LEARNING MADE EASY

2nd Palo Alto Networks® Special Edition

Cloud Security & Compliance

for dummies®
A Wiley Brand

Embrace DevSecOps

Get started with cloud-native application security

Use a Zero Trust Strategy

Brought to you by:

CORTEX® CLOUD
BY PALO ALTO NETWORKS

Lawrence Miller, CISSP
Petros Koutoupis

About Palo Alto Networks®

Palo Alto Networks is the world's cybersecurity leader. Our next-gen security solutions, expert services, and industry-leading threat intelligence empower organizations across every sector to transform with confidence. With Prisma® Cloud, Palo Alto Networks delivers the industry's most comprehensive cloud-native application protection platform (CNAPP) with the broadest security and compliance coverage—for applications, data, and the entire cloud-native technology stack—throughout the development lifecycle and across hybrid and multicloud environments. Our integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate secure cloud-native application development.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cloud Security & Compliance

Palo Alto Networks 2nd Special Edition

by Lawrence Miller, CISSP, and Petros Koutoupis

for dummies®
A Wiley Brand

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cloud Security & Compliance For Dummies®, Palo Alto Networks 2nd Special Edition

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

Copyright © 2023 by John Wiley & Sons, Inc., Hoboken, New Jersey

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. 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: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY 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 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

ISBN 978-1-119-90416-8 (pbk); ISBN 978-1-119-90417-5 (ebk)

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 www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

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

Project Editor: Elizabeth Kuball
Acquisitions Editor: Ashley Coffey
Editorial Manager: Rev Mengle
Client Account Manager: Cynthia Tweed
Production Editor: Saikarthick Kumarasamy

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Table of Contents

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

Today, digital technology defines the competitive battleground, and organizations are constantly striving to improve their services with new applications. These organizations are rapidly adopting cloud technologies to keep pace with growing business demands and take advantage of efficiencies and scalability in the cloud. As a result, the traditional corporate perimeter is fading, and mobile workers are driving ever-increasing usage of Software as a Service (SaaS) applications. Organizations today are using a mix of private and public cloud services to gain the cost savings, agility, and speed benefits of the cloud.

As a result of this digital transformation, risk management and data protection are top concerns for organizations migrating to the cloud. IT leaders worry about securing the business. Whether on-premises, in the cloud, or mobile, the entire IT architecture must be secure to preserve the integrity and longevity of the business.

Legacy security tools, policies, and processes designed for traditional data centers and IT operations can't adapt to address SaaS applications or the continuous deployment model and pace of change in the cloud. Although many tools are available for securing the cloud — including native security services from public cloud providers — siloed security products, manual operations, and human errors continue to slow down the business and create risk.

Visibility and control in the cloud are challenging, and cloud environments are complex.

To be successful, organizations need a consistent approach to security that spans all their operating environments, from on-premises data centers to multiple public and private clouds. They need tools and processes that simplify operations through automation driven by machine learning and analytics, and cross-platform capabilities that prevent data breaches across the cloud, data center, and endpoints.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

About This Book

Cloud Security & Compliance For Dummies consists of six chapters that explore

- The evolution of cloud and cloud-native computing and cloud security (Chapter 1)
- How to secure the cloud and cloud-native applications in your organization (Chapter 2)
- The regulatory landscape in the cloud (Chapter 3)
- How to build an effective cybersecurity team and leverage automation in the cloud (Chapter 4)
- Coming trends in cloud security (Chapter 5)
- Best-practice recommendations for securing the cloud (Chapter 6)

Foolish Assumptions

It has been said that most assumptions have outlived their uselessness, but we assume a few things nonetheless:

- You're a chief information officer (CIO), chief technology officer (CTO), chief information security officer (CISO), cloud architect, IT compliance and risk manager, network practitioner, DevSecOps engineer, or security practitioner.
- You generally understand cloud computing and how it supports business agility in your organization.
- You need to better understand the scope and breakdown of cloud risks and how to deploy frictionless security to prevent data breaches without negatively affecting your business and development needs — today and in the future.

If you see yourself in any of these descriptions, then this book is for you! If none of these describes you, keep reading anyway. It's a great book, and when you finish reading it, you'll know quite a bit about cloud security and compliance.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Icons Used in This Book

Throughout this book, we use special icons to call attention to important information. Here's what to expect:


REMEMBER

The Remember icon points out information that you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!


TIP

The Tip icon points out useful nuggets of information. Tips are appreciated, never expected — and we sure hope you'll appreciate these.


WARNING

The Warning icon points out the stuff your mother warned you about. Okay, probably not. But you should take heed nonetheless — you may just save yourself some time and frustration!

Beyond the Book

There's only so much we can cover in this book, so if you find yourself at the end of it, thinking, "Gosh, this was an amazing book! Where can I learn more?," just go to `www.paloaltonetworks.com/prisma/cloud/cnapp-5-must-have`.

Where to Go from Here

If you don't know where you're going, any chapter will get you there — but Chapter 1 is a good place to start! However, if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is written to stand on its own, so you can start reading anywhere and skip around to your heart's content! Read this book in any order that suits you (though we don't recommend upside down or sideways).

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Understanding how the cloud and cloud-native applications have evolved
- Determining your organization's cloud maturity level
- Assessing risk in the cloud
- Defining customer and cloud provider responsibilities

Chapter 1
The Evolution of Cloud-Native Applications and Their Impact on Security

Data drives the market, and for an organization to succeed, its data needs to be constantly accessible by users. That ever-evolving drive for greater accessibility is one of the key reasons why businesses are increasingly moving their IT to the cloud, where 24/7 instant access is the norm. This paradigm shift toward a wider and more accessible network has forced both hardware vendors and service providers to rethink their strategies and cater to new models of storing information and serving application resources.

The cloud has become synonymous not only with all things data storage, but also with web-centric services, which often access that same back-end data storage. Cloud computing provides simplified access to server, storage, database, and application resources, with users provisioning and using the minimum set of resources to host their application needs. Cloud technology is designed to scale its resources up and down to meet constantly

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

evolving consumer demands. This form of computing has enabled businesses to migrate most (if not all) of their workloads from local data centers to the cloud.

In this chapter, you discover the basics of — and transition to — the cloud and cloud-native computing, as well as how to assess your organization's cloud maturity level. You also find out how risk has evolved in the cloud and what the shared responsibility model means for your organization.

Learning Cloud Lingo

It seems as though the cloud is everywhere today. But to ensure we're on the same page when talking about the cloud, let's start by defining a common cloud lexicon with some help from our friends at the U.S. National Institute of Standards and Technology (NIST).

In *Special Publication 800-145*, NIST defines the following five essential characteristics of cloud computing:

- **On-demand self-service:** "A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider."
- **Broad network access:** "Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (for example, mobile phones, tablets, laptops, and workstations)."
- **Resource pooling:** "The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth."
- **Rapid elasticity:** "Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

appear to be unlimited and can be appropriated in any quantity at any time."

- **Measured service:** "Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service."

NIST defines the following four cloud deployment models (although community clouds are not that common):

- **Private cloud:** "The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (for example, business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises."
- **Community cloud:** "The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (for example, mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises."
- **Public cloud:** "The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."
- **Hybrid cloud:** "The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (for example, cloud bursting for load balancing between clouds)."

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Finally, NIST defines the following three cloud computing service models:

- **Software as a Service (SaaS):** "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (for example, web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."
- **Platform as a Service (PaaS):** "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment."
- **Infrastructure as a Service (IaaS):** "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (for example, host firewalls)."

Now that we're speaking the same language with regard to the cloud, let's take a look at the next era of cloud computing.

Introducing Cloud-Native Computing

Cloud-native computing offers a new way of architecting, deploying, and hosting applications in the cloud. The concept challenges what has traditionally been the norm and puts more power into

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

the application itself, while abstracting away everything underneath it.

Each application or process is packaged in its very own container, which is in turn scheduled and managed across a cluster of server nodes. This approach moves applications away from physical hardware and operating system dependencies and into their own self-contained and sandboxed environment that can transparently and seamlessly run anywhere within the data center. The cloud-native approach is about separating the various components of application delivery.


REMEMBER

Containers decouple software applications from the operating system, giving users a clean and minimal computing environment, while running everything else in one or more isolated containers. It's as close to bare metal that you can get when running a virtual instance; the technology imposes very little to no overhead. The primary purpose of the container is to launch a limited set of applications or services (often referred to as *microservices*) and have them run within their own sandboxed environment.

Why a Code-to-Cloud Security Strategy?

Cloud-native applications differ from their legacy counterparts in that they're built from the ground up to run in the cloud. Therefore, any next-generation security strategy needs to be holistic in scope and focused on delivering *secure* applications in the cloud. DevOps, cloud infrastructure, and security teams must have equal visibility and an integrated set of capabilities to safeguard cloud-native applications throughout the entire code/build-deploy-run life cycle. This includes creating secure code and a secure infrastructure for it to run on, across multiple clouds.

Products that can deliver across this entire spectrum are known as Cloud-Native Application Protection Platforms (CNAPPs), and they're fundamentally changing how the cloud is secured. CNAPP, as defined by Gartner, represents a fundamentally new approach to cloud-native security — one that prioritizes systematically identifying and remediating risks, at all stages of the application life cycle, in real time.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Compared to conventional cloud security tools, CNAPPs stand apart in these ways:

- **Automation:** CNAPPs use automation to reduce the manual effort required to secure cloud-native applications, allowing for faster deployment and scaling of the applications.
- **Security policies:** CNAPPs use security policies to define how applications are secured. These policies are used to automatically configure the underlying infrastructure, such as firewalls and load balancers, to protect the applications.
- **Visibility:** CNAPPs provide visibility into the security posture of cloud-native applications, allowing organizations to quickly identify and respond to security incidents.
- **Integration:** CNAPPs integrate with a variety of other security tools and technologies, such as threat intelligence platforms, vulnerability scanners, and incident response tools, to provide a comprehensive security solution.
- **Scalability:** CNAPPs are built to handle the scale and complexity of modern cloud-native applications, providing security protection without adding significant overhead.

A CNAPP protects applications across the full continuum of the development life cycle — from code, build, and deploy to the runtime environment. They can identify security problems in source code, as well as in packages and container images that are staged prior to application deployment. During runtime, too, CNAPPs monitor for risks and vulnerabilities to detect problems that slipped past earlier scans.

CNAPPs address security challenges more efficiently and effectively than conventional cloud security tools. Although it is theoretically possible to stitch together an array of traditional security solutions to detect and respond to various types of risks across the many stages of the cloud application delivery life cycle, only a CNAPP enables you to find and react to such risks in a comprehensive, centralized manner that is tailored to the unique security requirements of cloud workloads.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Securing the Application Life Cycle with CNAPP

Modern, cloud-native application development follows an application life cycle that differs from traditional waterfall models. In the past, applications would have major releases once or twice a year. But today's application development uses a continuous integration/continuous delivery (CI/CD) pipeline that allows applications to be developed, fixed, and enhanced at a rapid pace.

Today's developers are agile and use a DevOps model that can be simplified to three application life-cycle stages:

- **Code/build,** where applications are coded and assembled (mostly from third-party open-source components)
- **Deploy,** where software is packaged for a container repository
- **Run,** where the application is operational, often across different on-premises and public clouds

Now consider the application life cycle from a *security* perspective. Specific risks and threats can occur in each of these stages:

- **Code/build,** where a single security flaw in code can lead to hundreds of vulnerabilities in runtime.
- **Deploy,** where a container image can be poisoned with malicious code before it reaches runtime.
- **Run,** where compromising vulnerabilities in web applications and application programming interfaces (APIs) are common targets for hackers.

Securing each stage is critical because:

- **Code/build:** Identifying misconfigured infrastructure as code and misconfigurations before committing your code leads to secure cloud services.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Deploy:** Policies should be enforced during deployment to ensure only trusted applications can launch within the cloud runtime environment.
- **Run:** The ability to quickly identify expected behaviors and prevent anomalous behavior is critical to securing applications in runtime environments.

Many organizations mistakenly believe that security in the cloud is the cloud provider's responsibility. But although cloud providers are responsible for security of the cloud, the customer is always responsible for the security of their workloads, services, and data in the cloud. This is known as the *shared responsibility* model, which we explain next.

Understanding the Shared Responsibility Model

Cloud-based applications and the data that go with them are becoming increasingly distributed among varying environments to improve organizational agility and reduce costs. These environments include private clouds, public clouds (hybrid or dedicated), and SaaS applications, each bringing its own unique agility benefits and security issues.

Concern over data exposure has made cloud security a priority. The challenge is to balance the organization's need for agility while improving the security of applications and securing the data as it moves between the various clouds. Gaining visibility and preventing attacks that are attempting to exfiltrate data, both from an external location and through a lateral attack, becomes imperative across all the locations where the applications and data reside.

A number of different groups within an organization — including the network team, security team, apps team, compliance team, and/or infrastructure team — may share responsibility for cloud security. However, cloud security is also a shared responsibility between the cloud vendor and the organization:

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Private:** Enterprises are responsible for all aspects of security for the cloud because it's hosted within their own data centers. This includes the physical network, infrastructure, hypervisor, virtual network, operating systems, firewalls, service configuration, identity and access management, and so on. The enterprise also owns the data and the security of the data.
- **Public:** In public clouds, like Amazon Web Services (AWS), Google Cloud, or Microsoft Azure, the cloud vendor owns the infrastructure, physical network, and hypervisor. The enterprise owns the workload OS, apps, virtual network, access to their tenant environment/account, and data.
- **SaaS:** SaaS vendors are primarily responsible for the security of their platform, which includes physical security, infrastructure, and application security. However, these vendors don't own the customer data or assume responsibility for how customers use the applications. As such, the enterprise is responsible for security that would prevent and minimize the risk of malicious data exfiltration, accidental exposure, or malware insertion.

As companies transition from private to public cloud, or to SaaS applications, the responsibility for securing data, apps, and infrastructure falls less into the hands of the enterprise and more into the hands of the vendor (see Figure 1-1). However, regardless of the platform used, the enterprise will always be responsible for ensuring the security and privacy of its own data.

In order to keep applications and data secure, IT security must clearly understand where cloud vendors' security responsibilities end and where theirs begin. To ensure they're fulfilling their security responsibilities as part of the shared responsibility model, organizations must have the right tools. These tools must provide visibility into activity within the cloud application, detailed analytics on usage to prevent data risk and compliance violations, context-aware policy controls to drive enforcement and remediate if a violation occurs, and real-time threat intelligence on known and unknown threats to detect and prevent new malware insertion points.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

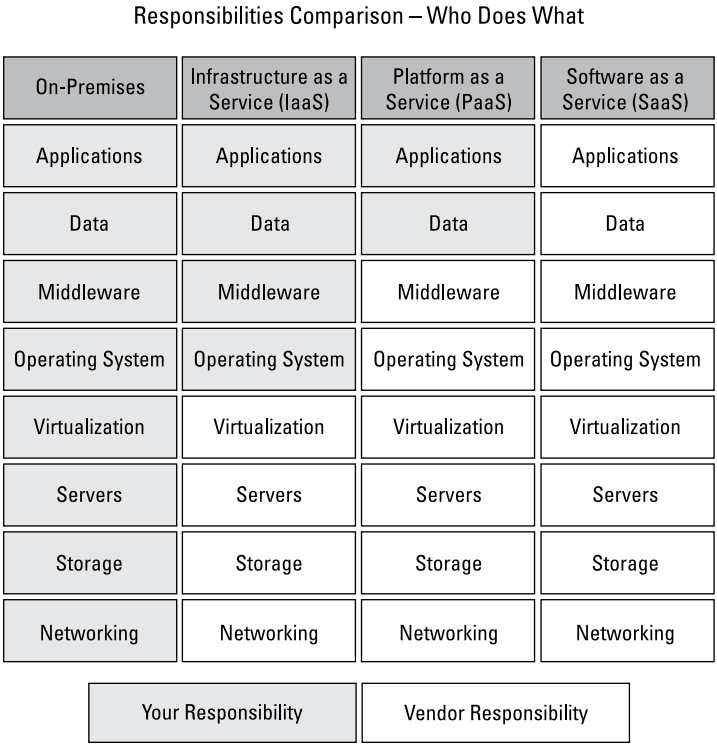

FIGURE 1-1: Cloud security is a shared responsibility.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Building cloud security into the process from the beginning
- Establishing clearly defined responsibilities in your organization
- Knowing your potential risks in the cloud
- Recognizing the limitations of existing tools
- Creating a secure multicloud strategy
- Implementing cloud security best practices

Chapter 2
Getting Started with Cloud and Cloud-Native Application Security

This chapter looks at individual cloud and cloud-native security responsibilities that you need to define in your organization. You find out how to assess risk in the cloud and take a look at your existing cloud security tools. You also discover what it takes to create a secure cloud strategy for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), multicloud, and container environments, and learn about some cloud-focused security best practices.

Building with Cloud Security in Mind

Security tends to be an afterthought in the software development, delivery, and deployment life cycle, and many organizations push it off to the final stages of the process. Before DevOps, the process

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

of developing, deploying, and securing software consumed many months or even years.

Now that more companies have adopted a more continuous integration/continuous delivery (CI/CD) model, releases tend to occur more frequently. The practice of CI/CD enables software engineers to make incremental code changes frequently and reliably while quickly and seamlessly deploying the updated code into production. It may take only weeks, if not days, for a new revision of an application to drop into the public domain.

Waiting until the very last minute to ensure that the application (and the environment in which it's running) is safe and secure destroys the entire process and could potentially derail the application or service delivery. This is why you need to ensure that your ecosystem is secured to its fullest, so you can prevent or mitigate any problems when an application may not have gone through comprehensive security testing before being deployed.

Defining Organizational Cloud Security Responsibilities

REMEMBER

Beyond the shared responsibility model (see Chapter 1), it's important to define individual responsibilities for cloud security within your organization and ensure everyone knows what's required. It's not enough — and even a bit of a cliché — to simply say, "Security is everyone's responsibility." Instead of treating cloud security as a stand-alone policy, the enterprise security strategy should encompass the entire environment, including on-premises data centers and public and private clouds. This strategy should reduce overall complexity with a consistent approach that leverages automation driven by analytics across the environment.

Beginning at the top, executive sponsorship is key. Fortunately, in today's regulatory landscape (see Chapter 3), executive sponsorship is practically mandated. The potential financial impact to a business of regulatory noncompliance can be as devastating as (or worse than) a data breach itself. Beyond the financial penalties, many regulations carry criminal penalties for business executives and other fiduciaries of a business.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Executive sponsorship begins with leading by example. Executives must not only talk the talk, but also walk the walk. If corporate policy, for example, requires corporate data on mobile devices to be encrypted and access to SaaS applications need multifactor authentication (MFA), then "one-off" exceptions shouldn't be made for executives. Beyond leading by example, executives need to ensure that security and compliance initiatives have the appropriate support and resources, and that the impact of strategic business decisions on the overall security and compliance posture of the organization is always considered.

Security and compliance teams must define and enforce appropriate policies that securely enable the business. To be effective, security and compliance teams must understand and align with business goals and objectives, and they must not be a bottleneck to productivity and efficiency.

Line-of-business managers have a responsibility to ensure that everyone in their respective areas of business understands and adheres to the organization's cloud security and compliance governance policies. As business needs evolve, line-of-business managers should partner with security teams to evaluate the risk versus return of adopting new tools. Circumventing a security policy, such as a requirement to use only sanctioned SaaS applications, to achieve a short-term business objective or productivity goal should never be acceptable. Instead, the security tools should adapt to the business need and drive the desired user behavior.

TIP

Working with security and compliance teams also helps to ensure that individual lines of business are able to take advantage of any current relationships the organization may have with vendors or cloud providers to procure services more economically and get support quickly when it's needed, instead of operating in a vacuum with siloed cloud solutions.

DevOps teams are under constant pressure to deliver software projects and updates quickly and reduce time to market. To meet these demands, they must define and understand security requirements at the beginning of any project and ideally integrate them into the application delivery workflow. In this way, development teams can continue moving forward without frequently having to stop and reset to address security vulnerabilities and compliance violations. This is where DevSecOps plays a vital role in the development and delivery process.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Finally, individual end users have a responsibility to follow corporate governance with respect to cloud security and compliance. They must understand the inherent risks in the cloud and safeguard the data to which they've been entrusted as if it were their own personal data.

Benefitting from DevSecOps

With DevSecOps, security is designed into the application or feature from the very start of the development process. A good strategy would be to determine risk tolerance and conduct a risk analysis of that one feature. While scoping projects, here are some common questions to ask:

- How much security are you willing to give the feature?
- How consistent are you with that requirement throughout the life cycle of the feature?
- What happens when you scale that model across multiple features, sometimes worked on simultaneously?

Automation is a key element to ensure consistency in developing and integrating a product according to security requirements and with minimal to no disruptions to operations.

Some key advantages to adopting a DevSecOps model include but are not limited to:

- Increased speed and agility for security teams
- Decreased response time to address change and needs
- Increased or better collaboration and communication across teams
- Increased opportunities for automated builds and quality assurance testing
- Early identification of vulnerabilities in application code

The end goal of DevSecOps is for cybersecurity to become another embedded aspect of your organization's existing culture. In doing so, security is desegregated from the application workflow to ensure that security can keep up with the pace of innovation.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Here are the six most important components that make up DevSecOps:

- The ability to deliver code in small chunks to quickly identify vulnerabilities
- Increased speed and efficiency to source code management and determine whether a recently submitted change is good or bad
- Being in a constant state of compliance (in other words, audit ready)
- The ability to identify potential emerging threats with every code update, giving an organization the opportunity to respond quickly
- The ability to identify new vulnerabilities with code analysis, giving an organization the opportunity to patch the affected code
- Always being up to date with training engineers on security guidelines for set routines

Some people may argue that the "security" piece of DevSecOps is nothing more than a mindset or philosophy. Even if that were the case, a large part of the challenge is identifying the risks early on and using the right tools to move through the entire process, from design to deployment.

Assessing Risk in the Cloud

To properly assess risk in the cloud, organizations should apply any internal risk assessment processes to their cloud deployments. They should also consider using a risk assessment framework, such as the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM). The CCM consists of 16 domains that describe cloud security principles and best practices to help organizations assess the overall security risk of a cloud provider. The 16 domains are as follows:

- Application and interface security
- Audit assurance and compliance
- Business continuity management and operational resilience

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Change control and configuration management
- Data center security
- Data security and information life-cycle management
- Encryption and key management
- Governance and risk management
- Human resources
- Identity and access management
- Infrastructure and virtualization security
- Interoperability and portability
- Mobile security
- Security incident management, e-discovery, and cloud forensics
- Supply-chain management, transparency, and accountability
- Threat and vulnerability management

The CCM also maps individual cloud controls to relevant data protection/information security regulations and standards such as the American Institute of Certified Public Accountants (AICPA), System and Organization Controls 2 (SOC 2), the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA), the International Organization for Standardization (ISO) 27001/27002/27017/27018, the U.S. *Health Insurance Portability and Accountability Act* (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and many more.


TIP

The Consensus Assessments Initiative Questionnaire (CAIQ) is a questionnaire consisting of nearly 300 questions across all 16 of the CCM domains to help you assess the risk of your organization and your cloud providers. Go to `https://cloudsecurityalliance.org` to download a free copy of the questionnaire.

Evaluating Existing Security Tools

Most of the cloud security approaches widely used today have proven insufficient in providing the holistic view of the cloud required to detect and prevent advanced threats and data

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

breaches. Here's a quick summary of the most popular ones and their shortcomings.

Native public cloud security

Cloud security is a shared responsibility between the cloud provider and the customer. In IaaS, customers are responsible for protecting their applications and data running within the public cloud, whereas in SaaS, they're responsible solely for the security of their data.

To aid with protection, cloud service providers offer basic native security services, including access controls and data protection tools. However, the level of security that these native security services provide doesn't meet enterprise requirements and is limited to only that cloud provider. For example, these services leverage tools that are focused on controlling access based on port information (using access control lists [ACLs] and port-based firewalls). They inspect only a small set of applications (using web application firewalls [WAFs]). Fragmented security and complex management overhead often result, because organizations tend to use IaaS, PaaS, and SaaS offerings from multiple cloud vendors. Therefore, organizations must supplement these native security services with additional enterprise security tools and services of their own.

Point products

Using multiple security tools from multiple vendors to solve for specific use cases results in a fragmented security environment in which IT teams must manually correlate data to implement actionable security protections. This level of human intervention increases the likelihood of human error, leaving organizations exposed to threats and data breaches. For example, cloud access security brokers (CASBs) are useful to mitigate risks within SaaS environments. Instead of adding another point security tool that increases operational complexity, CASB capabilities should be part of a broader cybersecurity platform.

Legacy network and content security

Legacy security vendors claim to offer an adequate level of protection to secure your cloud environments. However, what they refer to is often a virtualized instance of hardware placed in the public cloud. This approach is not truly cloud-integrated security,

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

negating the on-demand nature of the cloud and agility benefits. Plus, it lacks the automation required to enable consistent, frictionless security across your entire multicloud environment.

Building a Security Strategy

Ideally, security should speed application development and business growth while preventing data loss and business downtime. Your security vendor should use the same technologies you're using to deliver services to customers:

- **Security delivered as a service** to ensure consistent protection across locations and clouds with an agile, scalable ecosystem
- **Analytics** to confidently automate prevention and prioritize your business
- **Automation** to bridge the cybersecurity skills gap by turning threat detection into prevention, adapting to dynamic environments through context-based access policies, and accelerating response using analytics and machine learning

WARNING

Cloud vendors will profess that their security is better than yours (and it likely is), but attackers don't care where your data is located. They have one goal in mind: to compromise your network, navigate to a target (be it data, intellectual property, or compute resources), and execute their end goal.

To minimize business disruption, organizations must protect their cloud assets. With today's sophisticated attacks, advanced enterprise-grade security is the only way to prevent successful breaches. More important, security capabilities must protect the entire IT environment, including multicloud environments (private clouds, IaaS, PaaS, and SaaS), as well as the organization's data centers and mobile users, using a consistent frictionless approach.

IaaS and PaaS security requirements

Many organizations will transition to the cloud following a "lift and shift" methodology that moves their enterprise applications directly to IaaS using only foundational components — compute,

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

network, and storage. Over time, those same organizations began building applications that leverage cloud efficiencies. Now applications consume multiple components from IaaS and PaaS services (see Figure 2-1). PaaS offerings significantly reduce development time and allow apps to scale efficiently based on demand.

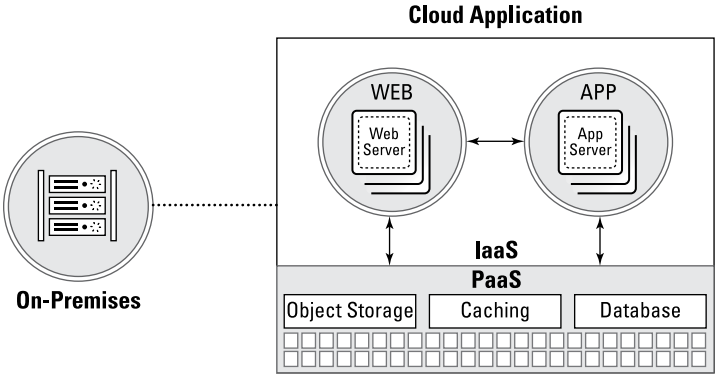

FIGURE 2-1: Application development in IaaS and PaaS.

To provide the enterprise-level security required for applications within IaaS and PaaS environments, a multidimensional approach is needed (see Figure 2-2):

- **In-line:** Protect and segment cloud workloads to safeguard against internal and external threats. By investigating communications in your cloud environment, you'll gain application-level visibility into north–south traffic flowing in and out of your cloud environment, as well as east–west traffic between workloads. Segmentation policies ensure appropriate levels of interaction between various cloud workloads, such as web applications and database workloads.
- **Application programming interface (API)–based:** Provide continuous discovery and monitoring, compliance reporting, and data security. The API-based approach is transparent to developers and enables security teams to discover and monitor cloud resources and assets for any suspicious activity, secure storage services by preventing misconfigurations, and comply with industry standards (such as CSA CCM, ISO 27017/27018, PCI DSS, and SOC 2), as well as regulations (such as the General Data Protection Regulation [GDPR],

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

HIPAA, the Network and Information Systems [NIS] Directive, PIPEDA, and the *Sarbanes–Oxley Act* [SOX]) with customizable reports and controls.

- **Host-based:** Secure the operating system (OS) and applications within workloads. A lightweight host agent deployed within the cloud instance detects any zero-day exploits and ensures the integrity of the OS and applications. As attackers uncover vulnerabilities, the agent-based approach can provide protection until organizations are able to patch components.

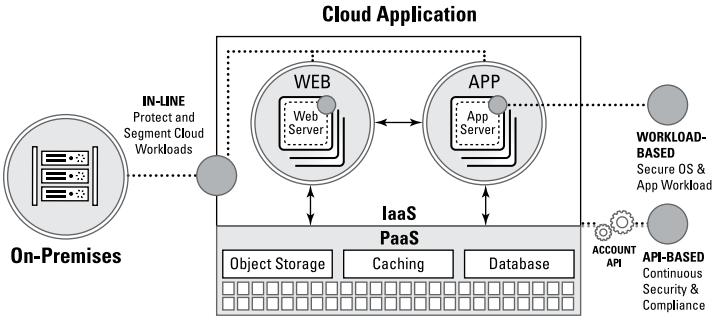

FIGURE 2-2: Critical cloud protections for IaaS and PaaS.

To provide a consistent, frictionless security approach throughout multicloud infrastructure, security should use automation to become part of the development process. Developers don't need to be security experts so long as automated, consistent protections can be inserted into the environment. In addition, it's critical to understand that security requirements for IaaS and PaaS must be delivered through a consistent security approach that supports applications and data across the three major cloud service platforms: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

The following are the deployment modes by which CASB functions are delivered, along with additional recommendations to ensure comprehensive security for your SaaS applications and data (see Figure 2-3):

- **In-line deployment** provides SaaS application usage visibility and granular, real-time policy enforcement. Through in-line protection provided by cloud-based security services

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

or hardware or virtual appliances, you can understand SaaS usage across your users and build policies to control your risk exposure accordingly. Policies can also be enforced when unmanaged devices access sanctioned SaaS applications. This helps prevent exfiltration of sensitive data across all cloud applications.

- **API deployment** provides deeper protections for sanctioned, enterprise-approved applications and performs several functions, including data leak prevention for all data at rest in the cloud application or service, as well as ongoing monitoring of user activity and admirative configurations.

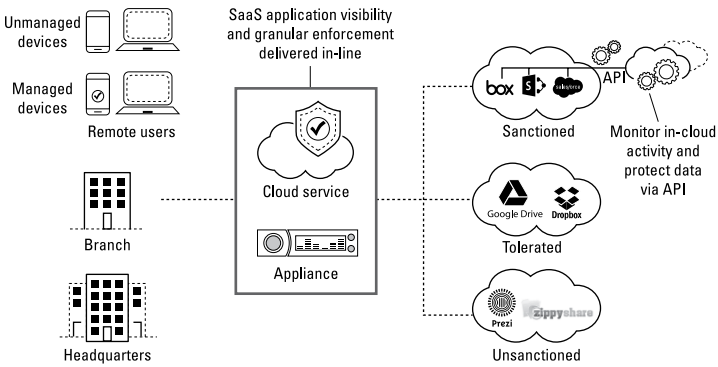

FIGURE 2-3: SaaS security approaches.

In the same way, IaaS and PaaS cloud components must be secured, SaaS applications, such as Box, Dropbox, GitHub, Google Drive, Office 365, and Salesforce, must also be protected using consistent policy enforcement, regardless of application and cloud provider.

Multicloud security requirements

Enterprise data and applications now frequently reside in a multitude of cloud environments, including private and public clouds, spanning IaaS, PaaS, and SaaS.

Despite this momentum, several barriers still slow adoption, and security remains a top concern. Also, although native public cloud security controls provide some degree of access control and identity management, breaches are often the result of improper use,

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

misconfigurations, or advanced threats. Confidently accelerating the move to the cloud requires consistent, automated protections across multicloud deployments that prevent data loss and business downtime.

As organizations embrace multicloud architectures, many will continue to support on-premises applications within traditional data centers or private clouds. Protecting these data centers, as well as your multicloud environments, requires a comprehensive, consistent security strategy. Consistent security becomes even more powerful when you share threat information across the security infrastructure.

MICROSERVICES ARCHITECTURES AND CONTAINER SECURITY

Microservices architectures (discussed in Chapter 1) and container technologies, such as Docker, Kubernetes, and OpenShift, are enabling new application architectures for legacy apps, refactored apps, and microservices, among others. Containers are popular among DevOps teams, in particular, because they provide a fast and relatively easy way to quickly deploy new application workloads in a self-contained "infrastructure as code" package that enables standardization, portability, efficiency, and scalability.

However, these new application architectures also introduce new attack vectors, including control plane attacks against the orchestrator, network-based attacks across the infrastructure, container registry attacks, and host OS attacks.

Current approaches toward securing container infrastructure are insufficient. These include built-in container security that is immature and ineffective, container security point products that have limited scope and don't address the security needs of hybrid applications that use containers and virtual machines, and legacy network security tools that negate the value of containers.

To properly secure container environments, organizations need to deploy in-line network protections and host OS security and API-based continuous monitoring and compliance checks. These security tools enable breach prevention, registry scanning, and orchestrator protections for information assurance, assessment, and monitoring.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Beyond securing your multicloud environments, a comprehensive security platform spans the network and endpoints as well. These security mechanisms — in clouds, networks, and endpoints — essentially act as sensor and enforcement points, working together to arm your business with the collective intelligence required to prevent successful cyberattacks.

Identifying Deployment Best Practices

For enterprises that use the cloud and cloud-native applications, the key to being protected starts with understanding the layers that make up the components of their cloud stack (see Figure 2-4). These different layers — services, identity, app edge, load balancer, compute, and storage — create multiple potential targets, and for the informed, each represents a piece of the cloud environment that can be secured against potential threats.

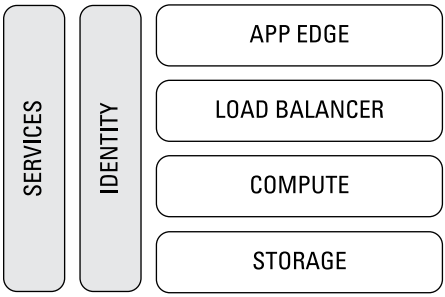

FIGURE 2-4: The layers of the cloud stack.

By focusing on the different pieces of the cloud stack and addressing their unique security threats, your environment will be far more resistant to cybersecurity threats. These best practices will help you secure all layers of your stack.

Lock down identity management

Identity and access management determines what parts of the cloud stack you have access to and what you can do when you're there. If a bad actor can gain access to your systems using your credentials, you're done. Do the following:

- **Require secure passwords.** Use the longest password or passphrase allowed by the system, or use a complex

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

password that includes a mix of letters, numbers, and symbols.

- **Implement MFA everywhere.** Having a strong password is not enough these days. You need multiple layers of protection. Using a second validation or authentication method provides another layer of protection for your user login.
- **Create least-privilege roles.** Give users access to only the fewest accounts and systems that enable them to be productive. Doing so limits the damage if a mistake is made or a bad actor gets access to the account. This is especially important for container images, because they provide a more direct path to the host OS's kernel. That's why it's standard procedure to drop privileges as quickly as possible and run all microservices as nonroot wherever possible. Whenever a containerized process requires access to the underlying file system, it's good practice to mount the file system as read-only.
- **Disable inactive accounts.** When people leave your organization, disable their access to all systems and their access keys immediately. Inactive accounts leave more endpoints vulnerable, and inactive account activity isn't usually monitored the same as active account activity is.
- **Monitor for suspicious user behavior or compromised credentials.** Use real-time monitoring that leverages machine learning and analytics to identify suspicious activity and possibly compromised account credentials.

Secure the compute layer

Take steps to secure your compute layer to ensure availability of systems and data and to keep bad actors from using your compute power to further spread malware across your business and the Internet. Do the following:

- **Harden the OS.** Remove unnecessary programs that only serve to broaden your attack surface. Stay up to date on service packs and patches as much as you can. You may still be vulnerable to a zero-day attack, but it makes such an attack much less likely.
- **Continuously check for misconfigurations and anomalies.** Use automated tools to detect changes across the environment, as well as anomalous behavior.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Enable secure login.** Issue Secure Shell (SSH) keys to individuals. This will keep your assets protected when moving across unsecured networks.
- **Implement inbound and outbound firewall rules.** Set definitive rules about what, how much, and who can send, receive, and access both inbound and outbound data. Many organizations are reluctant to set up outbound rules, but because attackers will try to steal (exfiltrate) your sensitive data and intellectual property, it's important to ensure you have explicitly defined outbound rules. These firewall rules need to be created at the Application layer rather than the Transport or Network layer (IP and port information) to prevent attackers from piggybacking off open ports (such as the Domain Name System [DNS] on port 53).
- **Use only trusted images.** Build your images or templates from scratch or get them from very trusted sources like AWS or Microsoft Azure. Don't use images from Stack Overflow or random message boards and user communities. When you deploy an unknown or unofficial image, you increase the risk of running vulnerable, compromised, or buggy code in your environment.

Secure your storage

If data is the new oil, you want to be sure to protect your precious resources. If attackers get access to your storage layer, they can potentially delete or expose entire buckets or blobs of data. Do the following:

- **Manage data access.** Identity and access management (IAM) policies and access-control lists (ACLs) help you centralize the control of permissions to your storage. Security policies enable you to enable or deny permissions by accounts, by users, or based on certain conditions like date, IP address, or whether the request was over a Secure Sockets Layer (SSL) encrypted session.
- **Classify data.** Automatically classify data to ensure you know what type of data is stored and where it's stored. Data classification policies should be matched to security policies, and any violations should be flagged or automatically remediated.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Encrypt, encrypt, encrypt.** Encrypt your data both in transit and at rest. Note that the metadata is often not encrypted, so be sure not to store sensitive information in your cloud storage metadata.
- **Enable versioning and logging.** Versioning allows you to preserve, retrieve, and restore data if something goes wrong. With versioning turned on, you can always restore from an older version of the data if a threat or application failure causes loss of data. Maintaining access logs provides an audit trail in case someone or something gets into your system.
- **Don't allow delete rights (or require MFA for delete).** You can set up roles in your cloud infrastructure that don't allow users to delete any data. In many cloud storage solutions, you can also enable a feature that requires MFA to delete any version of data stored in your storage layer.
- **Continuously check for misconfigurations and anomalies.** Use automated tools to detect misconfigured storage and permissions settings, as well as anomalous file access behavior.
- **Protect your cloud services.** After you've secured the perimeter and enforced smart policies, you need to focus on security specifically for your services in the cloud. Use source control to secure versions, access to builds, and deployment instances. This will reduce the surface area of your code and limit the potential for attacks across your entire network.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Exploring how cloud impacts GDPR, NIS, and other regulations
- Leveraging automation and continuous monitoring to help achieve compliance
- Understanding how DevSecOps can be used to implement these strategies early in the development process
- Getting ahead with a proactive compliance strategy

Chapter 3
Looking at Regulatory Compliance in the Cloud

This chapter fills you in on several data protection and cybersecurity laws relevant to the cloud. It explains the need for automated, continuous compliance monitoring, and shows you how to be proactive in your compliance efforts.

Navigating the Regulatory Landscape

The regulatory landscape is constantly evolving, with an ever-increasing number of laws and statutes worldwide mandating information security and data protection requirements. Along with more established regulations and standards, such as the U.S. *Health Insurance Portability and Accountability Act* (HIPAA), the U.S. *Gramm–Leach–Bliley Act* (GLBA), SWIFT data protection policies, the Payment Card Industry Data Security Standard (PCI DSS), and the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA), recent laws and regulations have garnered a lot of attention, including the European Union's General Data Protection Regulation (GDPR) and Network and Information

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Systems (NIS) Directive (EU 2016/1148), both of which became enforceable in 2018. These new laws, among others, have important implications for organizations operating in the cloud.

REMEMBER

Compliance requirements are typically based on information security best practices, but it's important to remember that security and compliance aren't the same thing. Security is about protecting the company's assets from harm or exposure; compliance is about following regulations (and avoiding fines for not doing so).

GDPR

The GDPR applies to entities that control or process personal data on individuals located in the European Union (EU). *Personal data* is defined in the law quite broadly as any information relating to an individual that is identified or identifiable. In general, this happens in one of the following scenarios:

- The data identifies or can be used to contact a person (for example, name, email address, date of birth, user ID).
- The data identifies a unique device (potentially) used by a single person (for example, an IP address or unique device ID).
- The data reflects or represents a person's behavior or activity (for example, location, applications downloaded, websites visited, and so on).

The GDPR represents a fundamental shift for personal data protection in the EU. It's much stricter than previous data protection laws, with greater scope of coverage — including companies outside the EU — as well as new data breach notification requirements and significant administrative fines.

The GDPR also introduces mandatory notification requirements for breaches of personal data. Supervisory authorities must be informed, in most instances, if personal data is lost, stolen or otherwise compromised without undue delay and, where feasible, not more than 72 hours after having become aware of it. In certain cases, individuals must be notified as well. Notifications must describe a range of details about the breach, such as its nature, categories, and number of personal data records concerned, likely consequences, and measures taken to address the breach and mitigate its effects.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The GDPR also stipulates administrative fines. The consequences of noncompliance (whether egregious or accidental) can be severe: a potential maximum fine of 4 percent of annual global revenue (or maximum €20,000,000, whichever is higher) for noncompliance with its data processing and data management obligations (such as the requirement to get consent, or various rules regarding data transfers to third countries), and 2 percent (or maximum €10,000,000, whichever is higher) for security and data breach notification-related obligations, amongst others.

The potential reputational harm of data breaches, in addition to the GDPR's mandatory notification mandate, the possibility of regulators' investigations, and significant administrative fines, has firmly placed personal data protection as a board-level concern.

WARNING

The GDPR is likely to require substantial technology, personnel investments, and business process changes for companies to achieve compliance. The GDPR will impact different groups within an organization, including the legal department, the privacy office, and the chief information security officer (CISO), as well as business teams and product engineers that must implement privacy by design. *Privacy by design* means that, within the architecture of the application, network, or transport, the organization has taken measures to ensure the privacy of personal data, regardless of the type.

To this end, the organization must understand the risks of collecting this information and build its systems with the appropriate security. This represents a shift in thinking for many organizations because they now must integrate security into their design process for architectures that are dealing with any kind of accounts or data. Privacy by default is a sister concept to privacy by design in that it accounts for the information that is collected and how organizations must strive to collect the minimum information necessary and minimize their handling of this data.

The vast majority of GDPR requirements center around data management, namely data collecting and processing. There are obligations to provide notice when collecting personal data, prohibitions of unauthorized data processing, requirements to maintain records of data processing activities, a duty to appoint a data protection officer (DPO) in certain instances, and rules regarding transfer of personal data to third parties and third countries, amongst others.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

But this should not overshadow the fact that data security is also a pillar of GDPR. GDPR has specific security-related language, as described in Table 3-1. Plus, a key component of protecting personal data is keeping it secure — both from exfiltration by cyber-adversaries and from internal leakage. So, as organizations work toward GDPR compliance, it's imperative that they complement investments in compliance activities and information management processes and technologies with appropriate investments in cybersecurity.

TABLE 3-1 Summary of Relevant Provisions from the GDPR

Topic	Summary of Provisions
Security of data processing	Organizations must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Those measures must account for the state of the art. **[Article 32]** Personal data should be processed in a manner that ensures appropriate security and confidentiality of the data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing. **[Recital, paragraph 39]** In assessing data security risk, consideration should be given to risks presented by personal data processing. Risks that should be considered include accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of, or access to, personal data. **[Recital, paragraph 83]**
Data breach notification	Supervisory authorities must be notified if personal data is lost, stolen, or otherwise compromised, unless the breach is unlikely to result in a relevant risk to the individual. Notification must happen without undue delay and, where feasible, not more than 72 hours after having become aware of the breach. In certain cases, individuals must be notified. Notifications must describe a range of information about the breach, such as its nature, categories and number of personal data records concerned, likely consequences, measures taken to address the breach and mitigate its effects, and other items. **[Articles 33 and 34]**
Administrative fines	Supervisory authorities are to impose administrative fines for GDPR infringements, on a case-by-case basis. When deciding whether to impose a fine and the amount, the authorities are directed to consider many factors, including the degree of responsibility in implementing technical and organizational measures, taking into account the state of the art as per Article 32. **[Article 83]**

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

The GDPR calls for technical and organizational security measures that account for the state of the art. Legacy security systems, made up of cobbled-together point products, have proven inadequate to prevent the rising volume, automation, and sophistication of cyberattacks. CISOs should review these legacy products carefully to determine whether they meet the state-of-the-art requirement of the GDPR.

NIS Directive

The NIS Directive is the EU's first law specifically focused on cybersecurity. Its goal is to improve the cybersecurity capabilities of the EU's critical infrastructure by establishing security and incident notification obligations for various organizations that offer essential and digital services. The NIS Directive also requires member states to enact national cybersecurity strategies and engage in EU cross-border cooperation, among other measures.

Not to be confused with a regulation, the NIS Directive sets out objectives and policies to be attained through legislation at an EU member state level within a certain time frame (a process called *transposition*). Member states were required to transpose the NIS Directive into national law by May 9, 2018.

The NIS Directive requires that operators of essential services (OESs) and digital service providers (DSPs) use state-of-the-art technologies to manage risks posed to the security of networks and information systems used to provide the covered services. These entities must also take appropriate measures to prevent and minimize the impact of incidents affecting the security of the networks and information systems that are used to provision essential or digital services to ensure the continuity of those services. Security incidents of a certain magnitude must also be reported to the appropriate national authorities. These obligations apply whether the OES or DSP manages its own network and information systems or outsources them to the public cloud, for example.

Recognizing the Importance of Automated, Continuous Monitoring

Security and compliance are shared responsibilities in the public cloud. Many organizations make the mistake of believing that because a public cloud provider manages the security and

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

compliance *of* the cloud, it's also responsible for security and compliance *in* the cloud. That's not the case. It's your data at the end of the day, and if there is a breach or compliance violation, your company will be accountable. The cloud provider delivers a service; the security of your workloads and data is your responsibility as a consumer of the service. It's your revenue, reputation, and customer relationships that are at stake.

A cloud security model should focus on continuous monitoring for, and management of, cloud security risks and threats. In the modern threat landscape, it's absolutely essential to leverage modern tools and automation techniques to ensure that the organization is aware of and prepared to address vulnerabilities at all times. Organizations must be able to rapidly discover and identify threats in real time; understand their severity; and then immediately act through automated policies, processes, and controls. Point-in-time snapshots of the environment are no longer adequate to ensure protection in the face of dynamic, constantly evolving automated threats.

Organizations must measure security and compliance results constantly and must have robust reporting capabilities in place. Achieving this state of continuous security-first compliance requires modern tools and a security platform that leverages the application programming interface (API)–centric architecture of the public cloud.

By using a platform that enables continuous cloud security monitoring and management, IT and security teams will have greater assurance that the organization will be compliant with all applicable policies and regulations within the required frameworks.

This model enables organizations to:

- Compile a complete, unified view across all cloud services.
- Generate compliance reports without the need for specialized knowledge.
- Identify, prioritize, and remediate compliance risks as they arise, with automation driven by machine learning and analytics — without requiring human interaction.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Monitor compliance throughout the entire development life cycle.
- Avoid "last-minute fire drills" to meet compliance requirements.
- Demonstrate to auditors that the organization is managing security 24/7/365 — not just in the last few weeks before an audit.

Compliance and application development teams can both benefit from continuous monitoring and compliance automation. Compliance can significantly reduce time spent on third-party security audits. Application development teams won't get bogged down by compliance audits that stop development projects, thus enabling speed of innovation and development to be competitive differentiators.


TIP

With the right cloud security platform, organizations can leverage automation to reduce risk and remove the human element from vital processes. This automation enables them to achieve complete and continuous visibility across all cloud deployments, enabling standardized, consistent deployments among usage environments such as development, staging, and production.

Avoiding the "Compliance Catch-Up" Trap

For many organizations, compliance is a never-ending cycle of audits, reactionary efforts to correct audit discrepancies, and an inevitable drift from the compliant state over time. This "no-win" situation frustrates everyone in the organization and can derail other projects and security initiatives. The speed of deployments and the pace of change in the cloud creates an impossible situation and, frankly, a futile effort for organizations that rely on legacy tools and manual processes to secure their cloud environments and achieve compliance.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Fortunately, new cloud security tools are now available, delivering an agentless platform designed specifically for public clouds and Software as a Service (SaaS) environments. These solutions leverage the cloud's API to derive tremendous flexibility in scaling and managing cloud security and compliance.

Here's a quick summary of how a modern automated approach to continuous cloud security and compliance works:

1. **Monitoring.**

   The cloud environment is changing continuously. These changes can be normal, routine activities of the DevOps or IT teams; they can also be the work of people who would do harm to the business. As changes are made — across all clouds, regions, and services — the cloud security platform monitors the configurations of the infrastructure to ensure that it adheres to security and compliance best practices.

2. **Evaluation.**

   The security platform securely collects data about an organization's cloud services and continuously performs checks against a series of predetermined security best practices and compliance guidelines. It also performs checks against any predefined custom signatures. These checks determine, on a continuous basis, whether there are any potentially exploitable vulnerabilities.

3. **Deep analysis.**

   The platform performs an analysis to determine whether the discovered misconfigurations and exposures are ranked as high, medium, or low risk.

4. **Automated remediation.**

   The resulting analysis is displayed on a dashboard and predetermined items can be sent to integrated systems for auto-remediation workflows to kick in when possible and appropriate.

5. **Robust reporting.**

   Detailed reports are made available, so teams can see information about the risk, including user attribution and affected resources. Audit reports from reporting and tracking are also available for compliance efforts.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Implementing a Proactive Approach with DevSecOps

The role of the DevSecOps engineer spans across the entire IT stack (including network, server, host, container, cloud and application security) and across the entire software development life cycle (development and operations). In development, the primary focus is on identifying and preventing vulnerabilities. In operations, that focus shifts to monitoring and defending against both inside and outside attacks while maintaining compliance. In order to limit the risk of exposure in the latter, it becomes increasingly important to integrate security practices from the very beginning of the development process.

When an organization implements a continuous integration/continuous delivery (CI/CD) pipeline in its current development model for application delivery, it must integrate security and compliance into this pipeline. Each phase of the pipeline must include automated tasks dedicated to security and compliance, requiring the organization to adopt tools and processes that continuously validate the application as code is written, integrated, tested, deployed, and eventually, operated. These security tools would likely cover

- **Unit testing:** This is the first opportunity to test a piece of code against its functionality.
- **Dependency scanning:** Every software project relies on libraries, and those libraries are often external to the project. Scanning these dependencies for vulnerabilities ensures that the libraries are safe to use and can recommend new versions of software libraries without vulnerabilities.
- **Dynamic application security testing (DAST):** The application is tested for vulnerabilities without analyzing the code in this phase, which is also known as *black-box testing*. Examples include APIs, SQL injections, cross-site scripting, and other external methods sending input parameters to the application.
- **Static application security testing (SAST):** SAST focuses on the code, making it possible to find vulnerabilities earlier and in the development stage without exercising the code.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Container scanning:** Even when obtaining or building container images from reliable sources, it's crucial to scan the container images for vulnerabilities, malware, and other security measures to ensure that nothing sneaks through the cracks and into production.

Four Ways to Improve Cloud Security and Compliance

The cloud requires a new way of approaching security. Traditional data center and endpoint security technologies and methodologies are not adequate to protect the highly connected architecture of the cloud. Without a modern, cloud-first approach, security will be compromised because of a variety of factors.

Organizations can address the inherent risk-related challenges by employing a security platform built for the cloud that leverages automation to provide continuous monitoring, analysis, prevention, and remediation for cloud security and achieving compliance.

This is a new model that provides comprehensive protection in the cloud. As organizations continue to rely on public cloud to drive both day-to-day business activities and innovation, they must reduce security risks and simplify the processes involved in ensuring protection and compliance. Continuous security and compliance present a new opportunity to maximize the value of the public cloud while minimizing risk.

Security experts seek innovative, usable solutions. They say it's important to focus on the following four key elements to achieve continuous and automated cloud security and compliance:

- **Rapid discovery to keep up with the fast pace of change in the cloud:** With the enormity of deployments in the cloud, it isn't unusual for organizations to have millions of data points (such as user or application behavior and configuration settings for cloud services) that need to be evaluated. You need a platform that can handle all the data in real time and rapidly isolate any security variation or deviation from known states.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **A "single pane of glass" to view your entire cloud environment:** When teams are very large, communication can falter. With each team using different tools to gain a different view of the environment, information becomes siloed and difficult for other teams to understand. Your platform should let teams own their own security, while also providing a big-picture view to security operations teams and corporate management. The platform must be able to evaluate security data in isolation, as part of the global customer base or across time and geography, to warn about potential issues before they occur.
- **Automated response:** Organizations need to automate not only monitoring and analysis, but also remediation to fix permission or configuration errors. They should have flexibility in determining the course of automated response, with the ability to inform human administrators if there is any other action that may be required.
- **Robust reporting:** Teams need to be able to measure and demonstrate security and compliance progress daily, not just during the yearly audit. With the right platform, you can show your security and compliance posture at the push of a button.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Identifying the cybersecurity resources and skills your organization needs
- Aligning cloud maturity and automation levels
- Creating a secure application development culture

Chapter 4
Building an Organizational Culture around Security

This chapter explores the key elements of creating an effective cybersecurity team, how to leverage automation to augment your cybersecurity team, and how to build a secure application development culture within your organization.

Managing Cybersecurity in the Modern Era

Enterprise security isn't easy, and the speed at which enterprises are moving today to innovate and deliver digital services isn't making the challenge any more straightforward. Considering aggressive timetables and delivery deadlines, it's easy to let the discipline required for effective security slip. But with today's hyper-connected world and fast-moving and changing

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

cloud environments, letting security slip for even a moment is just something that enterprises simply can't afford. To succeed, enterprises must have the processes and technology — and most certainly the people — in place to keep systems adequately secured.

Cybersecurity is more than just the technology required to secure an organization's computing environment. A company's cybersecurity culture includes the attitude, knowledge, assumptions, norms, and values of the workforce, and is shaped by the organization's goals, structure, policies, processes, and leadership. The people who make up the organization are the most effective tool for responding to cyberattacks and security threats. An organization is only as good as its least secure weakest link, so it's critical to foster an environment where the employees have the knowledge and instinct to both identify and immediately respond to cyber-threats. A cyber-savvy and secure culture improves an organization's reputation with customers while also building employee pride.

Creating an effective cybersecurity team

Creating an effective cybersecurity team begins with an assessment of your organizational needs. This includes identifying teams that you may need to create (for example, incident response and compliance audit teams), as well as the required skill sets. Next, identify any skills gaps within your current cybersecurity team and decide whether those gaps can be filled by training current team members. If they can't, you may need to hire additional staff.


TIP

When assessing your organization's cybersecurity needs, remember that automation can enable more rapid response to security incidents by eliminating manual security tasks. Automation frees up existing team members to perform other value-added cybersecurity tasks while also limiting the need to hire additional team members.

Planning your automation strategy

Automation can be a bridge between the shortage of qualified cyber-talent in the market and effective cybersecurity. A recent joint research project by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) found that

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

28 percent of cybersecurity professionals and ISSA members feel their organizations depend upon too many manual processes for their day-to-day security operations, such as chasing down data, analyzing the data, investigating false-positive alerts, or managing remediation tasks. This is exacerbated by a looming shortage of skilled cybersecurity professionals.

There simply aren't enough hours in the day to get to everything, no matter the skill level of your cybersecurity team. With automation, advanced analytics, and security integration, you can begin to bridge the gap. From the cyber-defender's perspective, there are three ways automation can help an organization:

- **Turn threat detection into threat prevention.** Organizations shouldn't spend any time manually preventing known threats, because prevention should be automatic. The same goes for unknown threats — they need to be automatically analyzed and blocked if they're malicious.
- **Adapt to dynamic environments through context-based access policies.** The IT landscape is constantly changing. Security teams must be able to set policies based on the context of what should be protected: users, data, and applications. Context-based policies stand the test of time and adapt to business changes without requiring constant updates.
- **Automate investigations using analytics and machine learning.** Automation supplies critical leverage, giving organizations an edge over adversaries with insight and context around exploits and techniques. With next-generation firewalls that can ingest third-party data feeds and dynamically update policies, automation turns information into prevention. By using rich security data across locations and deployment types, analytics and machine learning find hidden threats and reconstruct attacks. Both of these automation capabilities save you valuable time.

TIP

A security vendor that offers automation essentially gives you back time to do more valuable, business-critical work. It allows your security teams to move away from basic operational tasks and focus on strategic efforts that directly benefit and improve the security and compliance posture of your organization. It also provides teams with the opportunity to train on the latest concepts, tools, and methods around security and application deployment.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Assessing security effectiveness

Finally, it's important to know what success looks like for the team. Key performance indicators (KPIs) should be defined to help the team continuously assess its effectiveness in protecting the organization's cloud assets. Some potential KPIs may include

- Number and types of security incidents reported
- Software as a Service (SaaS) usage, including misconfigurations, accidental sharing, and promiscuous sharing
- Instances of improperly secured virtual private clouds (VPCs) in Amazon Web Services (AWS) and Google Cloud Platform (GCP), and virtual networks (VNets) in Microsoft Azure
- Time to detect security breaches
- Time to remediate breaches and incidents
- Vulnerabilities identified and patched
- Threats prevented

Recognizing How Cloud Maturity Affects Automation Levels

Your organization's cloud maturity (discussed in Chapter 1) is often linked to the level of automation implemented throughout your environment. Automation can oftentimes be applied to processes throughout the security organization, not just in the cloud. Organizations that already use automation extensively in their cybersecurity processes understand the value of automation in reducing potential configuration errors and enabling rapid security response actions when threats are detected.

For intermediate businesses (cloud implementers) and advanced businesses (cloud optimizers), automation becomes increasingly important as these organizations increase cloud usage, expand to multicloud deployments, and optimize cloud operations. With automation, these organizations can successfully scale their cybersecurity operations and reduce the risk of error, allowing them to protect the organization's entire cloud footprint.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Automation helps secure the business by

- Creating touchless deployments to enable security for application development teams
- Protecting the environment from threats without slowing the business
- Flagging noncompliant services as they're spun up
- Dynamically updating policies as the environment changes or new threat information is collected

Embedding Security in the Developer Workflow

Moving at the speed of the cloud raises the concern that costly mistakes could happen. The worry is that, as an organization automates processes and makes rapid decisions in an environment that prioritizes agility, security compromises will be made. Different stakeholders (such as application development teams and individual business groups), who may not be focused on the broader security picture, now play a more significant role in the cloud conversation. If security isn't properly addressed, unintended consequences may ensue — such as security holes due to misconfiguration, choosing "good enough" security, or forgoing security considerations altogether.

Compounding this challenge, enterprises face an unprecedented shortage of professionals with cybersecurity skills, especially skills that are critical when it comes to securing DevOps organizations and cloud environments. Consider how much this gap has grown in recent years: According to the International Information System Security Certification Consortium or (ISC)², the cybersecurity workforce gap increased by 26.2 percent in 2022 compared to the previous year, despite the addition of 464,000 professionals to the industry.

Cloud computing does help to simplify some areas of security, but it doesn't simplify everything. Enterprises are still responsible for the security of their data, applications, operating system, network, firewall configurations, and so on. And although DevOps

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

helps to speed development, it can be challenging to adapt security techniques to keep pace with new application development and deployment capabilities.

In "10 Things to Get Right for Successful DevSecOps," published in October 2017, Gartner wrote:

> Don't force information security's old processes to be adopted by DevOps developers. Instead, plan to integrate continuous security assurance seamlessly into the developer's continuous integration/continuous development (CI/CD) toolchain and processes.

That's easier said than done, of course. It certainly requires having the right technology and processes in place. Getting them in place and keeping them there requires both assembling the right team and making sure everyone on the team does their part. The following critical elements will help an enterprise form a smart framework for running a DevSecOps organization (see Chapter 2).

Continuous cybersecurity skills training and enhancement

DevSecOps teams adhere to security best practices, but how those are implemented, and the speed at which they're used, must adapt to the speed and agility of a DevOps environment. To successfully implement security essentials, the entire DevOps team must understand security basics, including the following:

- Managing secure access to cloud environments
- Keeping configurations in a secure state
- Putting automated controls in place

It's an achievable goal, with the appropriate cross-training and security training. Organizations must train operation teams on good security practices, how to use relevant security tools, and how to script securely. The same goes for developers, who should be continuously trained on secure coding practices to create security champions within the DevSecOps team. And, above all, security professionals need to be in continuous contact and collaboration with the rest of the technology teams (for example, development and networking).

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

To build a team that can keep systems secure at the speed of DevOps, you need staff that collaborates, understands each other's strengths and weaknesses, helps each other to compensate for those differences, and continuously cross-trains.

Security from design through production

Security efforts should be an integral part of the entire IT process, from the new product, feature, or application design phase through development and application testing and into production. Too often, security is first addressed during the quality assurance phase or, worse, in production. Staying secure and compliant requires continuous and automated security monitoring of all systems running in production.

TIP

Integrating security processes and built-in security controls into DevOps empowers application development teams with a DevSecOps model that ensures security is properly addressed throughout the application development life cycle.

Executive leadership

Talk with any chief information officer (CIO) or chief information security officer (CISO) about what it takes to build a security-aware DevOps team, and the top answer — nearly unanimously — will be that leadership support is the determining factor. Successfully building a secure DevOps organization requires leadership that will help to drive and instill security culture and processes.

Automation

When a process can be automated, it should be automated. Through automation, you can accomplish two critical prevention-focused tasks:

- Embed security into your application development workflow, ensuring that security keeps pace with development.
- Ingest external information that can be used to drive or create policies that are dynamically updated as workloads are added or removed from your cloud environment or as new potentially malicious threats are discovered.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cultivating the collaborative mindset

The spirit of DevOps is to break down the silos in IT departments among developers, operations teams, IT leadership, quality assurance (QA), and security, and embed security as a priority throughout all aspects of development and management. However, for most enterprises, security has been more of a roadblock than an enabler.

Communication among security managers and every other team is essential so everyone understands the roles and challenges of others on the team and is able to identify opportunities to improve. This has always been how the relationship between security and the rest of the IT and development teams should be, but it's especially true for DevOps. Communication and empathy regarding the needs of others are critical success factors.

Finally, to foster security collaboration, the right incentives should be in place, such as having security-related KPIs that span multiple teams. Create an environment where security teams collaborate with other groups and set incentives to help keep such collaboration aligned.

Security accountability

To get the DevOps team and the entire organization aligned when it comes to mitigating business risks, it's crucial to have someone who leads the security efforts. Top-level leaders must actively show that they care about security, and there must be regular, continuous, and comprehensive conversations at all levels of the business about the security programs that need to be in place. This is best achieved by having a CISO in place, with backing from the board of directors. Engagement helps create competent security leadership that aligns with DevOps and keeps security efforts synchronized with business needs.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Seeing how cloud threats have evolved
- Analyzing the trend toward tool consolidation
- Looking into the future of cloud security
- Bringing artificial intelligence and machine learning to automation
- Preparing for the future with a blueprint for risk

Chapter 5
Forecasting Changes in Cloud and Cloud-Native Security

This chapter looks at the current landscape of cloud threats and offers a glimpse into the future of cloud computing and security.

Surveying the Evolution of Cloud Threats

Even though Software as a Service (SaaS) application usage proliferates, and workloads are increasingly migrating to Infrastructure as a Service (IaaS), many enterprises continue to maintain on-premises applications, storage, and private clouds. This hybrid IT environment continues to challenge existing security paradigms while also creating additional complexity, exposing organizations to:

- **Cloud-jacking:** Typically, code-injection attacks carried out through third-party libraries, from SQL injection and cross-site scripting.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Phishing:** Attacks that steal user credentials for cloud-services. This can also lead to on-premises attacks. The most innovative phishing attempts are launched through cloud applications instead of the traditional email.
- **Application programming interface (API) vulnerabilities or breaches:** API-based breaches are becoming the most common cloud-native security threats, putting users' privacy and data at risk.
- **Exploitation of system administrative tools to breach enterprise networks:** Cybercriminals will continue to utilize these tools to execute harmful software on the systems that they have direct access to or that are accessible in the now-compromised network.

Consolidating Tools and the Importance of CNAPP

The dispersed-tool approach is time-consuming to manage and creates both unnecessary overhead and friction between security and development. IT teams are forced to work in silos, which can potentially lead to misconfigurations between the tools, creating vulnerabilities and opening the possibility for attacks. In this environment, enterprises are unable to successfully implement cloud and cloud-native security. Identifying this gap, vendors are now offering single converged tools with multiple security capabilities catered to applications and services. These tools reduce security risk, overhead, and operational costs.

The Cloud-Native Application Protection Platform (CNAPP) is a cloud security platform converging multiple existing security and compliance capabilities into one. Originally coined by Gartner, the term CNAPP refers to a new type of cloud security platform focused on securing cloud-native applications from development to production while also reducing friction and mitigating risks that usually result from tool silos.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

At a high level, CNAPP incorporates three key components:

- **Cloud security posture management (CSPM):** Automate the detection and remediation of security risks through security assessments and compliance monitoring and detect misconfigurations that lead to data breaches.
- **Cloud infrastructure entitlement management (CIEM):** Manage access and enforce least-privilege access in the cloud through monitoring cloud identities and recommending policies.
- **Cloud workload protection platform (CWPP):** Protect workloads deployed across public, private, and hybrid clouds. Integrate security solutions early and continuously throughout the application development life cycle.

However, CNAPP is more than the combination of these components. It's designed to ensure

- Clear visibility into workloads and across infrastructure to identify and prioritize risk
- Improved identification and remediation of risk via a consistent life-cycle approach
- Fewer misconfigurations and streamlining of the management of all the components in your environment
- Minimal overhead and complexity while managing tools and software/hardware vendors
- Seamless integration of scanning capabilities into the software development life cycle and developer tools
- Shift-left security (that is, guaranteeing application security at the earliest stages of the development life cycle)
- Insight into and governance of attack path analysis, such as permissions and configurations
- Cloud-native security, not on-premises security adapted to fit the cloud
- Infrastructure and application security

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

CNAPP is an emerging category, still considered more hypothetical than an actual tool with all the converged capabilities vendors are offering. Despite that fact, the risks of cloud security are very real, and until vendors offer these capabilities, you should take action and build your organization and tooling to be ready for CNAPP by doing the following:

- Create a cloud security plan.
- Research vendors with capabilities that offer a strong basis for CNAPP, and evaluate their offerings.
- Continuously scan artifacts, containers, and so on to identify vulnerabilities and malware.

Looking into the Future of Cloud Security

According to Cortex Cloud's *The State of Cloud Native Security Report,* enterprise workloads hosted on the cloud jumped in 2022 to an average of 59 percent (from 46 percent in 2020). It also reported that 69 percent of the 3,000 organizations surveyed now host more than half of their workloads in the cloud. This is more than double the 31 percent surveyed in 2020.

As businesses everywhere continue to migrate their critical applications, workloads, and data to the cloud, public cloud providers will continue to rapidly grow their data center footprints around the world. Data, intellectual property, and compute resources — regardless of their location — are all targets for attackers.

Hackers' goals are to access the network, navigate to their target, and then execute their attack objectives. The public cloud, by the very nature of its growth and visibility, will be a target-rich environment for attackers for the foreseeable future. Attackers understand the shared responsibility model (see Chapter 1) as well as — or better than — most cloud customers do. As such, attackers for the most part will continue to follow the path of least resistance. They'll seek to exploit the weakest link in an organization's cybersecurity chain to gain access to its cloud resources, instead of attempting a direct assault on major public cloud providers such as Amazon, Google, and Microsoft, who themselves invest extensively in cloud security resources.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

One trend in cybersecurity that will clearly continue in the future of cloud security is automation. The speed and scale of change makes it impossible for organizations to effectively manage their cybersecurity posture in the cloud with manual tools and processes. Attackers have wholly embraced automation to proliferate malware and brute-force account credentials, among other attack techniques. Cybersecurity teams must respond with automation tools and techniques of their own.

Cloud application architectures will also continue to evolve with practically infinite compute processing resources, increased adoption of containers, and new innovations in serverless computing. Extremely large data lakes will also be necessary to handle the deluge of data generated by the Internet of Things (IoT), big and small data analytics, machine learning, and more.

These trends will have security implications themselves, but they'll also impact the technologies used to secure enterprise multicloud and on-premises environments of the future. For example, data collection sensors deployed across clouds, users, sites, regions, and devices will enable ever greater visibility and continuous monitoring across heterogeneous environments. The data these data collection sensors generate could be hosted as a common data lake of security and threat events, which security vendors can use to build apps or services to add more value and enhance their customers' security and compliance posture.

As artificial intelligence and machine learning technologies continue to mature and advance, automation will become more critical in areas such as threat detection and security analysis, particularly given the deluge of sensor data and threat information. Anomalies will increasingly be detected and stopped in real time, effectively closing the window of opportunity for cybercriminals.

Drafting a Blueprint to Manage Risk

When your organization moves to the cloud, not only does your risk of breach change, but your risk of failure increases. Developers could take a system down with the click of a button or one wrong line of code in an application deployment. To combat this problem, you must build protections that will reduce security risk and also ensure the availability of critical systems and data. As

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

you re-architect systems and begin to utilize new technologies and architectures like containers and microservices (or whatever comes next), consider how you'll test to ensure that systems perform as designed and deliver the expected results.

You need to adapt your existing risk management and cybersecurity frameworks to address the cloud, as well as new and evolving technologies. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is one example of a great framework to help you get started. The following sections cover the core functions of the framework and how they're affected by your move to the cloud.

Identify

REMEMBER

If data is the new oil, then machine learning is the new filter that makes it usable by your teams and systems. Leveraging algorithms to discover and classify large amounts of data is a must in the cloud.

As you prepare for the future, review your current tool set and skill set to ensure that your team is able to take advantage of new advancements in automated monitoring, detection, reporting, and machine learning. Traditional data center solutions are often unable to keep up with the high volume of data and speed of change. Embed automated security scanning into your DevSecOps workflows, so that analysis and testing become an integrated part of your development life cycle. To speed adoption, don't make developers learn new tools. Instead, look for tools that support application programming interface (API) enablement and provide rich context.

Protect

It used to be that an organization only had to protect and defend what was inside the perimeter of its data center and network. However, as organizations move more workloads to SaaS systems and the cloud, network perimeters are expanding and becoming less distinct at an exponential pace. You now need to protect inside your network, across multiple clouds, and out to wherever your mobile users are connecting to the network. Now that the world is your perimeter, you need different means and tools to protect it. Implementing a Zero Trust security model (see Chapter 6) will help set up your organization for success in the cloud.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Detect

Every organization has been impacted by the shortage in security talent, so it's becoming imperative that organizations of all sizes begin leveraging automation to continuously monitor and analyze events and the effectiveness of deployed controls and protections. Keep in mind that services, virtual machines (VMs), and configurations can change rapidly in the cloud. In fact, some microservices may exist in your cloud environment for only a few minutes. You must be certain that the tools you employ to detect and log changes can keep pace with these rapid fluctuations.

TIP

Cloud technologies can make certain aspects of the detect function more challenging, but they can also be used to your advantage. Consider using security technologies and services to leverage advanced techniques to detect issues, whether vulnerabilities or attacks, in your networks and systems. Technologies and tools that make use of machine learning to address well-defined security problems, like classifying data for compliance purposes, analyzing and correlating events in log files to find insider threats, or identifying malware and advanced threats across all your endpoints, are just a few examples.

Respond

When things go wrong, recognize that you need to do more than just stop an attack. You need to know what was impacted, understand what data was accessed, recognize whether there is a compliance impact, and know what your responsibilities are to report the incident.

Today, this function is as much a business response as it is a technical response. Business leaders need to work closely with security and IT teams to ensure that projects are executed within an acceptable level of risk. Response plans need to rise to the level of the board and executive management to ensure they're prepared if a major incident impacts the business. Lessons from the Equifax breach or the impact of the Yahoo! breaches on its sale to Verizon are not-so-subtle reminders of how important security and public relations are to the valuation and long-term viability of a business.

As part of your response plan, you can use advanced technologies, such as security tools that streamline the orchestration of threat intelligence and enforcement of prevention-based controls.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

New tools can remove the manual work of intelligence gathering by allowing you to make use of public, private, and commercial intelligence sources across both government and commercial organizations — and also enable you to share your threat indicators with trusted peers to contribute to global cyber-defense efforts. These technologies unify your operational, security, and risk management teams through a single source of truth — the same contextual security data from your modern, advanced systems.

Recover

For your recovery efforts, it's important to ensure that you have enough information to know what went wrong, so you can fix it — but in cloud environments, that amount of data is enormous. Look for tools that will provide you with a single pane of glass for all your event and security logs and will normalize disparate data types so your operational teams can establish a new security baseline. Use this new security baseline to reevaluate your existing risk framework and suggest possible improvements.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Looking into the future of DevSecOps
- Adopting a cloud-centric approach and knowing your responsibilities
- Applying "never trust, always verify" to the cloud
- Engaging stakeholders early
- Understanding your potential exposure and adversaries
- Evaluating your options and recognizing the power of knowledge
- Preventing known and unknown threats in IaaS and PaaS environments
- Leveraging automation

Chapter 6
Ten (or So) Cloud Security Recommendations

This chapter highlights the important role that DevSecOps plays in the data center of the future and outlines some key recommendations to protect data and applications in the cloud.

Embrace DevSecOps

Today, DevSecOps is focused on implementing security and risk management protocols into development workflows, ensuring secure and compliant code early in the development process.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Within the next five years, this will likely be the standard way organizations will use DevOps. And through the use of automation, security will continue shifting left, with an increasing number of security and compliance controls embedded into the DevOps life cycle. DevOps and DevSecOps will merge, sharing the same philosophies.

Further growth will continue in the public cloud space, leaving more organizations and their consumers exposed to potential risk. DevSecOps will be a fundamental requirement to operate in the digital world. DevSecOps will provide enough of an incentive for all organizations to adopt its approaches and principles toward a more secure development life cycle.

As we get better at implementing security into the software toward the beginning of the development life cycle, it's likely that the term *DevSecOps* will disappear. The security piece of DevOps won't go away, but it will become standardized in the continuous integration/continuous delivery (CI/CD) process. Having a separate name emphasizing the "security" in DevOps won't be necessary.

Take a Cloud-Centric Approach

The cloud enables your organization to address business challenges with an agile, more scalable approach. To take full advantage of the cloud, apply the concepts of the modern data center to your cloud deployment architecture, while leaving the traditional constructs behind. Doing so will enable your organization to achieve high availability and scalability organically.

Understand the Shared Security Model

Public cloud providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure make it clear that security is a shared responsibility. In this model, the provider is responsible for ensuring that the platform is always on, available, and up to date. In fact, the cloud provider's global data center infrastructure is more secure than most organizations' own data centers. However, you, the customer, are responsible for protecting your own applications and data running within the public cloud.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Figure 6-1 highlights the responsibility breakdown. You're in complete control of what security to implement and you must take steps to safeguard your content, be that customer data or intellectual property. The benefit of embracing the shared security model is that your team is focused on protecting your apps and data, typically your most valuable assets.

Public Cloud Security Responsibility

Security is on you	Applications (including operating system) and associated data deployed
	Account controls (access control, services enabled, and so on)
	Deployment architecture, configuration management, and so on
Security is on the provider	Worldwide footprint (regional presence and so on)
	Physical components (buildings, server hardware, resiliency, and so on)
	Compute infrastructure (network, database, storage, and so on)

FIGURE 6-1: Public cloud shared responsibility model.

Use a Zero Trust Strategy

When you ink a deal with a public cloud or web service, the vendor agrees to provide you with an array of services, but it doesn't assume responsibility for managing your cyber risk. Instead, the vendor provides you with a number of options for how you may set up and configure its security tools.

Traditional, perimeter-centric security strategies fail to provide adequate visibility, control, and protection of user and application traffic. Zero Trust architectures apply the principle of "never trust, always verify" to all entities — users, devices, applications, and packets — regardless of what they are *or* their location relative to the bounds of the corporate network (see Figure 6-2).

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

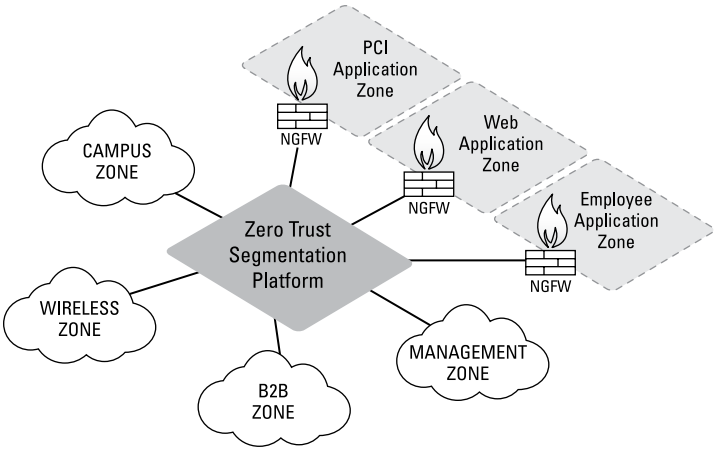

FIGURE 6-2: A Zero Trust segmentation platform.

When enterprise leaders are considering entering into a cloud agreement, they must start developing a security model for protecting the digital business. What's more, because most companies are in multiple cloud environments, they must be able to put in place and oversee a strategy that encompasses multiple platforms in multiple locations, where regulations can vary dramatically.

By establishing Zero Trust boundaries — just as they would to effectively compartmentalize different segments of their own networks — companies can better protect critical data hosted in the cloud from unauthorized applications or users, reduce the exposure of vulnerable systems, and prevent the movement of malware throughout their network.

Engage with Business Groups, Governance, and DevOps Early

Most cloud projects are driven by business groups and managed by DevOps teams. Quickly spinning up new products or functional prototypes is commonplace and can happen with only a few hours' notice.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

In all too many scenarios, the security team is brought in to review the architecture *after* the workload is already running in the cloud. By including security and governance earlier in the process, business and architecture decisions can be made with a security-first approach. This greatly reduces the burden of maintaining a secure environment and achieving compliance when required.

Know Your Potential Exposure

Public cloud usage is prolific due to the ease of spinning up compute and storage resources. Employees doing what's "right for the business right now" versus what's "right for the business" may create security holes if the environment isn't configured properly. It's imperative to know who in your organization is using the cloud and ensure the environment is configured correctly.

To reduce cloud risk, do the following:

- **Monitor cloud usage.** Perhaps the quickest way to determine usage is to look at how much your organization is spending on AWS, GCP, and/or Microsoft Azure.
- **Ensure proper configuration.** Configure the environment with security best practices in mind. Establish secure defaults for identity and resource access, enable all audit and security logging capabilities, and properly segment workloads into dedicated environments. This gives you a secure baseline from which to implement workload-specific configurations.
- **Require multifactor authentication (MFA).** To minimize the risk of an attacker gaining access using stolen credentials, MFA should be required. Using intelligent challenge-response mechanisms can also protect apps in the cloud from unauthorized access.
- **Lock down administrative interfaces.** For example, Secure Shell (SSH) on port 22 is a preferred method for securely managing cloud servers, yet it's often left exposed in AWS, GCP, and Microsoft Azure environments for convenience. Other administrative ports — including those for container management systems, application admin consoles, and other similar interfaces — should be strictly controlled and protected.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Understand the Attacker

Attackers leverage automation to find potential targets within minutes. After they've identified those targets, they look for weaknesses, checking default passwords, probing for SSH misconfigurations, and so on. To highlight the effects of attackers' automation capabilities, Palo Alto Networks spun up a test environment with a database and a web server in the public cloud to demonstrate the extent of attackers' capabilities. The environment was probed from more than 35 countries with more than 25 different attacker applications. In Palo Alto Networks' research efforts, a full global scan of all AWS, GCP, and Azure servers took 23 minutes to complete and revealed tens of thousands of exposed systems. Unlike in a private data center, where there is less concern about public exposure, resources in the public cloud are widely exposed and should be handled carefully.

Evaluate Your Security and Compliance Options

There are several security options to choose from when moving to the cloud, most of which are like the options for physical networks, including the following:

- **Native security services:** Cloud service providers offer native security services, including security groups, web application firewalls (WAFs), configuration monitoring, and many more. These tools are a good starting point for those without added security technologies but should be supplemented with enterprise-grade security offerings. The following two examples highlight the need for third-party security tools:
  - Security groups and port-based firewalls are essentially port-based access control lists, providing filtering capabilities. They can't identify applications by content, and you won't be able to prevent threats or, more important, stop outbound data exfiltration like a next-generation firewall can.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- WAFs are limited because they can only protect Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) applications. This means that WAFs can't protect applications that may use a wide range of ports to function properly. Plus, they aren't an effective means of identifying and controlling remote management or access tools, such as SSH or Microsoft Remote Desktop Protocol (RDP).

- **Point products:** Organizations that deploy point products that are designed to solve a particular use case end up deploying numerous products from different security vendors. This creates complexity with a fragmented set of security tools that don't seamlessly integrate and communicate with each other, and require specialized skills to operate and manage. Automation becomes difficult, if not impossible, to achieve.

- **Do-it-yourself (DIY) security:** Some organizations choose a DIY approach to securing cloud workloads, using custom scripts and open-source projects to protect deployments. Disadvantages to this strategy include the burden of improving and deploying custom tools, lack of expertise to manage the security implementation and operations, and nonexistent support in the event of a security breach.

  
  WARNING

  Organizations that rely on internal personnel to manage cloud and security deployments must be prepared for attrition. Typically, only a few engineers know the environment well, but they don't necessarily have time to keep proper documentation or manage knowledge-sharing requirements.

- **Security platforms:** The goal for many organizations is to eliminate a fragmented security approach where the security tools don't communicate with each other to successfully prevent attacks. To overcome this challenge, organizations typically adopt a security strategy that utilizes a platform approach. This approach delivers security through in-line, application programming interface (API)–based and host-based protection technologies working together to minimize attack opportunities:

  - Secure in-line traffic to implement inbound and outbound protections, segmentation of workloads, and threat prevention capabilities.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Monitor and protect public cloud resources via cloud provider APIs. These resources need to be monitored continuously rather than through point-in-time checks.
- Maintain the integrity of the operating system and applications on the virtual workloads blocking exploits, ransomware, malware, and fileless attacks.

Empower Yourself with Knowledge

Personal branding consultant John Antonios once said, "Knowledge plus action is power." In cloud security, knowledge begins with ingesting large sets of data produced by the cloud, network, and endpoints. Action involves analyzing the data to find the threats that need to be acted on to protect your cloud.

Security tools must be able to share this threat information with other parts of the cloud, points of enforcement, and the broader enterprise-wide IT deployment. Then, to help fight large-scale attacks and ensure future detection of similar attacks, the organization should share this information with the broader community and security industry. Attackers must then develop new tools, acquire new infrastructure, or develop different attack techniques from the ones already exposed. These changes require time, money, and other resources, which increase the cost to conduct the attack. As you build your cloud security strategy for your environment, ensure that your security tools are capable of sharing threat intelligence across your broader enterprise and receiving threat data from external sources.

To fast-track secure cloud adoption, consult cloud security experts through communities or vendors. The guidance will ensure you build the right security foundation to enable your business in the cloud.

Believe in Prevention

Some people believe the attackers have already "won," so they choose to focus primarily on a detection and remediation approach. However, if you're constantly reacting, you're always going to

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

be a step behind. Adopting a prevention philosophy is critical to dealing proactively with threats. Strong prevention minimizes the number of events that require detection and response, enabling you to rapidly stop sophisticated attacks before the attackers can steal confidential data. Preventing successful cyberattacks in the cloud requires four key capabilities:

- **Provide complete visibility.** The combination of knowledge and enforcement is a powerful security tool. It's critical to identify all your cloud resources, ongoing cloud activity, relative risk tied to current security measures, and any changes to your environment. With this knowledge, you can deploy a more consistent security policy globally to protect your cloud from known and unknown attacks.

  
  TIP

  Legacy security tools and techniques designed for traditional data centers must evolve to be relevant in the cloud. For a complete perspective, ensure that your security tools give you full visibility into Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) resources.

- **Reduce opportunities for attack.** Using a Zero Trust ("never trust, always verify") security approach and application identity as a means of enforcing a positive security model reduces the opportunity for attack by enabling only allowed applications and denying everything else. You can align application usage to business needs, control application functions, and stop threats from gaining access and moving laterally within your cloud and network infrastructure.
- **Prevent known threats.** Leveraging globally shared threat intelligence to apply threat prevention policies is a key step in adhering to a prevention philosophy. These threat prevention policies can block known threats, including vulnerability exploits, malware, and malware-generated command-and-control traffic.
- **Prevent unknown threats.** Unknown and potentially malicious files must be analyzed based on hundreds of behaviors. If a system determines that a file is malicious, it deploys a prevention mechanism quickly and automatically. The organization can then use the information it gains from file analysis to continually improve all other prevention capabilities.

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Secure IaaS and PaaS

Development teams and cloud administrators are responsible for ensuring that their data and applications are secure, as defined in the shared responsibility model. Here are some specific critical steps you should take to ensure that you're doing your part:

- **Disable root account API access keys.** A *root user* is the login credential you used to create your cloud account. Best practices recommend that the root user is used only to create your initial administrative accounts. You should then complete all future administration through newly created identity and access management (IAM) accounts.
- **Enable multifactor authentication (MFA) tokens everywhere.** MFA should be required of all users, both inside and outside your organization.
- **Follow the principle of least privilege.** Computer scientist Jerry Saltzer described it best: "Every program and every user of the system should operate using the least set of privileges necessary to complete the job."
- **Reduce the number of users with admin rights.** The more granular you are with access to your cloud accounts, the more you help protect your business if and when something is compromised.
- **Rotate all keys regularly.** Credentials, passwords, and API access keys should all be rotated on a regular basis. If a credential is compromised, this limits the amount of time that a key is valid.
- **Don't allow 0.0.0.0/0 unless you mean it.** Allowing traffic from 0.0.0.0/0 means that every machine, everywhere can make a connection to your cloud resources — and it also means that your systems can make outbound connections to every system everywhere. Instead, use security groups and network access control lists to limit both inbound and outbound traffic.
- **Turn on logging everywhere.** Too often, activity logging in cloud environments is turned off or never turned on. Without logs, how will you ever know if your environment has been breached?

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

From the perspective of the software developer, when writing the code of an application, ensure that there are enough relevant and clear logging routines to further isolate application errors, potentially exposing security risks, while running in production.

- **Turn on encryption.** Make sure your data is encrypted from the start. It's much more challenging to go back and sort through data to try to re-encrypt it after the fact. Much like enabling the service itself, encryption will help keep your data secure.

Use Automation to Eliminate Bottlenecks

Automation is a central tenet of the public cloud, where rapid change is constant. When an organization follows its security best practice change control policies, the delay in allowing that process to unfold may introduce friction, slowing deployments or, worse, weakening security if the deployment doesn't "wait" for change control to work.

Here are two automation tool sets that can help organizations eliminate security-induced friction and take advantage of the flexibility and agility benefits offered in the public cloud:

- Automated deployment systems and orchestration frameworks that enable security infrastructure to be deployed "as code" in a seamless and touchless manner
- Automation tools that use continuous monitoring, data analytics, and enforcement to respond more quickly to the ever-changing threat landscape

These materials are © 2023 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

WILEY END USER LICENSE AGREEMENT

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