KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | August 2017

Thycotic Secret Server

Thycotic Secret Server is a mature enterprise-class offering for Privilege Management, supporting the key areas of the market such as Shared Account and Privileged Password Management, Session Monitoring, Account Discovery, and others. The solution convinces with its approach for rapid deployment and an overall strong feature set.

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

Content

Related Research

Leadership Compass: Privilege Management - 72330
Vendor Report: Thycotic - 71112
Snapshot: Thycotic Secret Server - 70633

1 Introduction

In the age of digital transformation, the requirements for 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 exposing a higher risk. Such accounts also include shared accounts, which frequently have elevated privileges, but are at even higher risk due to the nature of shared credentials. The capabilities of Privilege Management services 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 are called zero-day attacks have usually, in fact, been running for a shorter or longer period of time, 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 identify 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.

When looking at the core area of Privilege Management, we expect to see Shared Account Password Management, Privileged Single Sign-On, Privileged Account Discovery and the management of their lifecycles, and Session Monitoring capabilities, which are a common feature in products nowadays. The main features we look at in these areas include, but are not restricted to, the following:

- Shared Account and Privilege Password Management
  - Central management of shared account privileges
  - Automated credential rotation or OTPs
  - Secure Access to privileged credentials
- Privileged Single Sign-On (SSO access to multiple privileged sessions)
  - Simple management of session assignments to users
  - Ad-hoc and upfront authorization of access with support of approval lifecycles
  - Simple yet secure UIs
- Privileged Account Discovery and Lifecycle Management
  - Automated discovery of privileged accounts on servers, clients, and other systems in scope (e.g. network devices)
  - Integration into CMDBs
  - Simple (automated) grouping of accounts and systems
- Session Monitoring, Analysis, and Recording
  - Session Monitoring
  - Session Recording
  - Session Analysis
  - All for both CMD based and GUI based sessions

2 Product Description

Thycotic is a Washington DC based software vendor, incorporated in May, 2000. Thycotic provides Privilege Management and Active Directory self-service solutions. Their approach is similar to most of the other vendors in this space, and they offer a full featured Privilege Management product. The company is privately held and recently funded by Insight Venture Partners. Thycotic is shedding the "underdog" label and becoming a globally distributed, enterprise ready solution. Thycotic has achieved this by coming from the lower end of the market and steadily making their way into enterprise level clients, helping some very large organizations enhance their privilege security program .

Thycotic is a very interesting and "young-minded" vendor, in that they focus very much on features supporting the emerging platforms such as support for REST and cloud services. They have gone from

being a pure Shared Account and Privileged Password Management software vendor to now offering a full-fledged Privilege Management platform ready for global enterprises.

Thycotic offers their Privilege Management solution, Secret Server, in two deployment models: on-premises leveraging the Microsoft stack and Software as a Service (SaaS) delivered from the Microsoft Azure platform. Secret Server is an application which relies on Microsoft Technology regarding web and application server technology. It provides a secure storage for information based on AES 256 encryption. Passwords are stored in a Microsoft SQL Server database which can be mirrored. All communication is encrypted. The use of a Microsoft SQL Server and the Microsoft infrastructure factually means that deployment is straightforward, but no specific hardened platform is offered. Thycotic has opted to deliver their solution on technology that is most readily available in organizations, allowing for rapid installation and implementation. Furthermore, advanced configuration such as active-/active-replication must be configured at the level of Microsoft SQL Server. On the other hand, Thycotic's cloud deployment overcomes the potential challenges associated with installing and maintaining the required Microsoft infrastructure.

The common frontend nowadays for all management tasks is browser-based. Additionally, mobile interfaces are provided. Based on the extensive set of REST-based APIs, further integration with existing applications and automation is straightforward.

The internal management concept is well-thought-out. Security is based on a role concept based on pre-configured roles, which can be tailored to the specific needs of customers. Furthermore, there are features such as 2FA (Two Factor Authentication), workflows for custom approvals, and other capabilities such as SIEM integration (Security Information and Event Management), real-time alerting and other important capabilities.

The system supports a variety of target systems, from RDP, SSH session, and PuTTY to managing Cisco environments, Unix and Linux servers, Windows server, VMware ESX, a variety of databases, IBM Mainframes, and other systems. On the other hand, there is also integration e.g. into Microsoft Active Directory for obtaining account information, into CMDBs, and other systems.

For the target environments, capabilities such as the management of passwords and their automated rotation, single sign-on access to sessions, session monitoring, and others are provided. Account discovery is another important feature of the product. Overall, all major features listed as requirements for that type of product are supported at a good to excellent level, providing a comprehensive solution for the core areas of Privilege Management. Notably, Thycotic offers additional products for Privileged Behavior Analytics and for Endpoint Privilege Management, thus also covering the emerging areas in the Privilege Management market.

Auditing is also supported, including out-of-the-box-reports targeted at the specific requirements of various compliance regulations, as well as the ability to create custom reports that tailor to the organization's requirements

Thycotic Secret Server is available in a free 25 user edition, which is restricted to the basic password vault and management features, and in two other editions. The professional edition provides the baseline capabilities for Privilege Management. This edition is also available from the cloud. The

premium edition adds workflow capabilities, service account management, and additional integration features. Some other features such as high availability and disaster recovery support are add-ons.

Despite the need for various Microsoft infrastructure components, Thycotic Secret Server counts amongst the tools in the market segment that are easiest to deploy. This is due to the heritage of Thycotic starting at the small end of the market, where complex and long-running deployment projects never have been an option.

3 Strengths and Challenges

Thycotic nowadays has numerous high-profile clients, and Secret Server has proven to be a mature enterprise class solution. Thycotic Secret Server would fit well into any organization looking for a good, reliable and comprehensive Privilege Management solution. A strength of the product is support for rapid deployment, based on the long-standing experience of Thycotic with a very large number of smaller customers where complex deployments involving professional services will not work.

Recently, they have added Privileged Behavior Analytics capabilities which, however, aren't yet feature-complete and are not fully integrated with Secret Server. Furthermore, there is a solution for Endpoint Privilege Management available from Thycotic as well, allowing for application whitelisting and privilege elevation.

From our perspective, Thycotic Secret Server is an interesting alternative to the established leaders in the Privilege Management market, providing a number of innovative features and strong capabilities in the key areas of Privilege Management.

Strengths	Challenges
• Supports a broad number of systems • Automatic password rotation of system accounts • Simple implementation & user friendly • Historical Auditing • Web and mobile access • Session monitoring capabilities • Strong set of APIs	• Still limited partner ecosystem • Can only be implemented on a Microsoft stack, optionally available as cloud deployment • Some features only available as add-on

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