KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | August 2017

One Identity SafeGuard 2.0

One Identity SafeGuard 2.0 is a re-architected, modular solution for Privilege Management, supporting both Shared & Privileged Account Password Management and Session Management, plus several additional capabilities. The product excels with its architecture, integration capabilities, and other features such as very strong workflow support.

by **Martin Kuppinger**
mk@kuppingercole.com
August 2017

Content

Related Research

Leadership Compass: Privilege Management - 72330
Advisory Note: Privilege Management - 70736
Executive View: One Identity Manager v7.0.1 - 70894
Executive View: Dell One Identity Cloud Access Manager - 71250

1 Introduction

In the age of digital transformation, the requirements on IT, but also the ways IT is done, are changing. Organizations need to reinvent themselves and become agile and more innovative, while meeting ever increasing regulation all in addition to constantly improving security, by having the right counter measures and preventing attacks. On the other hand, with the vast number of attacks that organizations are facing and the burgeoning of regulations, organizations must invent new methods of meeting these needs while still perfectly serving their customers. In addition, smart manufacturing and the internet of things massively expand the attack surface of organizations. Among the various countermeasures Privilege Management plays a central role.

Privilege Management describes the domain of technologies that help better manage and control so-called "privileged accounts", i.e. accounts having elevated privileges and thus imposing a higher risk. Such accounts also include shared accounts, which frequently have elevated privileges, but are at higher risk per se due to the nature of shared credentials. The capabilities of Privilege Management nowadays range from Shared Account Password Management to Session Management and Privileged Behavior Analytics.

Privilege Management can be considered a domain of Cybersecurity since attackers usually go after the high privilege accounts. The users of the privileged accounts have the broadest access to sensitive company data such as HR records, financial information, payroll details or a company's IP. Therefore, a strong emphasis needs to be placed on protecting these accounts, which eventually results in a reduced risk of breaches.

Furthermore, Privilege Management is an essential element in protecting organizations against attacks that are not yet identified. What commonly is called zero-day attack in fact has been running for a shorter or longer while, sometimes for years. All attacks go through a phase where they are run but are not yet detected. Traditional technologies such as signature-based Anti-Malware don't help in these scenarios. New Cybersecurity tools looking for anomalies and outliers can help identifying such long-running attacks.

Privilege Management helps in two ways in these situations. On the one hand, it increases the protection of digital assets by protecting the most critical accounts and access to these systems. On the other hand, Privileged Behavior Analytics helps in identifying anomalies in privileged user behavior.

Additionally, Privilege Management also is part of the IAM (Identity and Access Management) domain, because it is about managing accounts and their passwords, as well as their access at runtime, e.g. by monitoring sessions.

Privilege Management thus is an essential element of both Cybersecurity and IAM infrastructures of organizations. It helps in mitigating risks and in protecting the crown jewels of organizations, their valuable digital assets and systems. Thus, it is no surprise that the market for Privilege Management is evolving, with new vendors entering and new and modernized offerings delivering better ways to tackle the challenges of Privilege Management.

2 Product Description

One Identity is part of Quest Software and has been a player in the Privilege Management market for many years, with some offerings such as their Unix-to-Active Directory integration (formerly Vintela) being renowned and available for quite a long time. One Identity as a company was started after Quest Software was split from Dell and runs the IAM business, with the flagship product One Identity Manager and offerings in a variety of other areas. One of these is One Identity Safeguard 2.0, which covers the Privilege Management market.

One Identity Safeguard 2.0 has been built from the ground up in a new architecture. The decision to re-architect the One Identity solution for Privilege Management has various targets. One is decreasing the time-to-value for customers by simplifying both deployment and integration. The other major target was delivering a fully integrated solution with a consistent architecture and UI, which can be easily expanded by adding further modules.

The architecture follows the microservices paradigm, with central services such as console interfaces, APIs, authentication capabilities, workflows, internal security and access management, and reporting being delivered as central services. These services then are used by the functional modules, with three modules being available right now and additional modules being under construction. Two modules are available as of now:

- Password Module (Shared Account Password Management)
- Session Module (Session Management)

Furthermore, One Identity already plans for a third module, the Unix Security Module (Unix Session and Privilege Elevation Management), which will become available later.

The platform exposes a comprehensive set of REST APIs, uses a modern HTML5-based console also supporting mobile devices, supports standards such as OATH2, and other features. At least in the first release, the solution is available only as a hardware appliance, built on a hardened software stack, starting with an embedded OS. Particularly for the highly sensitive area of Privilege Management with storing and managing shared credentials, such an approach mitigates risks of attacks through other software components such as the host OS, guest OS, or hypervisor. The architecture is designed to be horizontally scalable, includes pre-configured clustering capabilities and active-/active configurations with multiple nodes out-of-the-box. The latter capability is rarely found, with active-/active configurations either not being supported at all or requiring massive extra effort in configuration in most other solutions in the market.

Other important areas of common functionality across the modules include a flexible workflow engine, e.g. supporting access requests and approvals for privileged accounts, and advanced audit features. The workflow engine also supports areas such as changes in access configuration settings and session settings. It also can be used for configuring emergency access. With this broad support, One Identity Safeguard excels in workflow support compared to many of the other players in the Privilege Management market.

One Identity Safeguard also provides strong integration capabilities. Privilege Management is not isolated, but has various touchpoints with other solutions. One Identity starts with integration to the 2FA (Two Factor Authentication) capabilities of its cloud-based Starling platform and the “Approval Anywhere” capability, which works flexibly across different types of devices. Safeguard also provides out-of-the-box integration to Servicenow and BMC Remedy as leading ticketing systems and, also based on the comprehensive set of APIs, allows for integration into existing IT Service Management workflows.

In the field of Shared & Privileged Account Password Management, the solution delivers the expected features such as 2FA for access to privileged sessions, discovery of privileged accounts, one-time passwords for shared accounts, and support for a broad range of target systems including servers, network devices, and applications. This area has evolved well beyond just providing one-time passwords for shared accounts nowadays. The target is to protect all access via privileged accounts.

In Session Management, One Identity Safeguard builds on a protocol-proxy technology. Communication via common protocols such as SSH or RDP is proxied through the appliance. This allows for implementing the common Session Management features such as auditing and recording sessions, but on the other hand leaves the administrative workstations unaffected. For command-line session, command detection is supported. Other features such as auto-login are supported as well.

3 Strengths and Challenges

In sum, One Identity Safeguard 2.0 is a well-thought-out solution for tackling the Privilege Management challenges organizations are facing today. The product supports the key capabilities required by customers with the initial modules, those capabilities being the management of access to privileged and shared accounts and the entire area of Session Management. Further modules covering Unix privilege elevation management as well as additional capabilities are planned.

While the hardware appliance form factor might be considered a challenge for customers focusing on highly virtualized IT infrastructures, it provides significant advantages in security through its hardened platform and ability for rapid deployments. A particular strength of One Identity Safeguard is its integration capabilities, with out-of-the-box integrations to various systems being available.

Other features such as the workflow capabilities and support for active-/active architectures also are above what is delivered by most other players in the market. On the other hand, not all functional modules are available yet. In particular, there is no Privileged Behavior Analytics module yet. However, this is commonly one of the features to be deployed by customers after the other capabilities, and integration to Identity Analytics is already planned.

In sum, One Identity is back as one of the vendors in the Privilege Management market that should be considered when evaluating products in this market segment. While there are some gaps in breadth and depth of functionality, the product excels with its modern, well-thought-out architecture, the integration capabilities, and the potential of being expanded by additional modules in a consistent manner.

Strengths	Challenges
● Strong support for discovery of accounts, Shared & Privileged Account Password Management, and Session Management ● Modern, well-thought-out and expandable architecture with functional modules ● Strong integrated workflow capabilities, specifically targeted at Privilege Management requirements ● Supports active-/active replication between various instances out-of-the-box ● Strong integration capabilities based on a comprehensive set of APIs ● Integrations to ticketing systems, cloud-based 2FA and other systems out-of-the-box ● Rapid deployment based on hardware appliance form factor ● Modern UI supporting all types of devices	● Currently only available in a hardware appliance form factor, which increases security of the solution but might be an inhibitor in some customer's IT infrastructures ● No support for Privileged Behavior Analytics yet, but integration into Identity Analytics already announced ● Some gaps in the depth of functionality, e.g. in support of older protocols for Session Management

4 Copyright

© 2017 Kuppinger Cole Ltd. All rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.