kuppingercole ANALYSTS

Executive View Pathlock Cybersecurity Application Controls

Martin Kuppinger

March 24

This KuppingerCole Executive View report looks at Pathlock Cybersecurity Application Controls (CAC), a solution for managing cybersecurity for SAP. A technical review of the solution is included.

Content

Figures

Introduction

SAP is the leading vendor of Line of Business (LoB) applications. Their applications covering Enterprise Resource Planning (ERP) and many other use cases form the backbone of business operations in many organizations, ranging from medium-sized business to the world's largest organizations. Aside from SAP, there are many other vendors. In addition, the SAP portfolio is becoming more diverse regarding architectures, implementation, and deployment models.

Taking such a central role in organizations, SAP systems of different types and other LoB systems operated in different deployment models, need special care from security teams that understand the specifics of these environments, and are equipped with specialized tools. SAP/LoB Security Solutions are essential for improving the security posture in the business application environments and mitigating risks to these core LoB applications.

There are various challenges organizations are facing for improving the security posture of their SAP and LoB application environments:

- System hardening: System hardening in SAP/LoB landscapes requires specialized solutions covering all elements of complex environments, from operating systems and databases to the business applications.
- Patch deployment: Deliver patches and hotfixes in a controlled, efficient manner without disrupting operations.
- Code vulnerability analysis: The specific programming languages used such as ABAP (Advanced Business Application Programming) require specialized tools for enforcing code security.
- Log analysis & threat detection: Complex, large-volume log information needs to be understood for extracting information about concrete threats.
- Heterogeneous environment support: The LoB landscape is becoming increasingly diverse, requiring solutions that support a range of different types of applications and deployment models.
- Siloed organizations: Many of these applications are still managed by dedicated teams residing in a distinct organizational unit. Integration with the broader cybersecurity and system administration teams is essential.
- Data Security: Dynamically masking and restricting access to sensitive production data based on user attributes and other customizable policies. Additionally, scrambling data to ensure security of replicated test data in non-production environments, when data is in transit, or when direct access to the database is possible. Dynamic data security controls are essential to ensure comprehensive protection of production and non-production data, as well as enforcing data loss prevention (DLP) mechanisms.
- Dynamic Access Control: Expanding access controls beyond a traditional, inflexible role-based access control (RBAC) security model with dynamic policies and attribute-based access controls (ABAC). A policy-based approach is important for managing access securely and effectively across an infinitely growing number of users and applications as organizations scale and migrate to S/4HANA.

Holistic SAP/LoB Security solutions support customer organizations in mitigating cybersecurity risks to their business application environments, both with specialized capabilities and in integration to other security systems such as centrally deployed and managed SIEM solutions. Traditionally, such solutions only cover specific capabilities that help in better protecting one security aspect such as code security. Modern cybersecurity best practices require a holistic and integrated security platform approach to improve the overall security of these environments. The various solutions on the market differ in both breadth and depth of capabilities as well as in their ability for supporting the wide range of existing SAP and other LoB applications, services, and environments.

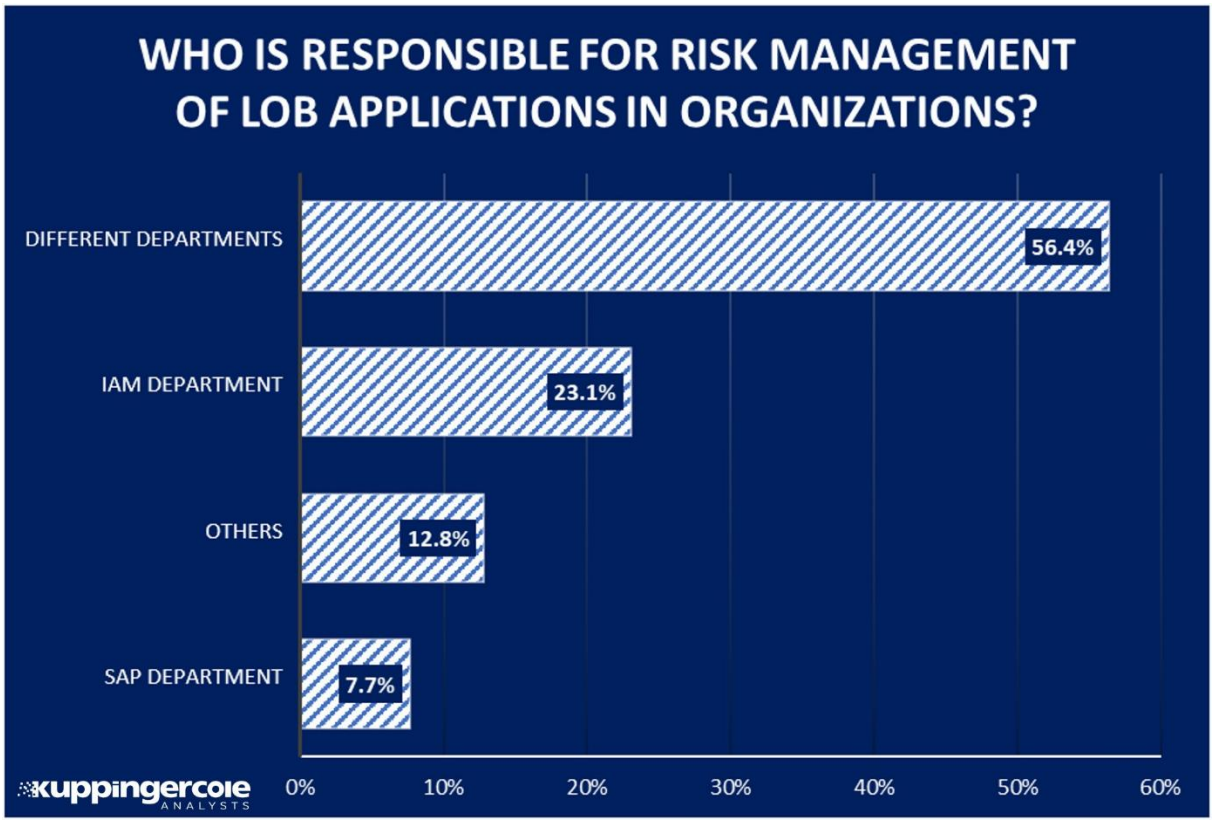

Figure 1: Risk Management and Security are still not handled consistently in organizations.

Pathlock is one of the vendors in this market, delivering a range of capabilities with their Cybersecurity Applications Controls offering.

Product Description

Pathlock, previously Greenlight GRC, is a leading provider of application access control and security solutions for SAP and other LoB environments. The company has acquired several other vendors in the past, including the SAST portfolio by Akquinet, CSI, Appsian, and SecurityWeaver.

Pathlock, while being most known for its application access control solutions that support organizations in managing access entitlements, Segregation of Duties (SoD) controls, and critical access risks for SAP and dozens more ERPs and LoB applications, also provides a

growing set of SAP/LoB security solutions. These are named “Cybersecurity Application Controls” (CAC) and form a separate part of the Pathlock portfolio. They are provided as part of the Pathlock Native Platform (legacy), which are the SAP-focused components utilizing an ABAP-native architecture. The focus of Pathlock for these components thus, as of now, is on the SAP ECC and S/4HANA environments.

The product consists of five distinct modules:

- Dynamic Access Controls (DAC) for masking data at runtime, securing replicated test data in non-production environments, preventing unauthorized transmission of data, and dynamically regulating user access via an attribute-based access control (ABAC) model.
- Threat Detection and Response for real-time threat monitoring, log analysis, and remediation.
- Transport Control for monitoring and securing SAP Transport Management System (TMS).
- Vulnerability Management for identifying and patching system, configuration, and custom code vulnerabilities and weaknesses.
- Code Scanning for scanning ABAP code and identifying security vulnerabilities, backdoors, and compliance violations within custom developed SAP environments.

Dynamic Access Controls (DAC) is a module that is rarely found in this type of solution. It enables organizations to define that sensitive information such as salary and credit card numbers, be masked dynamically, based on customizable policies. Additionally, Data Scrambling anonymizes sensitive data and secures duplicate test data in non-production environments and data in transit. These data governance policies provide a significantly higher level of granularity than could be achieved via role-based approaches, given that they add another level of control at the field, application, and database levels. Policies can be implemented centrally across business applications and do not require specific coding or customizations at the application level.

Session Logging and Data Loss Prevention (DLP) functionalities enable organizations to monitor sessions for a range of signals. These include logins, but also data access such as the download of large amounts of data. Additionally, data in downloads and exports can be blocked or masked to secure sensitive information, again based on the centrally managed dynamic data governance policies.

The Dynamic Access Controls (DAC) module is closely integrated with the Threat Detection and Response module. Pathlock CAC’s Threat Detection and Response module scans up to 67 different log files (including SAP Cloud Logs) in SAP environments. The module can extract security-relevant log entries and correlate these for identifying complex threats.

Additionally, by integrating user and entity behavior analytics (UEBA) and automated response mechanisms, the module is adept at rapidly identifying and mitigating SAP security threats. Integration is supported to any commonly used Security Information and Event Management (SIEM) tool and ensures a comprehensive and centralized overview of relevant security data. This enables real-time critical event analysis, streamlines incident response and management, and simplifies compliance efforts. Overall, Pathlock’s Threat Detection and Response module delivers 1500+ OOTB, customizable threat detection signatures and

supports continuous monitoring of SAP environments to help organizations detect both internal and external threats in real-time.

A specific area of securing systems is Transport Control. SAP environments utilize the SAP TMS (Transport Management System) for deploying changes to SAP environments. In the absence of appropriate security measures, vulnerable code, manipulated data, and other malicious activities could be injected into the SAP systems during these change management processes. The Pathlock Transport Control module enhances the SAP Transport Management Systems (SAP TMS) and delivers 90+ OOTB, customizable security checks. The module continuously monitors, reviews and, if required, blocks transports with potentially malicious content. The module works based on preconfigured and customizable security controls and rules.

One of the most powerful capabilities of Pathlock Cybersecurity Application Controls is the Vulnerability Management module that provides 4000+ OOTB, customizable scans and supports two distinct capabilities. The first is orchestration of audit campaigns to monitor systems, configurations, the database, and automating the prioritization of necessary steps to remediate identified vulnerabilities and weaknesses across the aforementioned components. Specifically, technical configurations, SoDs, critical user authorizations, and role quality are vetted for potential vulnerabilities. This ensures the secure and efficient management of user access reviews (UAR campaigns), SoD risk analysis tasks, and other access-related tasks.

The second is auditing and monitoring SAP environments for their state of security configuration and current posture of security patches and hotfixes. A dynamic dashboard with customizable widgets and drill-down functionality enables a comprehensive view and detailed insights into monthly SAP security patches and system security and implementation status. This provides an analysis of which patches are applicable and prioritizes which are most critical to your unique SAP environment. Specifically, the module facilitates prescriptive remediation and targeted deployment of patches but does not yet support automated deployment of patches.

The Code Scanning module enhances the SAP ABAP Test Cockpit (SAP ATC) and provides 150+ OOTB, customizable security and compliance checks. The module automates vulnerability scanning for ABAP custom code, enabling organizations to identify potential weaknesses and compliance violations in the code they have developed and want to deploy. This capability enables organizations to identify security vulnerabilities early in the development lifecycle and eliminates the chance of introducing vulnerable code to production SAP systems. This helps in reducing downtimes from taking production systems offline to correct ABAP code errors.

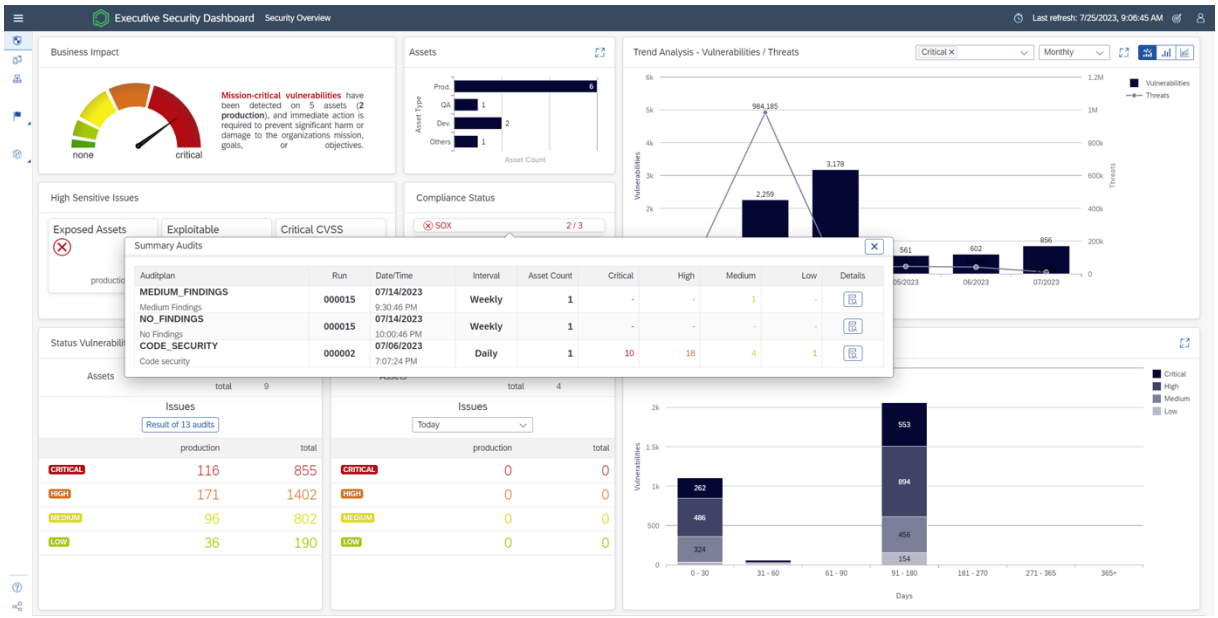

Figure 2: Pathlock CAC provides modern dashboards for users to access the status and drill down into details.

With the various modules, Pathlock Cybersecurity Application Controls provides a powerful set of capabilities for securing SAP environments. The solution is closely integrated with SAP ECC and S/4HANA and is delivered on-premises, using SAP-native interfaces.

Pathlock also provides a wide range of integrations to other solutions such as a wide variety of Security Information and Event Management (SIEM) product, Microsoft Entra ID (formerly Azure Active Directory), ServiceNow and their ITSM (IT Service Management) solution, SAP Solution Manager (SolMan), and many others.

The solution is well-suited for SAP customers that continue to run their SAP solutions on-premises, as well as for customers with S/4HANA or undergoing S/4HANA migration.

Strengths and Challenges

Pathlock Cybersecurity Application Controls is a unique solution in this market segment. It covers several of the relevant capabilities and differentiates itself with data-focused security controls. Currently, it lacks support for a broader set of LoB applications beyond SAP.

Among the weaknesses, there is a lack of automation for deploying patches and hotfixes. Automated deployment of patches is near-term on the CAC roadmap and is currently being developed with expected functionality by the end of 2024.

We expect to see significant progress in some of these areas, with the overall strategy of Pathlock being focused on support for multi-vendor LoB environments and continuous expansion of functional capabilities.

Customers with business applications being centered around on-premises SAP ECC, public and private cloud S/4HANA, SAP BTP, and hybrid deployments are well advised in evaluating the Cybersecurity Application Controls product from Pathlock as a solution for strengthening the cybersecurity posture of their SAP environments.

Strengths

- Proven solutions for addressing security challenges in SAP environments
- Broad set of capabilities for securing SAP environments
- Neat integration for SAP ECC on-premises and S/4HANA cloud deployments
- Excellent coverage of SAP specifics such as log files
- Facilitates prescriptive remediation and targeted deployment of patches based on applicability, criticality, and priority for customers' unique SAP environment.
- Close integration to application risk management capabilities provided by Pathlock
- Experienced services and support team
- Rarely found data masking, data scrambling, data loss prevention (DLP), and attribute-based access control (ABAC) capabilities with a policy-based approach

Challenges

- Currently only supporting on-premises SAP ECC, SAP BTP and S/4HANA cloud deployments, but no other LoB applications
- No support yet for automation of patch / hotfix deployments
- Code vulnerability analysis not supporting Java, but only ABAP

Related Research

Executive View Pathlock Platform
Leadership Compass Access Control Tools for SAP Environments
Leadership Compass Access Control Tools for Multi-Vendor LoB Environments

About KuppingerCole

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

Copyright

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.

KuppingerCole Analysts support 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.

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