LEARNING MADE EASY

Pathlock Special Edition

SAP Application Security

for dummies®

A Wiley Brand

Get clean

Stay clean

Optimize governance

Brought to you by

pathlock

John Carucci
Keri Bowman
Kyle Benson

About Pathlock

The Pathlock platform protects the leading enterprise business applications and the critical transactions they power. Pathlock's application governance solutions help companies enforce GRC controls and take action to prevent loss. Enterprises can manage all aspects of application governance in a single platform, including user provisioning and temporary elevation, ongoing user access reviews, control testing, transaction monitoring, and audit preparation.

SAP Application Security

Pathlock Special Edition

by John Carucci, Keri Bowman, Kyle Benson

for dummies®
A Wiley Brand

SAP Application Security For Dummies®, Pathlock Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-394-23624-4 (pbk); ISBN: 978-1-394-23625-1 (ebk);
ISBN: 978-1-394-28359-0 (epub). Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager and Editor: Carrie Burchfield-Leighton
Sr. Managing Editor: Rev Mengle
Acquisitions Editor: Traci Martin
Client Account Manager: Jeremith Coward

Introduction

Securing your data and critical business systems is now more crucial than ever, particularly when protecting the fundamental systems that form the backbone of your organization's core business operations. The protection of data and systems is achieved through SAP application security, which involves vigilant monitoring and control of access, both internally and externally.

SAP is a major component in an extensive network of business processes that can span diverse application domains. Securing access to your SAP environment requires enhanced interoperability and extensibility. Addressing this requirement necessitates the deployment of innovative tools designed to manage the evolving landscape of SAP application security.

About This Book

SAP Application Security For Dummies, Pathlock Special Edition, covers a variety of measures, including access risk analysis, compliant provisioning, elevated access management, risk quantification, threat detection, and other capabilities. This book goes beyond conventional SAP tools and offers insights into optimizing the management of your SAP application security.

You also discover Pathlock's comprehensive SAP application security capabilities. Pathlock's approach includes Continuous Controls Monitoring (CCM) and more — all requirements for effective security.

This book also appeals to non-SAP-focused individuals, such as internal auditors, by demonstrating a breadth of capabilities to solve issues beyond the SAP domain.

Icons Used in This Book

What's a *For Dummies* book without icons pointing out pertinent information that quickly gives you what you need and lets you get on your way? Here's a brief description of the icons used in the book:

REMEMBER

This icon marks a generally interesting and useful fact — something you may want to remember for later use.

TIP

Tips point out helpful suggestions and useful nuggets of information that may save you time or frustration.

WARNING

The Warning icon highlights lurking danger. With this icon, we tell you to pay attention and proceed with caution.

Beyond the Book

This book is intended to help you along the path toward an SAP application security strategy that's built on best practices, designed for scale and efficiency, and can help you maximize the ROI of your existing investments. To learn more about the solutions in this book, visit `www.pathlock.com/sap` and get a free demo.

IN THIS CHAPTER

- Looking at the existing state of affairs
- Considering a new approach
- Implementing application access governance

Chapter 1
Understanding the Value of SAP Application Security

Providing application access is a major risk factor when it comes to rising cyber threats. Traditional security measures alone are insufficient. Zero Trust, once highly popular, still holds sway in certain circles. However, implementing it, especially for application access, poses challenges. Zero Trust advocates for the absolute minimum access trust, which potentially hinders the benefit of users having precisely what they need, when they need it.

An adaptive approach focuses on implementing a Zero Risk strategy by considering compliance, internal threats, fraud, and change management through continuous monitoring, which enhances digital space safety and security. In today's digital landscape, with companies adopting hybrid environments that combine on-premises and cloud applications, seamless interoperability and integrations are crucial. This heightened complexity and interconnectivity amplify business risks, which means that organizations require new tools to manage SAP application security.

Examining the Status Quo

REMEMBER

When it comes to managing application risk, the status quo just won't do anymore. In the past, managing application risk often relied on third-party consultants and auditors due to the manual nature of assessment. The extensive manual work, which should be simple, results from the vast amount of data and complex multi-step tasks required to collate and review results, often limiting risk discovery to sample testing.

The traditional approach

The traditional approach to managing application risk involves providing a tool connected to a single application. This tool manages tasks such as provisioning, separation of duties (SoD), sensitive access (SA) reporting and mitigation, user access reviews, and sometimes even elevated access management or role management.

AAG maturity

Application Access Governance (AAG) platforms provide advanced solutions that go beyond the basic access controls. They offer a range of capabilities such as risk and control revalidation, user identity and risk information, cross-application provisioning and risk analysis, controls management, risk quantification, threat detection and response, and advanced dynamic access controls, and data masking. So why is moving to a more mature access governance process difficult? Maybe it's due to the number of applications or perhaps the complexity and scope of controls involved in moving governance programs from the status quo to optimized best-in-class.

Take a look at the following issues:

- **Comparing apples to apples:** Virtually every application has its own unique security schema, which complicates the ability to conduct a consistent comparison of data across applications and hinders the establishment of an equitable basis for assessing potential risks. For these reasons, most legacy Identity and Access Management (IAM) systems only offer a high-level, coarse-grained view of risks, but these risks often manifest themselves deeper in the application permissions structure.

- **Security models not lining up:** This issue often causes gaps in understanding what scope of access is needed and can result in the overprovisioning of privileged assignments, higher counts of user access risks, and inefficient processes. Differing security models for each application also adds to the complexity of compiling audit data because the source locations for various testing screens and audit trail evidence are varied by application.
- **Tried and denied:** The primary difficulty lies in managing the actions and permissions objects within these applications. While having extensive connections to applications is one aspect, the real challenge is gaining a comprehensive understanding and the capability to administer the fundamental activities within the apps.

Changing the status quo


REMEMBER

Transitioning to the cloud often leads to cost savings and improved user productivity, but this transition comes with the risk of creating control silos. When considering digital transformation and the integration of cloud-based applications, recognizing the interdependence of applications that share business processes across various systems is essential. That tech is likely deployed in a hybrid architecture that encompasses on-premises, hybrid cloud, and public cloud. With increasing compliance mandates, the demand for enhanced cross-application visibility becomes imperative.

Moving from on-premises to the cloud creates control silos. Take a look at yesterday and today:

- Yesterday
  - Users are on-premises and inside the firewall
  - Distributed, disjointed, and manual processes
  - Single-app solutions and siloed visibility
  - Limited compliance requirement
  - Vulnerability awareness at the network/application level
- Today
  - Cloud app landscape living outside the perimeter
  - Requirement for automation, cost savings
  - Hybrid environments

- Multi-app driven business processes
- Ever-increasing compliance mandates such as the Sarbanes-Oxley Act of 2002 (SOX), the General Data Protection Regulation (GDPR), and the International Organization for Standardization (ISO)
- Fine-grained and user-centric
- Increasing threat vectors (such as phishing)

Taking a New Approach

Identity has emerged as a significant source of risk, so it's essential to adopt a fresh strategy to address contemporary challenges. A practical approach focuses on implementing a Zero Risk strategy, considering risk from a compliance, internal threat, fraud, and change management perspective with continuous monitoring.

Spanning multiple applications


TIP

The integration of cross-application business processes has brought forth best-of-breed solutions but has simultaneously introduced new access risks. This proliferation has also altered how organizations need to approach separation of duties (SoD). Security models now span various applications, emphasizing the importance for enterprises to identify SoD conflicts across apps. Enabling continuous controls monitoring becomes critical to detect and quantify violations as they occur.

Targeting growing threats

Security and operations teams frequently lack the visibility and tools needed to proactively understand threats to critical business applications. The proper threat detection and response offers focused visibility, continuous monitoring, and integration with incident response capabilities, empowering your team to identify and respond to internal and external threats affecting core business processes.

Identifying threats

WARNING

Detecting and responding to threats is crucial for preventing attacks that could disrupt operations or cause data breaches. However, organizations often face challenges in detecting these threats. Threat Detection and Response (TDR) software solutions can help address these challenges by quickly analyzing forensic data and automating threat responses.

Here are a few common cybersecurity threats:

- **Injection attacks:** Bad actors may use Structured Query Language (SQL) injection or similar tactics to exploit weaknesses in SAP applications and the underlying advanced business application programming (ABAP) code. This threat could lead to running harmful commands that can jeopardize system security.
- **Inadequate logging and monitoring:** Lack of proper logging and monitoring makes it hard to quickly spot suspicious activities or promptly identify security incidents. This issue can lead to delayed and reactive responses or measures to address the situation.
- **Denial of Service (DoS):** Malicious actors may try overwhelming the SAP system with a barrage of requests that aim to disrupt services or render the system inaccessible to legitimate users.
- **Password cracking via brute force attacks:** Threat actors use this attack to gain unauthorized access by employing an automated program to discover the correct username and password combination.
- **Remote command execution (RCE):** This vulnerability enables attackers to remotely execute commands on a target system. In SAP, this may lead to unauthorized access, data manipulation, or service disruption.
- **Authorization buffer exploits:** SAP systems use buffer tables to speed up database access during logins. These tables store recent login data, eliminating redundant queries and enhancing system efficiency. Without continuous monitoring, hackers could exploit weaknesses that modify data in buffer tables and grant unauthorized permissions.

- **Remote function call (RFC) callback attacks:** This mechanism in SAP systems allows communication among different SAP systems or between SAP and external systems. In an RFC callback attack, an attacker exploits the callback functionality to execute unauthorized and potentially malicious code on the SAP system.
- **Hidden OK codes:** Attackers can exploit hidden routines in SAP to bypass standard access controls, enabling them to manipulate vendor payment information without detection. This can lead to unauthorized access to sensitive data, critical process manipulation, and financial fraud.

Although they aren't cybersecurity threats, the following are threats within access control:

- **Insider threats:** These attacks originate from within an organization and are initiated by current or former employees or business associates with access to privileged accounts or sensitive information on the corporate network.
- **Fraudulent activity:** This threat covers a broad range of activities, such as money laundering, fraudulent banking claims, cyberattacks, identity theft, forged bank checks, and other illegal practices.

Implementing AAG: Continuous Risk Assessment and Mitigation

In today's world, safeguarding sensitive data is crucial, and large and medium-sized businesses achieve this through AAG solutions. AAG ensures that only authorized individuals can access vital information, promoting data security, regulatory compliance, and risk mitigation.

When implementing a new system for controlling application access, you may be tempted to start immediately provisioning users. However, it's advisable to conduct a baseline risk analysis first to address any unmitigated risks before initiating the provisioning process. This proactive approach, grounded in thorough analysis and risk mitigation, is essential in navigating the

complex and ever-evolving risk landscape. Skipping this step can result in serious problems such as fraud, system breaches, non-compliance, and damage to your company's reputation.

The practice of AAG

REMEMBER

AAG is the practice of managing, monitoring, and controlling who can access which applications and data within an organization. AAG ensures that only authorized individuals have the right level of access based on their job duties, risk profile, and specific application functionalities. AAG helps prevent unauthorized access, data breaches, and internal fraud through defined rulesets, policies, and automated monitoring. It simplifies how access is granted and revoked, keeping everyone accountable and minimizing the risk of sensitive information falling into the wrong hands. Additionally, it provides a centralized platform that offers a single audit trail, which simplifies the audit and compliance process for businesses.

Identity mapping and access inventory management

Identity mapping connects user identities from various systems (like Active Directory or Human Resources databases) to the applications they're authorized to use. This mapping ensures that only recognized individuals can enter specific application "zones," preventing unauthorized access attempts. Organizations can use role design to build these identity maps.

Access inventory management continuously scans and tracks all access rights granted within your applications, identifying any discrepancies or potential risks. This includes

- **User entitlements:** Which applications can each user access, and which actions can they perform within those applications?
- **Group memberships:** Which user groups have access to specific functionalities, and are these memberships still valid?
- **Unused or excessive privileges:** Are there dormant accounts or users with privileges beyond their job requirements?

Access inventory management helps prevent issues like privilege creep (where users gradually accumulate unnecessary permissions). It ensures compliance with internal policies and external regulations.

Risk analysis and reporting

Access risk analysis and reporting is a proactive way to protect sensitive data and systems. It involves examining the potential risks associated with user access to applications and data and then presenting those findings in a clear and actionable way.


TIP

The key aspects include identifying risks by analyzing user privileges, access levels, application functionalities, and data sensitivity to pinpoint potential vulnerabilities. For example, a user with extensive functional financial access poses a higher risk than one with limited reporting and display access. The identified risks can then be assessed for their likelihood of occurring and the potential impact. If a risk does occur, the organization can prioritize remediation efforts based on the severity of the risk.

Finally, the organization can evaluate the security measures and controls they have in place to determine their effectiveness. The analysis findings can then be presented via reports and dashboards to make the analysis easy to understand.

Granular access control and compliant provisioning

Granular access grants users precise permissions or entitlements within applications and systems based on their specific needs and roles. This focused approach minimizes risk by ensuring that individuals only access the resources they require, preventing unauthorized data exposure or manipulation.

Provisioning is the process of granting access, and it often becomes a juggling act between efficiency and compliance. Compliant provisioning simplifies this by automating access provisioning and life cycle management while ensuring adherence to internal policies and external regulations. This streamlines onboarding, avoids manual errors, and provides audit-ready documentation.

IN THIS CHAPTER

- Understanding the capability maturity model
- Explaining governance

Chapter 2
Leveraging SAP Application Security

Leveraging SAP application security entails using security features to protect the data and processes within the SAP software applications. This includes implementing measures to ensure that only authorized users can access certain information or perform specific actions within the SAP system.

Explaining the mysteries of SAP application security can often feel like walking through a hedge maze. This chapter helps you navigate the path while dealing with danger that lurks at every turn. So, protecting your space depends on keeping your valuable data inside and the problems outside.

Integrating CMM with Security Protocols

The need to fortify digital assets should be as clear as a shiny silver bell. Robust security depends on integrating the capability maturity model (CMM) with various security protocols. This process involves incorporating best practices from CMM into the development, implementation, and management of your security protocols, thus marrying efficiency with resilience.

REMEMBER

CMM is crucial because it allows organizations to objectively evaluate how well they're protected. It provides a clear plan for improving protection, helping organizations manage risk and become resilient against tricky cyber dangers. In this connected world, CMM is a key model for ensuring a more secure digital environment for everyone.

Seeing the value of CMM for SAP security

Applying the CMM approach to SAP application security involves strategically integrating its best practices into every aspect of your SAP system's governance. This means incorporating these practices into the development, implementation, and management of your security protocols. Think of CMM as a valuable tool that helps you systematically improve your security posture by providing clear guidelines and procedures. So, in the world of SAP security, understanding the value of CMM can lead to improved, compliant, and more efficient and effective IT management.

Analyzing levels of security

TIP

Keeping your data safe often takes a measured approach, depending on the threat level. When analyzing levels of application security, make sure to monitor how well each business process team or business organization manages and protects information. Through CMM, teams can assess their security practices, where naturally low levels mean basic security, and higher levels show advanced strategies. By measuring and understanding these levels, companies can identify and fix weaknesses, ensuring that they have strong, reliable security measures in place.

Moving through Application Governance

Governing your applications helps with increasing data security and making sure that these applications run efficiently. Companies today use an average of seven or more compliance tools and service providers. Surprisingly, despite this arsenal, 75 percent of controls are manually tested, leading to 49 percent of companies reporting material weaknesses. Last year, audit costs surged by 30 percent. The challenge arises from using numerous tools without effectively reducing material weakness risks.

Conversely, automation, as demonstrated by Pathlock, can bring an 80 percent risk reduction in audit and compliance initiatives. This underscores the significance of application governance and automation in navigating complex compliance landscapes.

Understanding your place

REMEMBER

Navigating the governance maturity spectrum involves evolving from ad hoc practices to continuous monitoring aligned with CMM. The journey advances by articulating, establishing, and transitioning processes from ad hoc to repeatable practices.

Delving into the key terminology, each point below integrates into a company's evolutionary path toward governance maturity:

- **Identity and Access Management (IAM):** The fundamental policy framework allows an organization to manage user identities and the privileges they have through policies and procedures that restrict user access to data and other resources.
- **Identity Governance and Administration (IGA):** This advancement of IAM fuses these policies with solutions that enable automation of access provisioning and reviews, allowing security administrators to efficiently manage user identities and access across the enterprise. Solutions referred to as IGA possess a suite of features that make this possible.
- **Application Access Governance (AAG):** Integral to safeguarding organizational assets, AAG enhances security by layering in risk management to all user access governance processes. The integration of IGA and access controls enhances automated provisioning by concurrently monitoring and managing the risks associated with the access granted throughout the user life cycle — from provisioning and reviews to elevated access management restrictions.
- **Continuous Controls Monitoring (CCM):** By testing and analyzing controls across various processes, CCM offers real-time insights that identify actual separation of duties, business process controls, and IT general controls violations. This proactive approach empowers organizations to maintain compliance, bolster security, ensure business continuity, and ultimately minimize losses and optimize performance.

- **Cybersecurity Application Controls (CAC):** This solution can be applied to protect systems at any development stage. CAC includes code scanning, managing vulnerabilities, dynamic access controls that support advanced ABAC, and enforcing data masking policies, along with active threat detection.

Examining governance policies


REMEMBER

Governance policies involve scrutinizing the established rules that guide activities, behaviors, and decision-making in an organization. They provide a framework to ensure ethical operations, regulatory compliance, and alignment with company objectives. The aim is to boost transparency, accountability, and organizational effectiveness by maintaining a robust governance structure in line with values and evolving business needs.

These policies can include the following:

- The principle of least privilege, which ensures that users only have the access necessary to perform their roles
- Access control policies, such as role-based access control (RBAC) or attribute-based access control (ABAC), which determine how access is granted based on user roles or attributes
- Life cycle management policies, which dictate when and how access is granted, changed, or revoked as a user's status within the organization changes

IN THIS CHAPTER

- Getting and staying clean
- Seeing the benefit of optimization

Chapter 3
Using CMM to Get Clean, Stay Clean, and Optimize

The governance and compliance life cycle encompasses the ongoing management and safeguarding of your organization's information systems and data against threats, both internal and external. This cycle includes stages such as getting clean, staying clean, and optimizing with the goal of establishing and maintaining effective access control measures.

You can manually accomplish the stages in this cycle, or you can tackle them in a more effortless way: through automation. The utilization of the Capability Maturity Model (CMM) in this process enhances your security measures by introducing organization and efficiency to your risk mitigation efforts. Check out Chapter 2 for more information about CMM.

Getting Clean

REMEMBER

Getting clean involves identifying the scope of your application landscape and executing access risk analyses to identify and correct risks in existing access. Next, implementing compliant provisioning ensures that net new risk isn't introduced into the

environment without performing a risk analysis. These analyses are followed by user access reviews at standardized time intervals, where management confirms or denies user access and certifies that access is correct on completion of the review.

Getting clean includes two important processes:

- **Inventory assessment:** Start by creating an inventory of all applications within your organization. Identify and document the applications that are currently in use.
- **Access analysis:** Analyze existing access rights and permissions for each application. Determine who has access to what and assess whether these permissions are appropriate.

Establishing rulesets


REMEMBER

Rulesets define sensitive actions that, when executed by a single user, can generate a violation of separation of duties (SoD). These rules help ensure compliance with regulations, protect sensitive information, maintain the integrity and confidentiality of data, and limit the potential for fraud. Specific risk rulesets can vary based on industry, regulatory requirements, and organizational priorities.

Measuring ongoing risk

When it comes to getting clean and all that follows, even the largest organizations can confidently manage security and compliance demands in their core enterprise resource planning (ERP) and beyond. Whether minimizing risk exposure, enhancing threat detection, addressing SoD effortlessly, or monitoring business process control violations, you can strengthen your ERP security and compliance.

Keeping sensitive data safe is more important than ever. Conducting risk analysis ensures that only the right people can access important information, which is crucial for keeping data secure, ensuring regulatory compliance, and mitigating access risks.

Risk analysis includes identifying, evaluating, and prioritizing potential risks that can affect your organization. The process of access risk analysis (ARA) helps identify and evaluate risks associated with user access to systems and data.

TIP

Conducting a thorough ARA yields many benefits:

- **Enhanced security and authorized access:** By having a comprehensive understanding of potential access risks, your organization can ensure that user permissions are managed securely, which prevents unauthorized access.
- **Assured regulatory compliance:** Conducting a comprehensive ARA ensures that application access governance (AAG) solutions align with industry-specific regulations and can avoid severe penalties and legal consequences.
- **Optimized resource utilization:** By granting only necessary privileges aligned with users' roles, companies can improve productivity, reduce the risk of errors, and prevent misuse of privileged information, which all result in a balanced workload and efficient use of skills and technology.
- **Guaranteed data integrity:** A comprehensive ARA policy ensures that access is structured to preserve data integrity. It also helps prevent unintentional or malicious changes of critical information. Ensuring data integrity sustains the reliability and trustworthiness of your organization's information assets.
- **Strengthened reputational standing:** By identifying and mitigating access risks in advance, your company can avoid incidents that may harm customer trust and investor confidence.
- **Reduced operational costs:** By preventing unauthorized access from the beginning, your organization can avoid the costly and resource-intensive processes involved in remediation efforts.

TIP

Pathlock provides a versatile simulation engine that can predict changes in risk across applications at the business and technical role levels and at the user level. Before and after perspectives include usage analytics that show potential business impact. Check out Chapter 4 for more on Pathlock's approach to SAP application security.

Staying Clean

Governance is the establishment of clear policies and procedures to ensure the secure and effective management of your digital assets. The idea of a path to Zero Risk is closely tied to CMM.

At this stage, you implement access request workflows to make sure the right people have access to the right data following the appropriate approvals. This refers to allowing only authorized personnel to access specific resources, data, or functionalities within your software ecosystem. Access request management streamlines this process by centralizing access requests, approvals, and auditing — all within a user-friendly interface.

Additional steps to staying clean involve implementing automation to streamline the provisioning and deprovisioning of access rights based on job responsibility. This helps in reducing the risk of human error and ensuring timely adjustments to access.

REMEMBER

The automation process should also encompass user access certifications to ensure that no outdated access rights linger with users and to maintain the regular review and revalidation of controls and risks to keep them up to date.

Striking the right balance between efficiency and effectiveness in application access certifications is crucial for modern organizations. By automating, centralizing, and optimizing the certification process, your company can reduce the time required for user access reviews while enhancing the accuracy and impact of their efforts.

Optimizing

Optimizing is focused on utilizing business roles, implementing risk quantification, and addressing threat detection. Through the life cycle process, you can effectively manage and monitor governance, which eliminates compliance concerns.

Here's what you can expect:

- **Continuous improvement:** Regularly review and update access governance processes based on your evolving business needs, changes in regulations, and emerging security threats.
- **User behavior analytics:** Implement user behavior analytics to identify unusual patterns of access that may indicate security threats or policy violations.

Utilizing business roles

REMEMBER

Role management manages the entire role life cycle. This module automates many of the key role management processes so that you can optimize how SAP roles are managed and improve your overall audit readiness. It ensures that role maintenance is auditable, the decisions are based on detailed usage data, role designs are SoD-free, and risks are properly mitigated.

This approach streamlines an organization's unique role request, design, development, and testing requirements, ensuring that access management processes are efficient and consistent. The module also helps companies gain auditor approval, increase productivity, lower costs, improve end-user satisfaction, and seamlessly implement only approved designs.

Implementing risk quantification

WARNING

Organizations today need to monitor and quantify their exposure to SoD conflicts. Of course, your company can't eliminate every risk, so the goal should be to identify the risks that threaten predefined thresholds of value.

You can analyze transaction data within your business applications to quantify the financial exposure of SoD conflicts in your application environment. This quantification identifies the monetary risk and impacts on your organization. You get detailed analysis that can be viewed by SoD control conflict, user, or application with complete transaction details.

Furthermore, you can track and report on all quantifiable risks that actually occurred, as opposed to having to report on potentially thousands of risks that never happened and, due to data size, can only be sampled for testing.

Enabling threat detection

Reduce the risk to your critical systems by focusing on what matters. Think about it; security and operations teams often lack the visibility and information required to proactively understand the telemetry data that constitute threats to critical business applications. They also lack the tools to properly respond to threats and compromised accounts.


TIP

Pathlock's threat detection and response provides security and application teams with focused visibility into threats facing their critical business systems. Pathlock provides the continuous monitoring necessary to identify internal and external threats that could affect your core business processes while integrating with your incident response applications and programs.

Threat detection and response capabilities include

- **Continuous threat detection coverage:** Get continuous monitoring for thousands of threat indicators.
- **Automatic updates:** Continuously update with the latest threat information, patch availability, and ongoing research.
- **Rapid response to threats:** Detailed context for issues with resolution guidance equals reduced investigation response times.
- **SIEM integrations:** Enrich your security information and event management (SIEM) applications with detailed threat detection data for further correlation across systems.

Check out Chapter 4 for more on Pathlock's approach.

IN THIS CHAPTER

- Getting clean with Pathlock
- Maintaining clean
- Optimizing solutions

Chapter 4
Examining the Pathlock Approach

When dealing with risk, Pathlock Cloud provides customers with a comprehensive set of modular capabilities. Designed to seamlessly work together, these tools reduce potential risk following the get clean, stay clean, optimize methodology.

Getting Clean with Pathlock

Every application access program holds inherent risks. In the get clean stage, the goal is to produce a more risk-free environment by creating more visibility into your risk landscape. An access risk analysis is executed to deliver a more risk-free environment by analyzing and reporting on risks across separation of duties (SoD), data privacy, and cybersecurity in a single fine-grained view.

Pathlock Cloud is comprised of modules with three distinct product categories: Application Access Governance (AAG), Continuous Controls Monitoring (CCM), and Cybersecurity Application Controls (CAC). You can find a detailed description of each in Chapter 2.

Analyze access risk in your enterprise applications, emphasizing the importance of SoD for fraud prevention and SOX compliance. Pathlock automates SoD and access risk analysis across human capital management (HCM), enterprise resource planning (ERP), and customer relationship management (CRM) platforms, offering customizable rulesets for quick implementation and reducing costs and risks through automation. You get the following:

- **Simulation analysis:** This flexible simulation engine forecasts risk changes at the business or technical role, or user level access, across applications.
- **Granular reporting:** This involves detailed access analysis reporting; conflict analysis by role, user, entity (business unit or plant), duty, privilege level, table access, and more.
- **User-friendly dashboards:** Easily view trend analysis and risk analysis results summary tracking.
- **Cross-application risk management:** Manage multiple applications and cross-application risks, all within the singular user interface within Pathlock Cloud.

Staying Clean for a Secure Environment

Staying clean in day-to-day operations for a secure environment can be challenging. Significant impact areas are handling access requests, time-bound elevated access, and certifying user access through regular campaigns. Staying clean entails the following:

- **Identity life cycle management:** Incorporate AAG into the Identity and Access Management (IAM) processes to ensure that access aligns with the employee life cycle (onboarding, changes, offboarding).
- **Automated provisioning and deprovisioning:** Implement automation to simplify the process of granting and revoking access rights. This minimizes the risk of human error and ensures timely adjustments to access.
- **Policy enforcement:** Consistently apply access policies across all applications, ensuring compliance with regulatory requirements, internal policies, and industry best practices.

- **Monitoring and auditing:** Consistently observe access activities and perform routine user access reviews to detect and resolve any stale or unauthorized access or potential security risks.

Addressing risk areas

Compliant provisioning ensures a risk-free environment by conducting an access risk analysis within the access request process. This allows users to obtain access through an automated process that considers both risk scoring and policy-based workflows, including preventative SoD and critical access risk checks. It eliminates the risk of introducing new application access without prior review, mitigation, or remediation, offering comprehensive audit trails and streamlined user access through assigned controls. This avoids post-provisioning challenges and ensures that users receive access based on specific needs and justifications.

Utilizing access requests workflows

Manual access requests during busy periods like mergers, seasonal changes, and growing teams can lead to backlogs, errors, and frustration. Pathlock Cloud tackles these issues by automating compliant provisioning, boosting efficiency by more than 90 percent. Its access request workflows guide users to suitable roles and track every request, ensuring an audit-approved, business-friendly path to Zero Risk.

Establishing certification processes

REMEMBER

Regularly recertifying user access is crucial as roles change or employees depart. Manual reviews using spreadsheets are cumbersome, resource-intensive, and error-prone. Pathlock's certifications module automates user access reviews across *all* business applications, replacing spreadsheets with streamlined workflows. This ensures efficient recertification, reducing the risk of overlooking critical access details. Reviewers gain cross-application support and understand the broader impact of decisions on business and compliance risks.

Enabling elevated access requests

REMEMBER

Granting temporary elevated access is a tedious and risky process riddled with concerns from auditors. Pathlock streamlines this by automating workflows, reducing IT resource strain, and adding security layers. It offers automated request workflows, detailed change logs, and audit-ready reports, ensuring compliance and simplifying access management.

Optimizing Solutions

After you get clean and stay clean, you're able to optimize your environment for the continuous improvement that creates a Zero Risk environment.

Enabling process improvement and organization controls

Optimizing security involves defining and refining controls for managing application access and business processes. Continuous monitoring and management of controls, including changes to configurations and master data, enable fine-tuning for process improvement or regulatory compliance.

Utilizing access analytics

TIP

Access analytics empowers both role owners and reviewers with data-driven insights, ensuring smarter access decisions. When creating or updating roles, unused or underutilized functionality can be identified and removed, adhering to the principle of least privilege. During user access certifications, usage analytics provide reviewers with context, guiding informed decisions on access retention or revocation.

Applying role mining

Outdated role management hinders access control and compliance, often leaving critical applications vulnerable. Role mining solves this by aligning permissions with security needs, preventing over-privileged accounts, limiting risk, and enhancing user account visibility. Its capabilities include fine-grained role design, risk simulation, continuous monitoring, and broad application support.

IN THIS CHAPTER

- Understanding your risk analysis
- Promoting access and role management
- Assessing risk
- Monitoring vulnerability
- Responding to threats

Chapter 5
Ten Ways Pathlock Cloud Helps with SAP Security

When it comes to creating industry-wide application governance and cybersecurity solutions, Pathlock Cloud is an advanced tool suite crafted for enhancing SAP application security. By continually monitoring user access privileges and detecting deviations from set policies in real time, it prevents unauthorized access and data breaches. Upholding zero-risk principles, it automatically flags control vulnerabilities. This empowers organizations to proactively manage SAP environments, strengthen cybersecurity, and protect sensitive data by streamlining access control and providing detailed user activity insights. In this chapter, we give you ten ways Pathlock Cloud can help you improve the application security of your SAP environment.

Leveraging Access Risk Analysis

REMEMBER

In the realm of effective risk analysis, identifying inter- and intra-role conflicts is key to managing separation of duties (SoD). Pathlock Cloud takes the reins in ensuring that individuals steer clear of conflicting responsibilities that may result in access misuse.

This fortifies internal controls for organizations, minimizing the chances of errors, fraud, and unauthorized activities. With automated SoD and sensitive access risk analysis, Pathlock offers pre-made and easily customizable rulesets. This not only ensures swift implementation for your organization but also reduces risks and costs through an automated approach to risk analysis.

Administering Compliant Provisioning

In terms of compliance, Pathlock's automated provisioning approach empowers you to effortlessly establish, manage, and revoke access across all your business applications. With its highly detailed provisioning capabilities, Pathlock ensures a seamless alignment of access with specific business needs, including transaction controls and sensitive data masking. Pathlock streamlines user access, risk, and control reviews through an automated workflow, eliminating extensive manual efforts to collate data across applications and distributing and tracking reviews across numerous business processes, divisions, and managers. Pathlock's capabilities include the following:

- **Fine-grained provisioning:** Allows for the industry's most detailed permission sets to align with business requirements
- **Broad application support:** Supports many commonly used business applications, allowing cross-app provisioning from a single UI
- **Continuous role monitoring:** The monitoring of organizational structure changes in your business applications and ERP systems
- **Deep integrations:** Acting as an official SOLEX partner for SAP and Microsoft MISA Partner for provisioning

Executing Certification Campaigns

Access certification is often a routine, yet challenging, task for organizations, particularly when done manually. The process involves creating spreadsheets listing users and roles, sending them to supervisors, constant email follow-ups, tracking

and consolidating responses, and manual access updates. This labor-intensive process can take months for a single application review.

Pathlock's module automates much of the manual effort in certifying access, providing campaign managers and reviewers with tools for effortless reviews across multiple applications simultaneously. Features that enhance compliance and streamline manual access reviews include the following:

- **Automated workflows:** Design customized workflows that streamline the entire access certification campaign.
- **Usage insights:** Usage insights are provided to reviewers to evaluate access necessity. Data includes last date and frequency of role and transaction usage at user, entitlement, and permission levels.
- **Robust certification information:** To prevent rubber-stamping and enable informed access reviews, detailed risk information (SoD/sensitive access risks), usage information, and user context (title, department, and so on) are included in access requests.
- **One-click access revocation:** If your role owners want to revoke specific access, they no longer need to send an email to IT. The module enables them to remove specific user access with a single click.
- **Campaign management and reporting:** Effortlessly track access review progress with status reports and reviewer dashboards, ensuring a seamless process.
- **Detailed campaign segmentation:** Recertification campaigns can be segmented based on attributes like role, department, geography, and SoD risks. This approach ensures that high-risk user groups are reviewed more frequently while low-risk users are reviewed less, addressing organizational risk differentials.

Managing Elevated Access

Elevated access provides time-limited access beyond a user's usual entitlements, which offers a crucial capability for secure operations. Controlling user permissions and roles helps organizations

restrict access to sensitive data, minimizing the risk of unauthorized use or data breaches and meeting the least privileged access model. This proactive approach enhances overall cybersecurity and ensures that only authorized personnel have appropriate system access.

Here's what you can expect:

- **Enhanced activity tracking:** Detailed activity tracking in a highly actionable user interface
- **Access analysis:** Automated reporting of SoD and SA risk analysis
- **Change log:** Detailed analysis allowing you to track changes to transaction and master data
- **Access certification:** Automated workflows streamline access approvals while notifications prompt reviewers to confirm termination decisions based on change logs, ensuring efficiency and control
- **User identity data:** Inclusion of relevant user identity information such as manager, location, department, and title

Understanding Role Management

Pathlock aligns your business priorities with compliant, audit-ready roles for critical applications. Automated role management serves as your protector in the access security realm, eliminating manual efforts in designing, updating, and maintaining SoD-free, task-based security. Pathlock's role management is a potent visual role builder for business applications. You can evaluate existing roles and design compliant new roles with simulations and what-if analysis. The fine-grained role design ensures dynamic adherence to access policies, which promotes compliance.

Prioritizing Risk Quantification

REMEMBER

Just like you enjoy the benefits of cars today over horse and buggy, the ability to quantify risks revolutionizes how you view and address an actual, occurring risk, versus the legacy approach of only identifying and reporting on potential risks. Organizations

today must keep an eye on and measure their exposure to SoD and business process controls conflicts — with the power to influence financial activities or reporting.

While eliminating every risk is a tall order, the aim is to spot those that surpass predefined value thresholds. Pathlock dives into your business applications, analyzing transaction data to quantify financial exposure from SoD and business process controls conflicts. This breakdown not only pinpoints monetary risks but also their impact on your organization. With detailed analyses viewable by control conflict, user, or application, Pathlock can slash the time and costs of SoD audits by up to 80 percent.

Looking at CCM

Continuous Controls Monitoring (CCM) helps you oversee business process, SoD, and IT general controls to maintain constant awareness of potential risks. Pathlock's CCM provides in-depth analysis, enabling you to monitor changes to transaction and master data, including the source of the change, the initiating user, and before-and-after values, even tracking deletions.


TIP

CCM is like having a team of meticulous observers constantly reviewing your system; examining your business processes, user access, and IT controls; and looking for any unusual activity. It tracks every change, including who made it, what was changed, and even when deleted data was removed.

Dealing with Controls Management

With Pathlock, you can bring together and simplify multiple control frameworks in one automated place. The perks of automating this consolidation for identifying and assessing risks include working more efficiently, cutting down on manual work, providing a holistic view of the risks monitored and risk exposure identified, having consistent controls, and meeting the rules of different frameworks. This setup also helps your organization better react to changing risks and regulations.

Monitoring Vulnerabilities

REMEMBER

Security patch backlogs expose even proactive organizations to risks, exploitation, and data theft. Pathlock's vulnerability management solution empowers security teams by providing clear visibility and prioritization, enabling them to swiftly address the most critical vulnerabilities and effectively eliminate threats.

Pathlock's vulnerability management solution offers a robust library of security checks and proven rulesets to manage and secure your application landscape. It allows you to schedule and run audits, providing a centralized view of your security status. Additionally, it offers audit-compliant documentation and mitigation of risks.

Responding to Threat Detection

Pathlock's threat detection and response gives teams visibility into threats that affect critical business systems. That's great because security and operations teams often struggle to proactively understand telemetry data that poses threats to crucial business applications due to a lack of visibility and information. It's widely expressed that "Patch Tuesdays" often lead to "Exploit Wednesdays," highlighting the crucial role of vulnerability management and threat detection. Through continuous monitoring, Pathlock identifies internal and external threats that impact core business processes, seamlessly integrating with incident response applications and programs.

You get continuous threat detection coverage, automatic updates, rapid response to threats, and SIEM integrations.

pathlock

Protect the Critical Applications, Users, and Data that Drive Your Business

Enjoy the peace of mind that comes with a solution designed to continuously monitor your systems for risk, provide actionable remediation, and deliver unparalleled control and visibility over sensitive data.

TAKE A PROACTIVE APPROACH TO SAP SECURITY:

- **Continuously enforce compliance:** Automate workflows and ensure the right users have the right access.
- **Eliminate hidden vulnerabilities:** Find and fix security gaps before they lead to breaches.
- **Optimize your security posture:** Use risk quantification to prioritize remediation actions.

PATHLOCK EMPOWERS YOU TO:

Stop reacting, start protecting: Focus on strategic initiatives, not security firefighting.

Boost efficiency and ROI: Gain back valuable time and resources.

Secure your entire system landscape: Protect your broader ERP ecosystem with comprehensive security solutions.

Simplify your processes, strengthen your systems, and protect critical data.

Visit **www.pathlock.com/sap** to learn more.

Embrace proactive SAP application security

Unlock next-level SAP application security: This book is your path to proactive protection. Embrace a get clean, stay clean, and optimize mindset to fortify your defenses. Uncover hidden risks, establish airtight rules, and automate workflows to banish security gaps for good. Effortlessly manage access requests, user certifications, and secure elevated access. Harness Pathlock's platform for deep risk insights, precise measurements, and tailor-made controls, optimizing your entire system landscape — let's go!

Inside...

- Assessing SAP application security
- Examining the status quo
- Taking a proactive approach
- Getting clean and staying clean
- Benefitting from optimization
- Improving efficiency and ROI
- Leveraging Pathlock Cloud

pathlock

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-23624-4
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.