LEARNING MADE EASY

Pathlock Special Edition

Zero Risk Application Security

for dummies®

A Wiley Brand

Understand a Zero Risk approach

Deploy a Zero Risk strategy

Achieve Zero Risk with Pathlock Cloud

Brought to you by

pathlock

Brett McLaughlin
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 identity and application access risk governance in a single platform, including user provisioning and temporary elevation, ongoing user access reviews, control testing, transaction monitoring, and audit preparation.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Zero Risk Application Security

Pathlock Special Edition

by Brett McLaughlin, Keri Bowman, and Kyle Benson

for dummies®
A Wiley Brand

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Zero Risk Application Security For Dummies®, Pathlock Special Edition

Published by

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

Copyright © 2024 by John Wiley & Sons, Inc., Hoboken, New Jersey. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Pathlock and the Pathlock logo are registered trademarks of Pathlock. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit be www.dummies.com/custom-solutions. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-23621-3 (pbk); ISBN 978-1-394-23622-0 (ebk); ISBN 978-1-394-28365-1 (ebk)

Publisher's Acknowledgments

Project Manager and Editor: Carrie Burchfield-Leighton

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager: Jeremith Coward

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Table of Contents

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

In the digital era, achieving a Zero Risk environment for application security has become a critical priority for organizations worldwide. Much like reinforcing a physical fortress, the virtual landscape requires meticulous planning and robust defenses to protect its valuable assets. Zero Risk application security aims to create a comprehensive shield against potential threats, ensuring the integrity, confidentiality, and availability of vital data and systems.

Zero Risk application security involves creating a system where risks are proactively identified, managed, and mitigated. This approach integrates automated risk analysis, stringent access provisioning controls, and continuous monitoring to prevent unauthorized access and vulnerabilities. The goal is to neutralize potential threats before they cause harm, maintaining the highest levels of visibility, security, and compliance.

Achieving Zero Risk means implementing appropriate layers of security controls that address various threats, from network to application and data security. Continuous monitoring provides real-time visibility, enabling immediate threat detection and response. Automated tools assess risks and prioritize remediation. Stringent access controls ensure only authorized users access sensitive systems, reducing breach risks.

About This Book

Understanding and implementing Zero Risk application security is vital for IT professionals and business leaders alike. Whether you're part of a global enterprise or a startup, this book can direct you through creating a Zero Risk environment, offering insight into the technologies, methodologies, and best practices essential for resilient cybersecurity.

This book serves as your comprehensive guide to achieving the goal of Zero Risk application security and emphasizes its significance in protecting sensitive data and ensuring robust security protocols in today's digital landscape. As organizations increasingly rely on complex digital infrastructures, achieving Zero

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Risk application security is essential to prevent potential security breaches.

In Chapter 1, you dive into the foundational principles of the Zero Risk methodology, learning how to proactively identify and mitigate risks. Chapter 2 covers aligning Zero Risk strategies with cybersecurity and regulatory compliance frameworks to ensure your organization meets critical standards. Chapter 3 explores layering security measures to comprehensively reduce risks, while Chapter 4 provides an in-depth look at establishing Zero Risk with Pathlock Cloud. In the last chapter of the book, Chapter 5, you discover ten ways Pathlock Cloud helps you achieve a Zero Risk application environment.

Icons Used in This Book

Within this book, you come across several unique icons in the margins that are crafted to draw attention to important information or underscore key points. Here's a quick summary of what to expect:


REMEMBER

The Remember icon highlights crucial points. This is the perfect place to use a highlighter, make a note in the margin, or fold down the page for future reference.


TIP

Tips offer brief summaries of useful information that can consistently improve your understanding and management of secrets.


WARNING

Warnings provide practical advice to help you avoid potential pitfalls, costly mistakes, or frustrating errors, much like the guidance a security-conscious mentor may offer.

Beyond the Book

This book lays a solid foundation for understanding Zero Risk application security, but to explore further, Pathlock offers a wealth of information and solutions online. Visit `www.pathlock.com/next-gen-iga` to access articles, case studies, and white papers that delve deeper into Zero Risk application security.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Unpacking the concept of Zero Risk in application security
- Distinguishing between Zero Risk and Zero Trust strategies
- Achieving and measuring results with Zero Risk

Chapter 1
Understanding the Zero Risk Methodology

In today's digital landscape, securing applications is more critical than ever. This chapter introduces the concept of Zero Risk in application security, detailing how it can protect your organization's data and operations. You discover how Zero Risk differs from Zero Trust, as well as practical, actionable steps to implement a Zero Risk strategy in your own organization.

Defining Zero Risk

Zero Risk application security is a proactive approach aimed at eliminating vulnerabilities within your application environment. Unlike traditional reactive methods, Zero Risk involves ongoing discovery, assessment, continuous monitoring, and immediate remediation of threats to ensure that applications always remain secure.

REMEMBER

Zero Risk involves several core principles:

- **Application access risk analysis:** Continuously identify and manage risks associated with user roles and access

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

permissions. By understanding who has access to what and why, organizations can prevent unauthorized access and potential data breaches.

- **Compliant provisioning:** Ensure user access is granted and revoked based on stringent compliance requirements. This process must be efficient to avoid delays in productivity while maintaining security standards.
- **Elevated access management:** Manage high-risk access privileges through automated workflows that ensure any elevated access is temporary, necessary, and monitored.
- **Continuous monitoring:** Real-time tracking of all transactions within the application environment to detect and respond to threats immediately. This helps maintain an up-to-date security posture.
- **Vulnerability management:** Regularly identify and patch vulnerabilities in the application and its underlying infrastructure. This proactive approach minimizes the risk of exploitation.
- **Risk quantification:** Analyze potential threats in terms of their financial impact to prioritize remediation efforts effectively. This helps allocate resources to the most significant risk exposures.

REMEMBER

Zero Risk isn't a one-time setup but an ongoing strategy that adapts to new threats and challenges within your organization.

Differentiating Zero Risk from Zero Trust

Although Zero Risk and Zero Trust share the common goal of enhancing security, they employ different strategies:

- **Zero Trust:** Operates on the principle that no entity, inside or outside the network, should be trusted by default. Every access request is thoroughly verified, which can add layers of complexity and potential friction for users.
- **Zero Risk:** Focuses on creating a proactive, integrated security platform that systematically eliminates risks. It unifies various aspects of IT, cybersecurity, audit, risk, and compliance into a cohesive strategy, ensuring seamless security without compromising user experience.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

While Zero *Trust* emphasizes verification, Zero *Risk* emphasizes early discovery, quantification, and eradication of vulnerabilities and continuous improvement.

Deciding whether to implement Zero Risk, Zero Trust, or a combination of both depends on your organization's specific needs and security goals:

- **Zero Trust:** Ideal for organizations looking to enhance security by verifying every access attempt, making it suitable for environments where security needs are extremely high and user activity is highly variable.
- **Zero Risk:** Best for organizations aiming to build a comprehensive, proactive security framework that integrates risk management and compliance into everyday operations.
- **Combining both:** In most cases, a hybrid approach can offer the best of both worlds. Implementing Zero Trust for critical access points while employing Zero Risk strategies for overall risk management can provide a robust and flexible security posture.

WARNING

Neglecting to integrate Zero Risk principles can expose your organization to undetected threats and compliance failures, potentially leading to severe consequences.

Getting Tangible Results with Zero Risk

Moving from the conceptual understanding of Zero Risk to practical implementation is crucial for achieving real security improvements. It involves taking concrete steps to enhance your organization's security posture, ensure regulatory compliance, boost operational efficiency, and improve user experience. This section outlines actionable strategies that can help you turn the idea of Zero Risk into a reality.

You should start with these key actions:

- **Enhance security posture:** Conduct continuous risk assessments and use real-time monitoring tools. Regularly update and patch systems to mitigate vulnerabilities. Continuous risk assessment is essential for a robust security posture.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Achieve regulatory compliance:** Use identity and application access governance software to automate monitoring and reporting. Regularly train staff on compliance standards. Automate compliance reporting to stay ahead of regulatory reporting requirements and reduce audit preparation time.
- **Boost operational efficiency:** Automate security processes like user provisioning and vulnerability scans. Implement Identity Governance and Administration (IGA) to streamline access management and identity life cycle governance.
- **Improve user experience:** Implement single sign-on (SSO) and role-based access control (RBAC) to simplify and secure user access. Ensure security measures are user-friendly to prevent workarounds.

By focusing on these practical measures, you can effectively secure your application environment, ensure compliance, improve operational efficiency, and enhance user experience. This approach not only strengthens your security posture but also supports sustainable growth and resilience. With these foundations in place, your organization will be well-positioned to tackle the challenges of a dynamic digital landscape and fully realize the benefits of a Zero Risk strategy.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Maturing your model systematically
- Leveraging the NIST framework for risk management
- Ensuring compliance with SOX, GDPR, and more

Chapter 2
Aligning Zero Risk to Cybersecurity and Regulatory Compliance Frameworks

Achieving Zero Risk in application security means aligning your strategies with well-established cybersecurity and regulatory compliance frameworks. This chapter dives into how you can mature your cybersecurity model, utilize the National Institute of Standards and Technology (NIST) framework, and ensure compliance with Sarbanes-Oxley Act (SOX) and General Data Protection Regulation (GDPR) regulations. By syncing Zero Risk principles with these frameworks, you'll not only enhance your security posture but also keep regulatory compliance in check.

Maturing Your Cybersecurity Model

To hit the mark on Zero Risk, you need to mature your cybersecurity model. The Cybersecurity Maturity Model Certification (CMMC) is your go-to guide for systematically enhancing your

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

security practices. Although it started with the Defense Industrial Base, its principles can work wonders across various sectors.

Using CMMC as a framework for maturity

The CMMC framework is currently divided into five levels of increasing security maturity:

- **Level 1: Basic cyber hygiene:** This is where you start by figuring out your current cybersecurity practices and understanding the basics.
- **Level 2: Intermediate cyber hygiene:** Here, you document all your cybersecurity practices to ensure they're consistent and repeatable.
- **Level 3: Good cyber hygiene:** At this stage, you've managed the risks by putting proper risk management practices in place to address identified vulnerabilities and threats.
- **Level 4: Proactive cyber hygiene:** Now, you're routinely and regularly reviewing risks. Continuous monitoring ensures you're proactive in managing them.
- **Level 5: Advanced and progressive cyber hygiene:** This top level focuses on optimizing your cybersecurity processes and continuously improving to stay ahead of emerging threats.

REMEMBER

Progressing through the CMMC levels requires a commitment to continuous improvement and adaptation to new threats and technologies. Getting through these levels means you're consistently enhancing your cybersecurity practices. Start by assessing your current status and work through each level methodically, making the necessary changes and improvements as you go. With CMMC 2.0 in the planning phase, which will reduce the levels from five to three, any steps taken to prepare for the current CMMC will translate to the new framework.

Building a plan to address your risks

To mature your cybersecurity model, you've got to build a solid plan to tackle the identified risks. The process looks something like this:

1. **Start by evaluating your current cybersecurity posture.**

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Identify existing risks and see how they measure up against the practices outlined in your target CMMC level. This initial assessment helps you figure out where you stand in terms of cybersecurity maturity.

2. **Draft a detailed plan to close any gaps you've found in Step 1.**

   This plan should cover necessary improvements in risk analysis, security policies, business process controls, and vulnerability management. Break the plan down into manageable steps and assign tasks to the right team members.

3. **Collect artifacts such as logs, configurations, and training records.**

   Documenting your cybersecurity practices is key to progressing through the maturity levels and proving you adhere to the CMMC framework. These documents provide evidence of your compliance with the CMMC framework and help you track your progress.

4. **Put your plan into action by implementing the identified security controls and processes.**

   Regularly review and update your practices to ensure they stay effective and relevant. Continuous monitoring and tweaking are essential for maintaining and improving your cybersecurity posture.

TIP

Regularly reviewing and updating your cybersecurity practices ensures they stay aligned with evolving threats and regulatory requirements.

5. **Continuously monitor your cybersecurity posture to spot and tackle new risks as they arise.**

   Use automated identity and application access tools to streamline this process and get real-time insights.

WARNING

Skipping continuous monitoring can leave your organization with outdated security measures, making you vulnerable to new threats.

By following these steps and moving through the CMMC levels, your organization can build a strong cybersecurity model that aligns with Zero Risk principles. This approach not only boosts your security posture but also supports ongoing compliance and resilience against emerging threats.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Taking Advantage of a NIST-Compliant Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 offers a solid approach to managing cybersecurity risks. It's designed to help organizations of all sizes and sectors improve their cybersecurity stance.

To leverage the NIST framework, you need to

- **Understand and assess:** Use the CSF core profiles and tiers to describe your current or target cybersecurity posture. Identify gaps and assess your progress towards fixing them.
- **Prioritize actions:** Organize and prioritize actions for managing cybersecurity risks. Align these actions with your organization's mission, legal requirements, and risk management goals.
- **Communicate risks:** Use the NIST framework to speak a common language for communicating cybersecurity risks internally and externally. This builds a shared understanding and a coordinated response to threats.
- **Implement core functions:** The NIST framework is broken down into six core functions: govern, identify, protect, detect, respond, and recover. Each function has categories and subcategories that define specific outcomes. Implement these to create a robust security posture.
- **Progress through tiers:** The framework includes tiers to measure cybersecurity risk management. Moving up the tiers involves improving governance and risk management practices. Aim to go from partial or risk-informed practices to repeatable and adaptive ones.

WARNING

Failing to progress through the NIST tiers can leave your organization vulnerable to evolving threats. Continuous improvement is vital.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Gaining and Maintaining SOX and GDPR Compliance

Achieving and maintaining compliance with SOX and the GDPR is crucial for many organizations. A Zero Risk approach can help streamline this process.

Identifying the path to compliance

To ensure SOX and GDPR compliance, you need

- **Deep knowledge:** Thoroughly research SOX and GDPR requirements. Understand how these regulations apply to your operations and data-handling practices.
- **Framework development:** Set up an integrated control framework that incorporates both SOX and GDPR requirements. Focus on key areas such as financial reporting controls, data governance, access control, incident response, and vendor management.
- **Gap analysis:** Do a comprehensive gap analysis to compare your current policies, processes, and technologies with SOX and GDPR requirements. Identify areas that need improvement.

After you've identified the gaps, create a detailed remediation roadmap to address them. Prioritize critical areas, allocate resources, and set timelines for completion. Develop or update policies to align with SOX and GDPR standards and communicate these policies clearly to everyone involved. Quantifying the financial impacts of potential gaps ensures not only compliance but also protection for the organization from material impacts.

TIP

Regular training and awareness programs for employees are crucial for maintaining compliance. Ensure that all staff understand their roles in protecting data and maintaining financial integrity.

Moving from assessment to compliance

After you've made your assessment, you're ready to execute. Start by implementing and integrating any necessary identity and application access security tools and solutions to meet

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

compliance requirements. This may include application cybersecurity tools, access control systems, and controls management tools. Systematically close each gap between your current state and a compliant one.

REMEMBER

The work doesn't stop after you become compliant. Conduct regular internal audits and test your financial controls and data security procedures. Keep an up-to-date record of all data processing activities and review compliance frameworks periodically to adapt to evolving requirements. This ensures you *maintain* compliance.

WARNING

While SOX and GDPR share some common ground, there are key differences. Keeping compliant requires a dual-track approach and close attention to each regulation's unique aspects. Reaching compliance with these standards is an accomplishment, but maintaining it is the goal. Falling out of compliance due to a lack of ongoing review will cost far more than staying compliant in the first place.

By aligning your cybersecurity and regulatory compliance efforts with Zero Risk principles, your organization can build a strong security posture that adapts to new threats and keeps you compliant with critical regulations. This integrated approach not only protects your organization but also supports sustainable growth in an increasingly complex digital landscape.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Understanding the importance of a layered security approach
- Implementing end-to-end security strategies
- Transitioning from legacy technologies to innovative solutions

Chapter 3
Layering Security to Reduce Risks

Layering security to reduce risks involves a comprehensive approach that includes securing the application architecture, managing code and transport, designing user roles, implementing dynamic access controls, and continuously monitoring and managing risks.

This chapter delves into defining the appropriate layers of defense, securing your environment comprehensively, and replacing outdated technologies with innovative solutions.

Defining the Layers of Security

Achieving Zero Risk in application security means setting up appropriate layers of defense that work together to protect against different threats. Each layer of security reduces overall risk and enhances your proactive security posture.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Securing application architecture

The foundation of any secure environment starts with the application architecture. Here are the key areas to consider:

- **Vulnerability management:** Regularly identify and patch vulnerabilities. This proactive approach prevents potential exploits before they can cause harm.
- **Patch management:** Keep all software and systems up-to-date with the latest security patches. This is crucial for protecting against known vulnerabilities.
- **System configuration:** Securely configure your systems to minimize potential attack vectors. Proper configuration reduces the risk of unauthorized access.
- **Log management:** Implement robust log management practices to detect and respond to anomalies. Monitoring logs helps identify suspicious activity early on.

REMEMBER

Securing the application architecture is crucial as it forms the base of your application cybersecurity strategy.

Code development and transport management

After the foundation is secure, the focus shifts to maintaining and transporting code securely. Key areas include

- **Code consistency:** Ensure that code development follows best practices and is consistently checked for vulnerabilities. This prevents introducing new risks.
- **Transport management:** Manage the transportation of code through the system landscape. Proper handling of code transport reduces the risk of tampering.
- **SIEM integration:** Integrate with Security Information and Event Management (SIEM) systems to monitor and manage security events. SIEM integration helps in real-time threat detection and response.

TIP

Maintaining code consistency and secure transport management helps prevent the introduction of vulnerabilities during development and deployment of system changes.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Securing user access

User access needs meticulous management to minimize internal threats. Focus on these key areas:

- **Role design:** Design user roles based on the principle of least privilege, ensuring access is limited to what's necessary for job functions. This minimizes the risk of unauthorized access.
- **Access analysis:** Regularly analyze and review access to prevent inappropriate access. Continuous assessment helps maintain a secure environment.
- **Separation of Duties (SoD):** Implement SoD policies to reduce the risk of fraud and error. Proper SoD ensures that no single user has excessive risky access.

Setting up dynamic access controls

Enhance security by implementing dynamic access controls that adapt to changing threats and user behavior. Consider these measures:

- **Data masking:** Use dynamic data masking to protect sensitive information. Masking data reduces the risk of exposure to unauthorized users.
- **Data filtering and scrambling:** Implement data filtering and scrambling techniques to further secure data. These techniques add an extra layer of protection.
- **Activity and session logging:** Monitor user activities and sessions to detect and respond to suspicious behavior. Continuous logging helps in early detection of threats.

WARNING

Failure to implement dynamic access controls can leave your organization vulnerable to sophisticated threats that exploit static security measures.

Managing controls and quantifying risks

Ensure quality risk detection and management by implementing robust control mechanisms:

- **Controls management:** Maintain a single repository for business process and IT general controls that monitor

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

100 percent of transactions. Centralized controls management simplifies compliance efforts.

- **Risk quantification:** Quantify risks to prioritize remediation efforts effectively. Understanding the impact of risks helps allocate resources efficiently.
- **Change monitoring:** Monitor changes to configurations and master data to identify potential breaches early. Early detection allows for timely response to security incidents.

By implementing these layers, you can create a resilient security posture that adapts to new threats and ensures comprehensive risk management.

Securing Your Environment from End to End

Building an end-to-end security strategy involves breaking down the layered security approach into executable steps. Each layer of security includes specific functionalities and benefits that contribute to the overall security posture. To secure your environment from end to end, follow these steps:

1. **Secure the system architecture to identify and address vulnerabilities and threats.**

   Key functionalities include

   - **Vulnerability management:** Regularly assess and patch vulnerabilities. Continuous assessment keeps your systems protected.
   - **Threat detection and response:** Implement systems to detect and respond to threats in real time. Real-time response reduces the impact of security incidents.

2. **Focus on managing code changes and data transportation through the system landscape.**

   Pay attention to repeated scans and frequent reviews. Both controls and transport management tend to change over time — often quickly — so what works today may need to be updated tomorrow.


TIP

Consider implementing a mandatory review process associated with any changes to code (such as deployment scanning) and transports.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

3. **Review existing access.**

   User access and role life cycle management are deeply connected. Aside from policy compliance — which is no small task — review processes are critical. Roles change often, so robust change management procedures and frequent user access reviews ensure those changes conform to your Zero Risk posture.

4. **Enable dynamic access controls.**

   Dynamic access controls are tied to your approach to access management. The more dynamic these controls, the more resilient to change they will be. Observation and testing to ensure that your data is well protected and masked are critical.

5. **Continuously monitor all elements.**

   Use a system that reports changes and risks in an easily digestible format with reports and dashboards. This allows you to quickly respond when risks surface or changes that may break policy are enacted.

REMEMBER

It's easy to think you're re-reading a section on continuous monitoring because it's mentioned so often. However, continuous monitoring is the critical, too-often overlooked component of a Zero Risk posture that *keeps* your identity and application access secure over time.

Replacing Multiple Legacy Technologies

Every organization is at a different stage in its journey toward Zero Risk. Some rely on outdated technologies, while others perform tasks manually or use multiple vendors to address various risk areas. Moving beyond these practices involves replacing multiple legacy technologies with innovative solutions that offer a unified approach to risk management.

TIP

Innovative platforms provide multiple benefits:

- **Reduced total cost of ownership:** By consolidating functionalities into a single platform, organizations can reduce costs associated with managing multiple tools.
- **Simplified vendor management:** Managing fewer vendors simplifies operations and reduces complexity.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Standardized user experience:** A unified platform offers a consistent user experience, making it easier for employees to follow security protocols.
- **Improved audit controls:** Simplified and improved controls ensure compliance with regulatory requirements.
- **Greater efficiency:** Significant daily task time savings and reduced risk exposure lead to overall cost savings.

REMEMBER

Transitioning to innovative solutions requires careful planning and execution to ensure a smooth transition from legacy systems. When you identify the solutions you want to utilize, integrate the following steps into your process:

1. **Assess current technologies.**

   Evaluate existing technologies and identify areas where legacy systems are still in use.

2. **Define quick wins.**

   Identify areas that can be quickly improved with the new solution and deliver these, remembering to communicate broadly the project's success.

3. **Plan the transition**.

   Develop a detailed plan for transitioning to innovative solutions, including timelines, resource allocation, and training requirements.

4. **Implement and monitor.**

   Execute the transition plan, continuously monitor progress, and address any challenges that arise.

5. **Optimize and improve.**

   Continuously optimize the new solutions to meet evolving security needs and regulatory requirements.

TIP

Throughout these steps, make sure to engage stakeholders across the organization to ensure a smooth transition and buy-in for the new solutions.

By transitioning from legacy technologies to innovative solutions, organizations can achieve a strong security posture that adapts to new threats and ensures ongoing compliance and resilience.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Exploring the comprehensive features of Pathlock Cloud
- Utilizing Pathlock's products in risk management
- Integrating Pathlock solutions for a Zero Risk security platform

Chapter 4
Establishing Zero Risk with Pathlock Cloud

Pathlock Cloud is a powerful platform designed to handle the complexities of risk and compliance management across various business applications. This chapter outlines the key offerings of Pathlock Cloud, takes a detailed tour of its individual products, and explains how integrating these products can help build a Zero Risk security platform.

Understanding the Pathlock Cloud Offering

Businesses today rely on a multitude of applications to manage operations, finance, human resources, and customer data. Ensuring that access to these applications aligns with security protocols and compliance regulations is a constant challenge. Misconfigurations, unauthorized access, and errors can create vulnerabilities leading to data breaches and costly compliance fines.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Pathlock Cloud is built to tackle these issues head-on by offering a centralized solution for visibility, control, and automation. Pathlock Cloud can help you with the following crucial areas:

- **Risk reduction:** Access risk is evaluated before user access is provisioned. This proactive approach prevents potential threats by ensuring that only authorized and verified users gain access to sensitive applications.
- **Simplified compliance:** Automated risk assessments and control testing ensure regulatory standards are met. By automating these processes, Pathlock Cloud reduces the workload on compliance teams and ensures consistent adherence to regulations.
- **Streamlined access management:** Efficient and accurate user provisioning and access reviews streamline the management of user permissions across various applications, minimizing the risk of unauthorized access.
- **Separation of Duties (SoD) enforcement:** Identifies and resolves conflicts that could lead to internal fraud. Pathlock Cloud helps organizations enforce SoD policies effectively, preventing any single individual from having too much control over critical processes.
- **Ease of use and reduced cost:** The cloud-based platform allows for quick deployment and intuitive use, reducing costs and workload associated with your most business-critical systems.

REMEMBER

Effective risk and compliance management with Pathlock Cloud can significantly enhance your organization's security posture and operational efficiency. Additionally, Pathlock Cloud supports a wide array of integrations with existing business systems, making it a versatile tool for organizations of all sizes. The ability to customize and scale its features to meet specific organizational needs further cements its role as a pivotal component in achieving Zero Risk.

Taking a Tour of Pathlock's Individual Products

Pathlock Cloud integrates with critical business applications and enterprise resource planning (ERP) systems, providing functionalities across different modules.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Establishing AAG

Application Access Governance (AAG) is essential for a Zero Risk environment, providing least privilege access and supporting multiple security models. It offers deep visibility and intelligent insights into application ecosystem risks, helping organizations manage user access more effectively. Pathlock Cloud offers:

- **Access risk analysis:** Identifies user and role conflicts and manages SoD for all critical business applications

  This module provides detailed insights into potential risks associated with user roles and permissions, enabling organizations to take corrective actions promptly.
- **Compliant provisioning:** Supports efficient onboarding, management, and removal of user access to maintain regulatory compliance

  By automating these processes, organizations can ensure that user access remains aligned with compliance requirements at all times.
- **Certifications:** Reduces the effort and costs associated with managing access reviews

  Automated certification processes help maintain up-to-date records of user access, risks, and controls and ensure compliance with internal and external audit requirements.
- **Elevated access management:** Provides audit-ready privileged access workflows and ensures access removal when no longer needed

  This feature helps mitigate the risks associated with privileged accounts by ensuring that elevated access is granted only when necessary and is properly documented.
- **Role management:** Automates the design, update, and maintenance of roles

  This ensures that roles are continuously aligned with organizational changes and security policies.

TIP

Regularly updating roles and access privileges based on usage data helps maintain a secure and efficient environment.

Getting visibility through CCM

Continuous Controls Monitoring (CCM) addresses challenges in a rapidly evolving risk landscape by offering real-time visibility

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

into control effectiveness through continuous monitoring of business transactions. The key components include the following:

- **Controls management:** Maintains a single repository for business process and IT General Controls, aligned with industry frameworks. This centralized approach simplifies the management of controls and reduces the administrative burden on audit and compliance teams.
- **Risk quantification:** Identifies controls violations and quantifies their financial impact, prioritizing remediation efforts. By understanding the potential financial consequences of control violations, organizations can allocate resources more effectively to mitigate the most significant risks.
- **Change monitoring:** Monitors changes to configurations and master data to identify potential breaches early. Early detection allows for timely response to security incidents.

REMEMBER

CCM expands an organization's cybersecurity posture from a snapshot of potential risks to a detailed picture of actual user activities, including complete audit documentation. This comprehensive view allows organizations to respond more effectively to emerging threats and maintain a robust security posture.

Establishing cybersecurity through application controls

Pathlock offers several core cybersecurity functionalities:

- **Dynamic data masking:** Dynamically masks and anonymizes data to enforce data governance policies

  By applying data masking techniques, organizations can protect sensitive information from unauthorized access while maintaining the usability of the data for legitimate purposes.
- **Vulnerability and code scanning:** Reduces application security risk backlogs, allowing quick action on significant risks

  Regular vulnerability scanning and code analysis help identify and remediate security weaknesses before they can be exploited.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Threat detection:** Offers focused visibility into threats with continuous monitoring and integration with incident response solutions

  This ensures that potential security incidents are identified and addressed promptly, minimizing the impact on the organization.

- **Transport control:** Monitors, reviews, and blocks suspicious transports, expanding on the SAP transport management system with additional security controls and automation

  This feature enhances the security of data transfers and ensures that only authorized and secure transports are allowed.

WARNING

Failing to implement continuous monitoring and dynamic data masking can leave your organization vulnerable to sophisticated cyber threats.

Integrating Products to Build a Complete Zero Risk Platform

Pathlock's suite of products is designed to provide a comprehensive Zero Risk strategy. This involves a structured approach of getting clean, staying clean, and optimizing processes.

REMEMBER

Integrating Pathlock products into a unified Zero Risk strategy provides a scalable, efficient, and secure framework for managing access and compliance. By following the get clean, stay clean, and optimize approach, organizations can establish a robust identity governance and risk management program. This leads to a more secure, compliant, and efficient application environment, paving the way for sustainable growth and resilience in the face of evolving cybersecurity threats.

Getting clean

To tackle getting clean, you want to cleanse your data, standardize your processes, and make sure you have risk assessment. Here's the process:

1. **Start by focusing on data cleansing.**

   In this step, you identify and remove duplicate or inaccurate user identities and access entitlements.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

2. **Standardize access request processes and entitlement descriptions for clarity.**

   This step ensures consistent and accurate access controls across all systems.

3. **Utilize application access risk assessments.**

   The analysis and review of access risks level sets the current risk landscape across all in-scope applications.

REMEMBER

These steps are crucial for establishing a strong foundation for your identity and access management (IAM) program.

Staying clean

Ongoing, you'll want to stay clean. You should implement automated processes for monitoring changes in user activity and access requests. Maintain dashboards and compliance reporting to give visibility across the application landscape, ensuring continuous alignment with security policies. This phase ensures that the integrity of your Identity Governance and Administration (IGA) system is maintained over time. Your checklist, then, is essentially to implement and ensure you have both of the following:

- **Automated monitoring:** Implement automated processes for monitoring and managing changes in user activity and access requests.
- **Visibility:** Maintain dashboards and compliance reporting to give visibility across the application landscape.

Optimizing

After you get clean and stay clean, you can *then* look to optimize. Analyze data collected during the stay clean phase to identify areas for improvement, such as streamlining user provisioning and access revocation workflows. Implementing self-service access request portals for low-risk activities can lead to significant efficiency improvements. Continuous optimization helps organizations adapt to changing security needs and regulatory requirements.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Planning and implementing a Zero Risk environment
- Automating access risk analysis and provisioning
- Managing elevated access and ensuring continuous controls
- Detecting threats and managing vulnerabilities

Chapter 5
Ten Ways Pathlock Cloud Can Help

This chapter outlines ten best practices from Pathlock that can help your organization achieve a Zero Risk application environment. From planning and analyzing access risks to managing elevated access and implementing continuous controls, these strategies help you maintain security and compliance.

REMEMBER

Pathlock's solutions give you critical tools for planning a proactive defense strategy to continuously monitor and manage risks, and each item outlined in this chapter plays a vital role in maintaining security and compliance while growing in an ever-evolving digital landscape. By following these ten best practices, you can effectively manage access and ensure a Zero Risk application environment.

Planning for a Zero Risk Environment

Achieving a Zero Risk application environment means taking a proactive stance with a layered defense strategy. This isn't just about patching up vulnerabilities as they pop up; it's about setting

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

up multiple layers of security to catch issues before they become actual problems.

Pathlock's team of certified information systems auditors (CISAs) and advisors help organizations plan their approaches to implementing new solutions to meet Zero Risk goals. Pathlock's portfolio of products and solutions, designed with flexibility in mind, provides the assurance that customers are met where they are today in their journey to Zero Risk and helps them plan for the future.

Analyzing Access Risk

Managing who gets access to what in your applications is a big deal. Pathlock helps simplify this with automated tools that handle Separation of Duties (SoD) and access risk analysis. Instead of juggling spreadsheets and manual tests, you get customizable rules that streamline the process, making compliance a breeze and cutting down on costs. Automating this analysis not only keeps you compliant but also tightens security by ensuring the right people have the right access.

Provisioning Compliant User Access

Granting and managing user access efficiently is crucial for maintaining regulatory compliance. However, the traditional process can be slow and disruptive, often leading to delays that affect productivity. Pathlock's automated approach to compliant provisioning streamlines this process. You can quickly onboard, manage, and remove user access as your business needs change — all while proactively managing risk and staying compliant with regulations. This means no more waiting for days to get access approved; users get what they need quickly, keeping everything running smoothly.

Managing Elevated User Access

Handling elevated or privileged access is a high-stakes game. If not managed properly, it can open the door to significant security risks and compliance violations. Pathlock simplifies this by providing automated workflows for managing privileged access. This

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

ensures that elevated access is granted only when necessary and is removed promptly when no longer needed. The built-in workflows not only meet audit requirements but also add extra layers of security, reducing the need for additional IT resources and mitigating risks associated with emergency access to critical systems.

WARNING

Be vigilant about granting elevated access. Always ensure access is necessary, temporary, and removed on a timely basis to minimize security risks.

Establishing Credibility through Certifications

REMEMBER

As employees move around within the company, make sure you routinely review and recertify user access to reduce the risk of excess and unutilized access. Pathlock makes this process easier by automating user access reviews. This automation eliminates the need for manual tracking with spreadsheets and reduces the hassle of chasing down reviewers. By ensuring that access reviews are accurate and timely, you can maintain compliance and enhance your security posture without the usual headaches.

Pursuing Zero Risk through Clean Role Design

Designing and maintaining user roles within critical business applications can be a complex task. Pathlock's role management solution simplifies this with a visual role builder and manager. It lets you assess the quality and compliance of existing roles and design new ones that meet regulatory standards. With features like simulations and "what if" analyses, you can dynamically adjust roles to adhere to access policies, ensuring that every role is compliant and optimized for security.

Setting Up Continuous Controls

Continuous monitoring of business processes is essential to maintaining a resilient security posture. Pathlock's continuous controls capability offers real-time visibility into the effectiveness of controls

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

by constantly monitoring and analyzing transactions. Using automation and advanced analytics, it identifies issues, quantifies risks, and prioritizes remediation efforts. This proactive approach not only helps in maintaining compliance but also significantly reduces the administrative burden associated with audit preparations.

Quantifying Your Risks

Understanding the financial impact of risks is crucial for prioritizing remediation efforts. Pathlock not only identifies control violations but also quantifies their financial implications. By analyzing transaction data, organizations can better understand the monetary risk associated with SoD conflicts and other access issues. This detailed analysis allows businesses to focus their resources on addressing the most critical risks, reducing the time and costs associated with audits.

Detecting and Responding to Threats

In today's digital landscape, detecting and responding to threats quickly is crucial. Pathlock's Threat Detection and Response solution offers focused visibility into threats facing your critical business systems. With continuous monitoring, it identifies both internal and external threats and integrates seamlessly with your incident response applications. This ensures that your security and application teams are always aware of potential threats and can act promptly to neutralize them, maintaining the integrity of your business processes.

Managing Vulnerabilities

Vulnerability management is a continuous process that involves identifying, assessing, and mitigating risks within your applications. Pathlock's vulnerability and code scanning tools help reduce the backlog of security risks by providing visibility and context. These tools enable application security professionals to prioritize and address the most significant threats, reducing the potential for exploitation and data theft. By focusing on the most critical vulnerabilities, you can ensure that your applications remain secure and compliant.

These materials are © 2024 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

pathlock

What Next-Gen IGA from Pathlock Looks Like

Is your identity governance system helping you identify and mitigate authentic entitlement risks? Or is it just provisioning and certifying access without usage and risk context included?

ELEVATE YOUR IDENTITY GOVERNANCE

- **Automate single and cross-app risk identification and analysis:** Minimize potential user access risk with simulated authorization decisions, fine-grained access controls, and compliant provisioning.
- **Streamline access certifications:** Automate access reviews with clear risk indicators and quantified potential impacts.
- **Achieve true security and compliance:** Go beyond basic compliance by focusing on real identity risks and ensuring your systems are genuinely secure.

PATHLOCK CLOUD EMPOWERS YOU TO:

Proactively identify SoD risks: Detect conflicts where a user's access might violate SoD policies.

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

Boost efficiency and ROI: Gain back valuable time, reduce cost, and optimize resources.

Enhance your IGA initiatives with Pathlock's Zero Risk approach.

Visit **www.pathlock.com/next-gen-iga** to learn more.

Your journey to Zero Risk begins here

Fight cyberattacks! This For Dummies guide unlocks Zero Risk application security for everyone. It's your blueprint for securing data in today's digital world. Learn how to build a fortress around your information, from startups to global businesses. Master proven technologies and best practices for ironclad cybersecurity. Achieve Zero Risk and safeguard your organization's sensitive data.

Inside...

- Understanding Zero Risk
- Zero Risk versus Zero Trust
- Planning your Zero Risk approach
- Maturing your cybersecurity model
- Aligning with regulatory frameworks
- Layering security to reduce risks
- Leveraging Pathlock Cloud

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

ISBN: 978-1-394-23621-3
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.