KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | August 2020

Cygna Auditor Platform

The Cygna Auditor Platform is a unified environment for collecting events from Active Directory, Azure AD, Windows Servers, Microsoft 365, and some other platforms, and providing analytics and alerting on these events. It incorporates the former BeyondTrust Auditor Suite. The Cygna Auditor Platform is a solution targeted on administrators of Microsoft Windows-centric environments, but also supports management of hybrid infrastructures.

by **Martin Kuppinger**
mk@kuppingercole.com
August 2020

Content

Figures

Related Research

Advisory Note: Future of Identity Management – 71303
Advisory Note: Redefining Access Governance – beyond annual recertification – 72579
Advisory Note: KRIs and KPIs for Access Governance – 72559
Leadership Brief: Find your Route from SIEM to SIP to SOAR – 80008
Leadership Brief: 10 Top Trends in IAM – 80335

1 Introduction

With the IT landscape changing from traditional network infrastructures with a perimeter protecting the internal systems to a more open and heterogeneous infrastructure, the focus of protecting sensitive corporate information has gradually shifted towards discovery and mitigation of threats, by both external and internal attackers. Reliable and comprehensive tools for managing and monitoring systems and analyzing the state and activities on these systems have become essential.

There are various levels such systems can operate. We find tools local to specific environments, both built-in and provided as add-on solutions. There are integrated capabilities offered by some of the cloud services for advanced analytics. There are SIEM (Security Information and Event Management) offerings, helping to collect and analyze information from a broad range of systems, offered as both tools and managed services. And there are products that help in managing a certain set of systems, bridging the gap between system-specific and built-in (native) solutions and the rather complex SIEM tools, that are targeted at enterprise-level solutions in larger organizations.

There are pros and cons for each of these approaches. Native tools are immediately available, without extra investment. However, they frequently fall short in functionality and are insufficient for the complex security challenges businesses are facing today. Integrated capabilities provided by cloud services also commonly are limited to that specific service, and only some of the cloud services provide mature and advanced integrated capabilities.

SIEM solutions, which have been positioned as the ideal solution for many years, are complex to implement and use. While managed service offerings might help in deploying SIEM solutions, these frequently are beyond what many organizations need. Furthermore, they are targeted at enterprise-level, cross-system deployments, leaving a gap for the use cases where administrators of a certain part of the IT infrastructure require specialized solutions with deep out-of-the-box integration into their system environment.

Common scenarios for specialized solutions that can manage certain parts of the environment include

- Solutions for managing Microsoft Active Directory, Windows file systems, and the related environments
- Solutions for managing Linux and Unix environments
- Solutions for managing enterprise business applications such as SAP

For the first group of solutions, there are two common scenarios. On one hand, there are the small to mid-market businesses in which such environments commonly form a major part of the IT infrastructure that is centered around Windows Servers. On the other hand, most larger organizations run a Windows infrastructure, with the administrator teams requiring specialized tools for the in-depth management of these.

While the requirements are changing, on-premise Microsoft Active Directory and Windows Servers are still widely deployed and used. While Microsoft 365 with Azure Active Directory and Office 365 is also used on broad scale, most organizations still are (and will remain) in a hybrid mode for long, thus requiring tools that help their teams managing these environments.

Cygna Labs is a provider of a set of such solutions. They recently acquired the former BeyondTrust PowerBroker Auditor product suite, which now is brought to market as part of the Cygna Auditor Platform. Cygna Labs has been founded by the team of people that developed the Blackbird Management Suite, which was acquired by BeyondTrust back in 2012 and formed the foundation for the BeyondTrust PowerBroker Auditor.

2 Product Description

Cygna Labs with their Cygna Auditor Platform is focusing on providing insight into the logs and thus activities of Microsoft Active Directory, Windows file system, other Windows (Server) security logs, but also Microsoft Office 365, Azure Active Directory, and VMware vCenter. It thus is a platform focused on a specific part of the IT infrastructure that is common to the vast majority of organizations. The target of Cygna Labs is providing centralized, unified insight and capabilities for analyzing events and alerting on these across all these systems.

In contrast to other solutions, the Cygna Auditor Platform provides both agent-based integration into Microsoft Active Directory (AD) and agentless integration, depending on the customer's infrastructure and requirements. It can gather all AD changes even if native event logging is not enabled in AD, based on the agent-based collection setup

With these systems forming a central part of the IT infrastructure, failure and attacks can cause major disruptions to businesses, but also cause audit failures. With the platforms commonly being operated by separate teams, the Cygna Auditor Platform also adds to the overall security and system management toolset required in large organizations.

Cygna Auditor provides a single, centralized console to manage all of the platforms mentioned above. The web-based user interface comes with dashboarding and management capabilities, delivering a unified view across events and alerts an all systems. It communicates with the central Cygna Server that runs on a Windows Server. The information collected from the range of supported systems is stored in the Cygna Database, which is based on a Microsoft SQL Server. For the systems running on premises, Cygna provides agents that can sit e.g. on Microsoft Active Directory Domain Controllers and on Windows File Servers. Data from Microsoft 365 including Microsoft Azure Active Directory and Office 365 is collected directly from these services by the Cygna Server and also stored in the Cygna Database.

This results in the Cygna Database becoming the central repository for all relevant data collected across the range of supported systems, and the Cygna Server delivering the analytical capabilities and alerting. Additionally, with the Cygna web console, there is a modern user interface providing detailed insight and analytics on all collected events.

The capabilities of the Cygna Auditor Platform support five distinct areas:

- Audit & Alert: At the core are the audit functions, tracking and analyzing changes to understand which changes occurred when and where, and who initiated these changes. Based on defined rules, alerts can be raised in case of critical or fraudulent changes. As mentioned, this analyzes spans the whole range of systems supported by the Cygna Auditor Platform.

- Protect: Additionally, Cygna Auditor can, based on its agent, lock down critical parts of the Active Directory and protect it against unauthorized and fraudulent changes and deletions. This also protects against access using the native tools at that platform.
- Discover & Inform: Beyond the manual insight into audit logs and the automated alerts, the platform also comes with comprehensive reporting capabilities, which e.g. simplify the task of delivering audit-relevant data to internal and external auditors.
- Recover & Rollback: Based on the tracked events, there is also support for rollback of changes and restore of Active Directory settings, allowing to return to a defined state. Furthermore, Group Policies also can be saved and restored.
- Manage: This capability is provided by the single management console that already has been mentioned above. In contrast to native solutions, this provides insight across multiple elements of common Windows infrastructures, and adds detailed insight.

With these features, the Cygna Auditor Platform provides a comprehensive set of capabilities for auditing and managing Windows Server environments, plus integration into the related cloud services delivered by Microsoft 365.

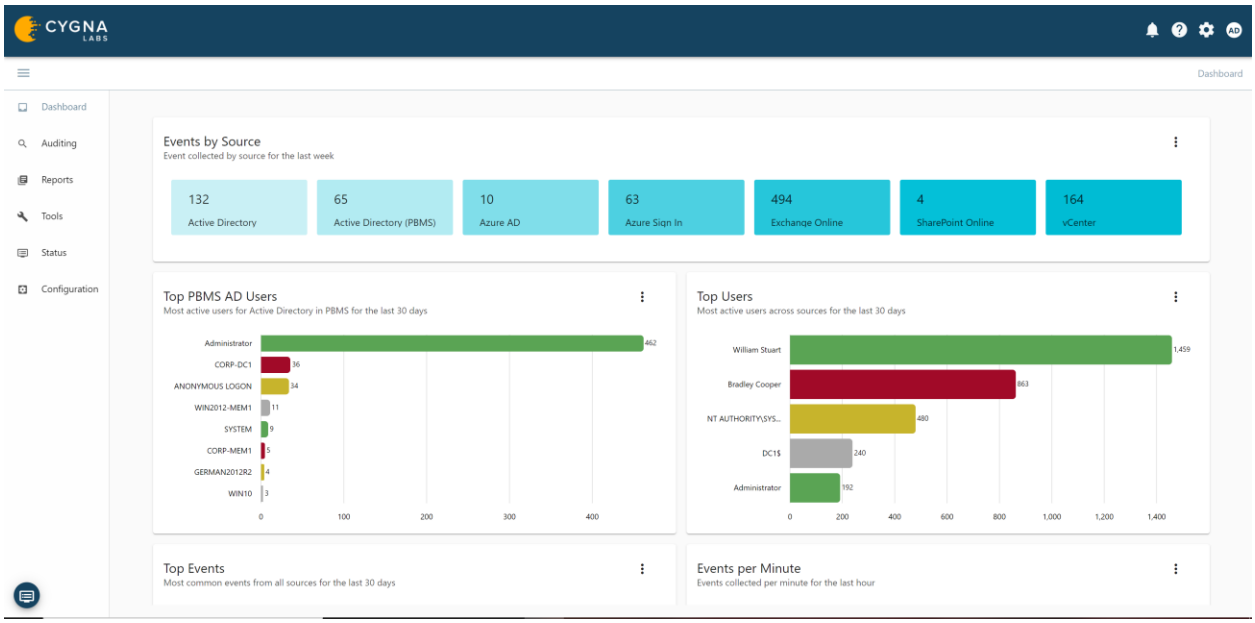

Figure 1: The Cygna Auditor Platform comes with a modern UI and already provides integration back to BeyondTrust Auditor

With the acquisition of the BeyondTrust Auditor Suite, Cygna Labs supports existing customers of that product suite, while integrating the offerings and extending it by the new, modern user interface and the integrations to Microsoft Office 365 and Microsoft Azure Active Directory. Cygna Labs already has communicated a roadmap for integration and further enhancements and, at the time of writing, can integrate BeyondTrust Auditor as a data source into the Cygna Auditor user interface. Thus, customers can search and run reports plus receive alerts based on their existing data, but will benefit from the new UI and extended capabilities of Cygna Auditor. These include, amongst others, the support of Microsoft Teams, of NetApp environments, of AWS events, and improved alerting capabilities based on machine

learning.

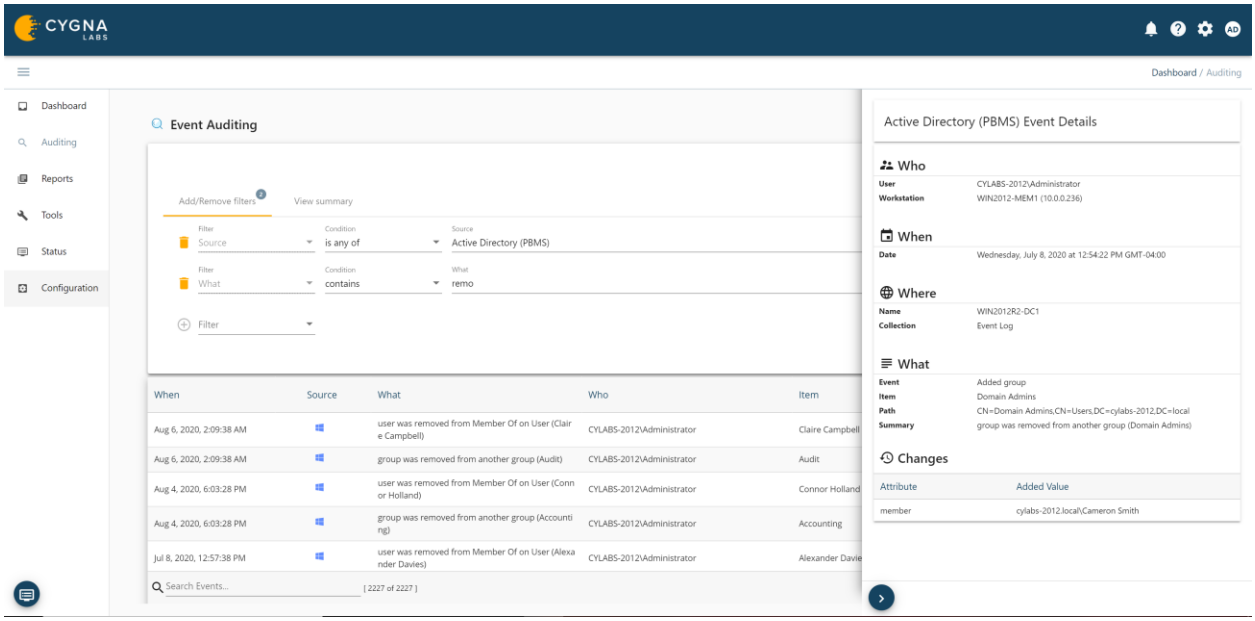

Figure 2 Cygna Auditor Platform provides access to BeyondTrust Auditor logs via its own user interface.

3 Strengths and Challenges

Cygna Labs provides a comprehensive solution for managing Windows Servers in conjunction with the increasingly common Microsoft 365 infrastructures many organizations are running. The solution comes with a modern UI and strong dashboarding, reporting, and analytical capabilities and is well-suited for both the IT teams of smaller organizations and the specific requirements of the Windows management teams in larger organizations. With adding Microsoft 365 to the list of supported systems, the focused approach chosen – in contrast e.g. to SIEM tools – is valid for these scenarios.

The company has a long legacy in creating such solutions and also provides a strategic path for customers running the BeyondTrust Auditor Suite. It thus also can build on a significant customer base and should be able to grow its partner ecosystem quickly.

Cygna Labs also has started adding support for other systems and environments such as Microsoft Teams and AWS. We consider this strategy as well-thought-out, providing a broad coverage of the solutions that are common to many of the small to mid-market organizations.

Cygna Labs on the other hand will need to increase its visibility in the market, where taking over the former BeyondTrust Auditor Suite should help. Currently, brand recognition is still low.

Strengths	Challenges
• Clear focus on common Microsoft/Windows environments • Already added Microsoft 365 environments, thus supporting the common scenarios of many customers	• Still low brand recognition of Cygna Labs • Need to grow their partner ecosystem globally, but building on former BeyondTrust Auditor Suite partners should help

• Serves both small to mid-market organizations being focused on Microsoft Windows and Microsoft 365 as the Windows administrator teams in large organizations • Modern user interface with strong dashboarding and reporting capabilities • Significant customer base due to acquisition of former BeyondTrust Auditor Suite • Defined roadmap for integration these assets with the Cygna Auditor Platform • Experienced leadership team	• Shift from on premises environments to cloud services will require continuous evolution regarding supported systems

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**

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