KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | January 2018

Osirium: Privileged Access Management

Osirium's Privileged Access Management provides a secure, streamlined way to monitor privileged users for all relevant systems. It manages context-driven access over any number of systems across an infrastructure, and supports an innovative, task-based approach. Furthermore, it comes with a well-thought-out gateway approach for supporting downstream applications.

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

Content

Related Research

Leadership Compass: Privilege Management – 72330

Leadership Compass: Access Management and Federation - 71102

Advisory Note: Privilege Management – 70177

Leadership Brief: Privileged Account Management Considerations – 72016

1 Introduction

Osirium is a leading software vendor for Privilege Management solutions, with specific focus on the domains of Privileged Access Management, Privileged Task Management, Privileged Session Management and Privileged Behavior Management. It was originally founded in 2008 in the UK and is privately held. Currently it has over 50 employees catering primarily to UK customers, but as of the time of writing, Osirium has also started addressing the Asia Pacific Region (APAC) and to expand into the DACH region, especially Germany. Further plans for geographical expansion include the Middle East & North Africa (MENA) region.

The decision to expand their geographical reach has been on the road map for Osirium for some time now. This approach is also centered around developing a comprehensive network of channel partners, mirroring what Osirium has been doing in the UK.

In the age of digital transformation, the requirements for IT – but also the way IT is done – are changing. Organizations need to reinvent themselves and become agile and more innovative. Smart manufacturing and the Internet of Things expand the attack surface of organizations. Also, they must meet ever increasing regulatory requirements. To stay ahead, with the vast number of attacks that organizations are facing and the evolving regulations, organizations must invent new methods of addressing these needs while still perfectly serving their customers. Thus, they also need to constantly improve security, to have the right counter measures implemented and thus prevent attacks.

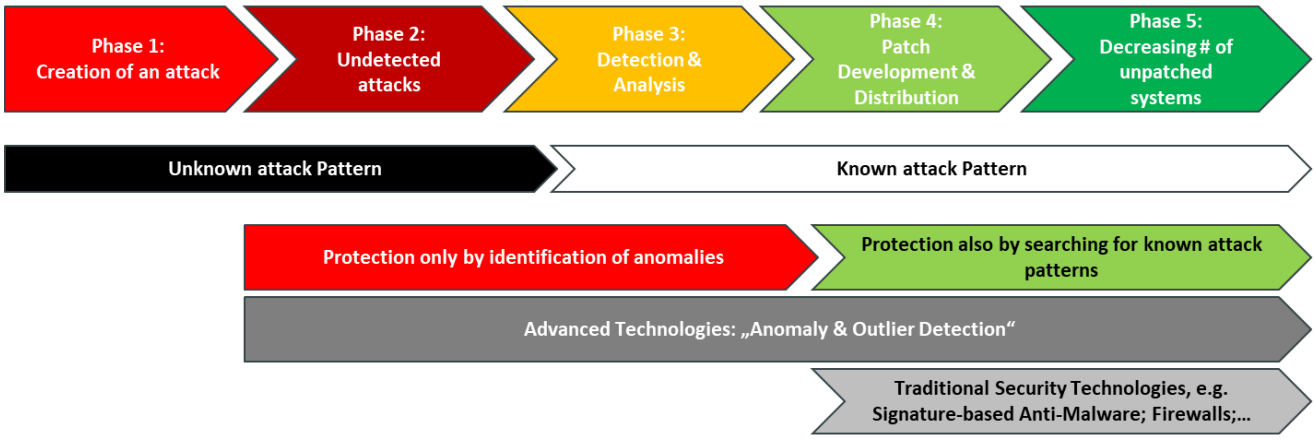

Figure 1: Phases of an attack

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. Privilege Management helps in these scenarios, by increasing the protection of digital assets through protecting the most critical accounts and access to these systems.

Privilege Management is also 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.

Modern tools for Privilege Management must support a variety of requirements, from protecting the passwords of shared accounts, rotating the passwords of service and system accounts, to session monitoring and behavioral analytics.

Mature Privilege Management solutions go much further than simple password generation and access control to individual systems, but also provide a unified, robust, and – importantly - transparent Privilege Management platform which is integrated into an organization's overall Identity and Access Management (IAM) strategy. While "password vaults" had been at the center of attention in earlier years, capabilities such as advanced analytics of privileged user behavior and advanced capabilities in session monitoring and analysis are becoming the new normal, all integrated into comprehensive suites. However, we also see a growing number of vendors taking different approaches to solve the underlying problem of restricting, monitoring, and analyzing privileged access and the use of shared accounts, such as focusing on task-based approaches for limiting the access for different types of users.

Among security risks associated with privileged users are:

- Leakage of credentials for shared accounts;
- Abuse of elevated privileges by fraudulent users;
- Hijacking of privileged accounts by cyber-criminals;
- Risks through abuse of elevated privileges on client systems;
- Risks through mistakes in using elevated privileges by users.

Furthermore, there are several areas of security, but also user convenience, with requirements which are associated with privileged accounts:

- Managing the ownership and knowing all privileged accounts, both individual and shared accounts;
- Single Sign-On to shared accounts for administrators and operators;
- Reducing elevated privileges of administrators, and in particular operators, to mitigate associated risks;
- Controls for managing, restricting, and monitoring access of MSPs when accessing internal systems;
- Controls for managing, restricting, and monitoring 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. Amongst these, we find Osirium with their approach that focuses on enforcing the least privilege principle by restricting access of users to systems through a task-based approach, which complements their overall Privilege Management suite that delivers to common requirements of Privilege Management.

For a detailed overview of the leading PxM vendors, please refer to the KuppingerCole Leadership Compass on **Privilege Management**[1].

[1] Leadership Compass: Privilege Management (#72330)

2 Product Description

Osirium offers a suite of products for Privilege Management, consisting of four modules:

- Privileged Access Management delivers the baseline functionality for managing passwords of shared accounts and enforcing least privilege access.
- Privileged Session Management provides the capabilities for monitoring and recording sessions, both command line sessions and graphical remote sessions.
- Privileged Task Management is the component within the Osirium Privilege Management solution which differentiates it from many of its competitors by delivering a well-thought-out, task-based approach for privileged activities.
- Lastly, Privileged Behaviour Management introduces behavioral analytics.

Osirium's product differs from most other PxM products currently on the market. Instead of just replicating similar Privilege Management solutions and features, their innovative approaches to the market set the Osirium products apart in this market segment. However, Osirium also provides good support for common feature sets such as Session Monitoring and Shared Account Password Management, but it is just not limited to these standard capabilities.

One area of differentiation is their task-based approach, which allows assigning restricted tasks to users. Thus, instead of granting full access to privileged accounts, customers can assign task sets to their administrators and operators, which allows implementing a real least privilege model. Osirium provides a range of pre-configured tasks across a variety of systems.

Osirium's task-based approach seamlessly integrates, e.g., with Cisco Infrastructure, but also with environments such as Microsoft SQL Server. The range of systems supported by task management and pre-configured tasks out-of-the-box is impressively large.

Osirium also supports the new area of Privileged Behavior Analytics. This new area uses machine learning technology to analyze privileged account behavior. It creates baseline behaviors for the users and privileged accounts to detect and alert the security team that anomalous behavior is taking place which may, in the long run, prevent insider abuse and breaches.

Another area where Osirium differs significantly from other vendors is their approach of using a sort of "gateway" system, which can be based on rather old operating systems. These are accessed and managed remotely, allowing the running of old software stacks that are still required for managing certain environments. Particularly with respect to the emerging demand in Operational Technology Security, e.g. for managing ICS (Industrial Control System) environments, this approach appears to be very valuable – in such environments, old software stacks are the norm, not the exception.Osirium connects the user to the remote server following a single sign-on approach, which removes the need for password files. This saves time, and generates more productivity for the user.

Osirium's Privilege Access Management has flexible, highly granular control features which reduce risk and allow the user to run the privileged commands. Furthermore, Osirium's feature of password lifecycle management makes it easier for the administrator to reset passwords and unlock user accounts

while at the same time it makes it easier for organizations to implement strong password policies. Additional features in this platform include agentless implementation, whereby no agents need to be installed and no reconfiguration is necessary on devices, servers or within desktop applications. In addition, there are also features such as password rollback, change tickets and template-based support.

In a nutshell, Osirium's Privilege Access Management seamlessly manages context-driven accesss over any number of systems across an infrastructure, particularly by assigning allowed tasks. In addition, it ensures that only authorized users have access to the use of the system and when the need expires it revokes the priviliges. Thus, it addresses security needs and compliance requirements.

3 Strengths and Challenges

Osirium's Privileged Access Management addresses security and compliance requirements by defining who gets access to what and when, based on their task approach. Thus, they can enforce a least privilege principle.

Osirium differs significantly from other vendors. While supporting core features we expect to see in Privilege Management solutions, their task concept and gateway approach add important capabilities, which are relevant to the vast majority of customers.

While offering support for common feature sets such as Shared Account Password Management or Session Management including Session Recording, there are some gaps, both in supporting specific areas such as Application Privilege Management and in-depth features. However, the main innovative feature areas such as Privileged Behavior Analytics are supported.

From our perspective, Osirium is an interesting alternative to the established players in the Privilege Management (PxM) market, and thus a strong contender, particularly because they opted for new, innovative approaches in certain areas instead of following a "me-too" approach. Despite their rather small partner ecosystem, they might be considered in evaluations to have an option for an alternative approach in Privilege Management, which might be the better fit for some customers.

Strengths	Challenges
• Task-based gateway approach allows restricting privileged access to pre-defined tasks, with a wide range of preconfigured tasks • Support for downstream target systems through "gateways" • Password never touches administrative workstations • Support for Privileged Behavior Analytics	• Lack of Application Privilege Management • Small vendor with a rather limited global scale and lack of a global partner ecosystem • Overall broad coverage of capabilities, but lack of depth in certain areas

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 global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

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