controlled elevation and delegation of privileges, session establishment and activity monitoring are now almost standard features, more advanced capabilities such as privileged user analytics, risk-based session monitoring,

advanced threat protection, and the ability to embrace PAM scenarios in an enterprise governance program are becoming the new standard to protect against today's threats - all integrated into comprehensive PAM suites.



SRM = Session Recording and Monitoring

SAPM = Shared Account Password Management

AAPM = Application-to-Application Password Management

CPEDM = Controlled Privilege Escalation and Delegation Management

EPM = Endpoint Privilege Management

Figure 1 The essential components of recommended PAM tools (Source: KuppingerCole)

Among the key challenges that drive the need for privilege management are:

- Abuse of shared credentials;
- Abuse of elevated privileges by unauthorized users;
- Hijacking of privileged credentials by cyber-criminals;
- Abuse of privileges on third-party systems;
- Accidental misuse of elevated privileges by users.
- The requirement to perform attestations on privileged users and admin accounts

Furthermore, there are several other operational, governance and regulatory requirements associated with privileged access:

- Discovery of shared accounts, software and service accounts across the IT infrastructure;
- Identifying and tracking of ownership of privileged accounts throughout their lifecycle;
- Establishing Single Sign-on sessions to target systems for better operational efficiency of administrators;
- Auditing, recording and monitoring of privileged activities for regulatory compliance;
- Managing, restricting, and monitoring administrative access of IT outsourcing vendors and MSPs to internal IT systems;
- Managing, restricting, and monitoring administrative access of internal users to cloud services.

Consequently, multiple technologies and solutions have been developed to address these risks as well as provide better activity monitoring and threat detection. A specific area is the in-depth protection of server platforms such as Unix, Linux, and Windows. These focus on protecting the accounts such as "root" or "admin" on these systems as well as delivering in-depth protection against unwanted privilege elevation, altogether with capabilities of restricting the use, e.g., of specific shell commands. While they do not cover everything, such tools are an essential element in a holistic PAM architecture, delivering the in-depth protection for defined target platforms.

2 Product description

One Identity is an IAM company owned by Quest Software based in Aliso Viejo, California. It has a portfolio of products covering identity governance, account management, and Privileged account Management all complimented with SaaS and hybrid cloud offerings. The company's core PAM solution is One Identity Safeguard. One Identity Safeguard includes three products; Safeguard for Privileged Passwords, Safeguard for Privilege Sessions and Safeguard for Privileged Analytics. Together with the existing Unix Security solution, One Identity Privileged Access Suite for Unix, the portfolio spans all key areas of PAM for the organizations. One Identity Safeguard for Privileged Passwords and Sessions is delivered as a virtual appliance as well as a hardened physical appliance.

The underlying, unified infrastructure delivers common APIs, reporting, and roles for managing access to the various functions of the modules. The One Identity Safeguard solutions also integrate with One Identity Starling products. These are:

- Starling 2FA
  This is a cloud-based two-factor solution that provides strong authentication capabilities and flexible approvals, which are needed for approving administrator and operator access to privileged sessions as well as for the required strong authentication of such users.
- Starling Governance
  This is a cloud-based access request and access certification solution that can easily be attached to the One Identity Safeguard platform to bring a higher level of unity for IGA across standard users and privileged users, Starling Governance will be available in the mid-2020 timeframe

Beyond the core area of PAM, One Identity delivers further integrations, to its Identity Governance and Administration product One Identity Manager. This allows for implementing unified approaches for Identity Provisioning and Access Governance, covering not only standard user accounts but also the highly privileged and shared accounts.

One Identity Safeguard is a modular yet integrated solution that allows organizations to start with either monitoring sessions or managing passwords. Because their Session Management solution can be set up using transparent mode, requiring minimal changes to the network, no onboarding of assets and no changes to the way that admins gain access to credentials. This way organizations can opt to start their PAM journey with Session Management while taking additional time to on-board assets and determine workflow and policies for password management. In addition, Safeguard for Privileged Sessions provides indexed recordings of sessions making it easier to find events and create reports for management. The detail of session capture is granular; individual keystrokes, mouse clicks and windows viewed are included in audit trails which can be saved and viewed as video files for analysis. Fully searchable, these audit trails are also encrypted, and time stamped making them ideal for compliance purposes.

Session management is an important part of privilege account management as it provides insights into usage and informs decisions in future credential allocation in addition to allowing organizations to meet compliance demands. It's also important that any PAM solution alert admins to suspicious data requests as quickly as possible. Safeguard for Privileged Sessions can recognize suspicious patterns such as unusual command line requests or an out-of-the-ordinary window title. Another compelling feature is full-text search via Optical Character Recognition (OCR) of commands, metadata and text seen by the user which helps with forensics and disaster recovery operations. One Identity claims that its tool acts as a virtual firewall by switching off access to servers instantly if it sees suspect behavior.

One Identity Safeguard for Privileged Analytics is delivered as a part of the same image as Safeguard for Privileged Sessions. With the number of privileged users extending far beyond the traditional perimeter of the organization, organizations need a PAM solution that provides a well-engineered and specified analytics engine. One Identity Safeguard for Privileged Analytics tracks user activity in real-time without recourse to predefined correlation rules. It uses actual usage data from the organization to define "normal" behaviour and uses advanced algorithms to detect deviations from this baseline. The algorithms built into Safeguard for Privileged Analytics can inspect regular user behaviour captured by Safeguard for Privileged Sessions even down to mouse and keystroke activities and then search for anomalies or abuses of privileges. The solution works with SIEM tools, including Splunk and categorizes event based on risk and deviation levels, highlighting those that are judged to be most dangerous. Because of the integration with Privileged Sessions it allows immediate termination of sessions if suspicious behaviour is detected. Safeguard for privileged analytics can also be used to help determine your most risky users and accounts

The final piece of Safeguard is One Identity's solution for password management Safeguard for Privileged Passwords. The solution uses a modern GUI design for ease of use and fast access to passwords. It also offers remote management tools via secure web browser and support for mobile devices. An extension of the functionality allows admins to approve or deny an access request without being on a Virtual Private Network (VPN) through One Identity Starling. Visibility of service accounts is supported; important to keep control especially when admins allow accounts to be used in various

places. A further update will align the code base for privilege and self-service password reset and users will get access to personal vaults.

A Workflow engine provides a degree of admin flexibility, which allows access to time-limited accounts, multiple approval requests, emergency access and policy updates. Reason codes can be integrated with a ticketing system or a request can be automatically approved.

An Activity Center allows visibility of all account activity and generates customizable reports, automated and scheduled queries. Two-factor authentication is supported as standard with RADIUS based 2FA as well as offering the cloud-based Starling 2FA Authentication service. Finally, One Identity Safeguard supports Open Source with SDK for third party plugins, making it customizable within the enterprise.

3 Strengths and Challenges

One Identity has created a comprehensive set of PAM tools with the Safeguard Suite which offers the ease-of-use and flexibility needed for today's disrupted and agile workplaces. One Identity has smoothly integrated much of the Balabit technology it acquired in 2018 to create a solution that also works with its own proven identity solutions such as Startling 2FA and One Identity Manager which gives organizations the opportunity to add capabilities to include control of shared accounts and highly privileged accounts. Further customization is available through support of APIs and an SDK for third party plugins (github.com/oneidentity). Such features will be reassuring to customers who wish to have a PAM solution that can grow and change with the organization. A good example is its ability to control access to corporate social media accounts such as Twitter or Facebook.

The modular approach that One Identity has taken for its PAM solution means that organizations can choose the basic module for controlling privilege passwords and build from there. On its own, Safeguard for Privilege Passwords is well featured enough to be considered as a robust core for a PAM solution for an organization looking to control privileged access for the first time or replace an existing solution. In addition, Unix and Windows security and PAM operations can easily be added to a program through One Identity solutions such as the Privileged Access Suite for Unix and Active Roles.

One Identity has improved compatibility with supporting solutions such FIDO2, RADIUS based 2FA solutions and integration into Hashicorp Vault, which will widen secure storage to include tokens, API, certificates as well as passwords. This kind of flexibility makes Safeguard worth considering for those organizations that need to secure DevOps and agile development projects. All three modules share the same easy to understand GUI that should simplify the task of integration with the wider infrastructure as well as each other.

Furthermore, integration with Starling 2FA, and the integration options with One Identity Manager and future cloud-delivered IGA functionality make One Identity a vendor that should be considered on short lists for Privilege Access Management. This is a well-considered PAM solution that covers most of the bases for privileged management in modern computing environments.

Strengths

- Strong feature set for Session Management
- Strong feature set for Privileged Password Management
- Strong support for virtualization
- Can be integrated with One Identity Manager for full stack Privilege Access Governance
- Flexible support for 2FA for privileged access and industry identity and encryption standards
- Unified reporting, security, APIs and other capabilities
- Extends access management into new business areas such as social media and RPA.

Challenges

- More work is needed to the PAM offering to integrate into audit and analytics to improve compliance
- SaaS deployment limited to Starling currently
- Mix of cloud and on premises components could be challenging to manage
- Level of features out of the box may make it challenging for SMBs to configure

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com