

LEARNING MADE EASY

Palo Alto Networks 3rd Special Edition

Cloud Security & Compliance

for
dummies[®]
A Wiley Brand



Focus on the
threats that matter

—
Secure by
design

—
Automate real-time
defense

Brought to you
by:

 **CORTEX[®] CLOUD**
BY PALO ALTO NETWORKS

Dan Sullivan

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations, and AI, enhanced by the expertise and threat intelligence of Unit 42. Our focus on platformization allows enterprises to streamline security at scale, ensuring that protection fuels innovation. Discover more at www.paloaltonetworks.com.

About Cortex

Cortex Cloud, the next generation of Prisma Cloud, merges best-in-class CDR with industry-leading Cloud Native Application Protection Platform (CNAPP) for real-time cloud security. Harness the power of AI and automation to prioritize risks with runtime context, enable remediation at scale, and stop attacks as they occur. Bring together your cloud and security operations center (SOC) on the unified Cortex platform to transform end-to-end operations. Experience the future of real-time cloud security at www.paloaltonetworks.com/cortex/cloud.

Cloud Security & Compliance

**for
dummies**[®]
A Wiley Brand



Cloud Security & Compliance

Palo Alto Networks 3rd Special Edition

by Dan Sullivan

for
dummies[®]
A Wiley Brand

Cloud Security & Compliance For Dummies® , Palo Alto Networks 3rd Special Edition

Published by

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

Copyright © 2026 by John Wiley & Sons, Inc., Hoboken, New Jersey. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

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

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

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

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

ISBN 978-1-394-35659-1 (pbk); ISBN 978-1-394-35660-7 (ebk); ISBN 978-1-394-35661-4 (ebk)

Publisher's Acknowledgments

Editor: Elizabeth Kuball

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager:
Cynthia Tweed

Content Refinement Specialist:
Bharaneedharan Murthy

Special Help: Emily Rodenhuis,
Dena De Angelo, and
Mohit Bhasin

Table of Contents

INTRODUCTION	1
About This Book	2
Foolish Assumptions.....	2
Icons Used in This Book.....	3
Beyond the Book.....	3
CHAPTER 1: Unpacking the Modern Cloud	5
Understanding the Cloud	5
Getting to Know Cloud-Native Applications.....	6
What makes cloud-native apps so special	6
Containers, Kubernetes, and serverless — oh my!.....	7
It's not just what you build — it's how you build it	8
Seeing the Impact of AI.....	8
AI needs a lot of muscle	9
AI is fueling even more cloud adoption	9
A perfect match.....	10
CHAPTER 2: Securing the Cloud.....	11
Addressing Cloud Security	11
Understanding the Shared Responsibility Model.....	13
Recognizing that different types of clouds bring different kinds of responsibility	13
Attacking using tried-and-true methods.....	15
Identifying emerging AI attack vectors.....	16
Implementing Security from Code to Cloud to Security Operations	16
Using AI to Eliminate Security Risks	19
CHAPTER 3: Defining Core Security Controls	23
Securing Clouds.....	24
Cloud security posture management.....	24
Cloud workload protection platform.....	24
Cloud infrastructure entitlement management.....	25
Data security posture management.....	26

	Artificial intelligence security posture management.....	26
	Attack surface management	27
	Implementing Security from Code to Cloud to Operations with Cloud-Native Application Protection Platforms	27
CHAPTER 4:	Digging Deeper into CNAPP: The Platform Approach to Cloud Security	31
	Understanding the Risks of Siloed Tools	31
	Defining the Cloud-Native Application Protection Platform	32
	Seeing Why the Platform Approach Matters	34
CHAPTER 5:	Looking at Regulatory Compliance in the Cloud	35
	Navigating the Regulatory Landscape	35
	General Data Protection Regulation.....	36
	Network and Information Security Directive.....	39
	Recognizing the Importance of Automated, Continuous Monitoring.....	39
	Avoiding the “Compliance Catchup” Trap	41
	Implementing a Proactive Approach with DevSecOps	42
	Four Ways to Improve Cloud Security and Compliance	43
CHAPTER 6:	Building an Organizational Culture around Security	47
	Managing Cybersecurity in the Modern Era	47
	Creating an effective cybersecurity team	48
	Planning your automation strategy.....	48
	Assessing security effectiveness	49
	Recognizing How Cloud Maturity Affects Automation Levels	50
	Embedding Security in the Developer Workflow.....	50
	Continuous cybersecurity skills training and enhancement	51
	Security from design through production	52
	Executive leadership.....	52
	Automation.....	52
	Cultivating the collaborative mindset.....	52
	Security accountability	53
CHAPTER 7:	Ten Cloud Security Recommendations.....	55
	Understand the Shared Security Model	55
	Involve Cross-Functional Teams.....	56

Take a Cloud-Centric Approach	56
Unify Data.....	57
Implement a Context-First Mindset	57
Use Automation to Eliminate Bottlenecks	57
Know Your Potential Exposure	58
Minimize Access Permissions	59
Prepare for Incident Response	59
Evaluate Your Security and Compliance Options.....	59
GLOSSARY	61

Introduction

Welcome to your easy-to-understand guide to cloud security and compliance! As more organizations move their data and applications to the cloud, protecting these valuable assets has never been more important — or more complex. The cloud offers incredible flexibility and power, but it also introduces new risks and responsibilities that can feel overwhelming.

This book is designed to help you cut through the jargon and confusion. Whether you're a business leader, IT professional, developer, or just curious about cloud security, you find straightforward explanations and practical advice to help you understand how to keep your cloud environments safe and compliant with regulations.

You learn about the modern cloud landscape — what cloud-native applications are, how artificial intelligence (AI) is changing the game, and why security in the cloud is different from traditional IT. I walk you through key security concepts like identity management, data protection, and threat detection, and introduce you to powerful tools and frameworks like cloud-native application protection platforms (CNAPPs), cloud infrastructure entitlement management (CIEM), and more.

Compliance is a big part of cloud security, so I also cover important regulations like the General Data Protection Regulation (GDPR) and Network and Information Systems (NIS) Directive, along with how to build a proactive, automated approach to meet them without falling behind.

Finally, I explore how to build a culture of security within your organization, empowering your teams and leaders to work together effectively.

After reading this book, you'll have a solid foundation to confidently navigate the cloud security landscape — helping your organization protect its most valuable digital assets in today's fast-changing world.

About This Book

Cloud Security & Compliance For Dummies, Palo Alto Networks 3rd Special Edition, consists of seven chapters that explore the following:

- » The evolution of cloud and cloud-native applications, as well as the impact of AI (Chapter 1)
- » How to secure the cloud and cloud-native applications in your organization (Chapter 2)
- » Foundational cloud security controls (Chapter 3)
- » CNAPP (Chapter 4)
- » The regulatory landscape in the cloud (Chapter 5)
- » How to build an effective cybersecurity team and leverage automation in the cloud (Chapter 6)
- » Best-practice recommendations for securing the cloud (Chapter 7)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you. There's also a convenient glossary in case you need to brush up on any acronyms or tech lingo!

Foolish Assumptions

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

- » You're a 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.

Icons Used in This Book

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



REMEMBER

This icon points out information that you should commit to your nonvolatile memory, your gray matter, or your noggin.



TECHNICAL
STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.



TIP

Tips are appreciated, but never expected — and I sure hope you'll appreciate these useful nuggets of information.



WARNING

These alerts point out the stuff your mother warned you about. (Okay, probably not, but they do offer practical advice.)

Beyond the Book

There's only so much I 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/cortex/cloud/cloud-security-posture-management.

IN THIS CHAPTER

- » Understanding the rise of modern cloud computing
- » Exploring cloud-native apps, containers, and DevOps practices
- » Seeing how AI is shaping cloud adoption and development

Chapter **1**

Unpacking the Modern Cloud

Welcome to the cloud! No, not the fluffy kind in the sky (although it's just as vast and sometimes just as confusing). I'm talking about the cloud that powers your favorite apps, stores your cat photos, and helps companies run at warp speed. In this chapter, I break down how the cloud has transformed the way organizations build and run applications., what makes cloud-native applications different from traditional software, how technologies like containers and Kubernetes support rapid development, and why modern teams rely on DevOps and open source. I also examine how artificial intelligence (AI) is not only powered by the cloud, but also accelerating cloud adoption across industries.

Understanding the Cloud

Imagine if instead of buying, maintaining, and babysitting a bunch of clunky hardware, you could just rent someone else's supercomputers by the minute. That's the basic idea behind cloud

computing. Companies no longer have to own the tech behind their tech — they just plug into the cloud and go.



REMEMBER

If you speak accounting, this means you're shifting from capital expenditures to operational expenditures.

Cloud computing lets businesses store data, run apps, and scale operations without having to build it all themselves. The cloud is kind of like Netflix for IT: Pay as you go, access it from anywhere, and skip all the setup pain.

Why is everyone moving to the cloud? The short answer: speed, scale, and savings.

- » **Speed:** Developers can spin up environments in minutes instead of weeks.
- » **Scale:** Companies can grow (or shrink) their infrastructure on demand.
- » **Savings:** No need to buy and maintain massive server rooms anymore. Plus, you only pay for what you use.

It's no surprise that cloud adoption is booming. Nearly every industry — from healthcare to finance to fast food — is putting more of its IT footprint in the cloud.

Getting to Know Cloud-Native Applications

Now that we're floating in the cloud, let's talk about what lives there.

Cloud-native applications are built specifically for the cloud. They aren't old-school programs retrofitted to work online — they're designed from the ground up to thrive in a cloud environment. Think of them as digital nomads: flexible, fast-moving, and always ready to adapt.

What makes cloud-native apps so special

Cloud-native apps are built to embrace change. They often use *microservices* (small, independent components that work together).



TECHNICAL
STUFF

Developers can update one piece without breaking the entire app, which makes it easier to move fast and stay agile.

The shift to microservices is a boon to security. It makes patching a more streamlined process.

They're also highly automated. Cloud-native systems can heal themselves when something goes wrong, update without downtime, and deploy new features at the push of a button.

Scaling is built in. Whether you're serving 10 users or 10,000, these apps can expand or shrink automatically based on demand.

And thanks to containers, they're portable. A container packages everything the software needs to run, so it behaves the same no matter where it's deployed — from a laptop to a massive cloud data center.

According to Cloud Native Computing Foundation (CNCF), 80 percent of organizations use Kubernetes in production (see www.cncf.io/announcements/2025/04/01/cncf-research-reveals-how-cloud-native-technology-is-reshaping-global-business-and-innovation/). That's proof that cloud-native is more than a buzzword — it's how modern software gets built.

Containers, Kubernetes, and serverless — oh my!

Many cloud-native apps rely on *containers*, which are lightweight environments that bundle code, configurations, and dependencies into one neat little package. Containers make sure your app runs the same in development, testing, and production.

As systems grow, containers are managed by Kubernetes. This powerful orchestration platform automates deployments, scales workloads, and handles failures behind the scenes — so teams can focus on innovation, not infrastructure.

Some teams go even further with serverless computing. With serverless, there's no need to manage or provision servers at all. You just write the code, and the cloud runs it when triggered. You only pay for what you use, which makes it cost-effective and low-maintenance.



TECHNICAL
STUFF

Serverless functions are especially useful for building event-based workflows.

These technologies help teams release updates faster, build more resilient apps, and spend less time worrying about what's under the hood.

It's not just what you build — it's how you build it

Cloud-native also represents a cultural shift in how software gets developed. DevOps practices bring developers and operations teams together so they can collaborate more efficiently across the entire lifecycle — from writing code to maintaining live apps.

Continuous integration/continuous delivery (CI/CD) is another cornerstone. Instead of big, risky releases, developers push small, frequent updates that are automatically tested and deployed. This leads to fewer bugs, faster feedback, and a better experience for users.

And most cloud-native teams don't build everything from scratch. They use open-source libraries and third-party application programming interfaces (APIs) to get up and running quickly. It's like starting with a half-built LEGO set instead of an empty table.

Fun fact: Sixty percent of organizations are leveraging CI/CD for most or all applications, according to CNCF (www.cncf.io/announcements/2025/4/01/cncf-research-reveals-how-cloud-native-technology-is-reshaping-global-business-and-innovation).

Together, these tools and practices make cloud-native development ideal for companies that need to move quickly, adapt constantly, and compete in fast-moving markets.

Seeing the Impact of AI

You've probably heard the buzz: AI is taking over (in a good way . . . we hope). But what does that have to do with the cloud?

Well, everything, really.

AI needs a lot of muscle

Training and running AI models requires serious computing horsepower and enormous amounts of data. That's a tall order for even the most well-equipped on-premises data center. Enter the cloud.

Cloud platforms offer high-performance infrastructure that's tailor-made for AI workloads — think graphics processing unit (GPU)-accelerated servers, petabyte-scale storage, and ready-to-go machine learning (ML) frameworks. Companies don't need to invest in racks of hardware or specialized teams to manage it. Instead, they can spin up AI environments on demand and only pay for what they use.

It's no surprise that businesses are running their AI models in the cloud by default. From fraud detection to content moderation to medical image analysis, cloud-powered AI makes it possible to process and act on massive datasets in real time.

Did you know that more than 90 percent of organizations use AI-assisted coding in application development, according to Palo Alto Networks (www.paloaltonetworks.com/resources/research/state-of-cloud-native-security-2024).

AI is fueling even more cloud adoption

But the relationship isn't one-way. AI is also *driving* cloud adoption. As more organizations adopt AI, they're moving workloads to the cloud to take advantage of its speed, scalability, and cost-efficiency.

And it's not just about running AI models — it's also about using AI to *build* the next generation of apps.

Developers today are increasingly using AI-powered tools to write code, generate documentation, and troubleshoot issues. Some even call it “vibe coding” — where developers guide the AI with natural language and let it handle the heavy lifting. Whether you're debugging JavaScript or prototyping in Python, AI assistants are becoming a daily part of the development workflow.

This new way of building software pairs perfectly with the cloud. Need to test your AI-generated code in a real environment? Just spin up a container or serverless function. Want to deploy it globally? One click, and it's running in five regions at once.

A perfect match

As AI continues to evolve, it's becoming tightly woven into every part of the cloud journey — from development to deployment to operations. And the more businesses rely on AI, the more they lean on the cloud to make it possible.

Bottom line: AI isn't just using the cloud — it's shaping the future of how the cloud is used.

IN THIS CHAPTER

- » Recognizing the challenges of cloud security
- » Getting to know the shared responsibility model
- » Exploring real-world cloud threats
- » Implementing end-to-end security from code to cloud to SOC
- » Leveraging AI in cloud security

Chapter 2

Securing the Cloud

So, you want to move applications and services to the cloud and you're ready to get started. That's a great position to be in, but before you get too far ahead of your skis, take a minute to think about security. In the cloud, you share responsibility for security with your cloud providers.

This chapter explores common cloud security challenges in the cloud, the shared responsibility model for security, and real-world cloud threats. It also examines a new approach to cloud security and the impact of artificial intelligence (AI) in cloud security.

Addressing Cloud Security

Let's start at the beginning. Cloud security is the set of principles and practices you employ to protect your assets within a cloud environment. And there are a *lot* of assets to protect. You need to ensure that your data that's stored and processed in the cloud remains confidential, available, and not tampered with. You also need to protect users whose accounts could be misused by malicious actors and to protect your infrastructure assets like virtual machines (VMs), containers, databases, and machine learning (ML) models that you have running in the cloud.

Cloud security requires a broad, holistic approach to ensure you can effectively protect the wide range of assets in cloud environments.

Here are some of the common security challenges you face in the cloud:

- » **Limited visibility:** The cloud is a complex environment. That makes it hard to completely monitor all the important stuff going on in your infrastructure, which can create blind spots where security risks can fester.
- » **Diverse threats:** Malicious actors have a knack for finding creative attack paths and workarounds to security solutions seemingly as fast as they're created.
- » **Difficulty consistently enforcing policies:** Enterprises often use multiple cloud providers and may have *private clouds* (that is, their own clouds they run in house). If this is how your organization operates, you're probably going to have to deal with a variety of security tools. This can make it difficult to centralize security policies and apply them consistently.
- » **Potential for misconfigurations:** To err is human, and humans certainly do have a knack for erring when it comes to configurations. Insecure storage configurations, excessive permissions, improper access controls, and poorly secured application programming interface (API) endpoints are just some of the ways you leave your cloud assets vulnerable to malicious activity.

Speed and agility are attributes of cloud-native application practices, but no matter what your architecture or development methodology, you have to follow secure practices. Without the right tools and procedures, compliance and security controls can be a drag on continuous integration/continuous delivery (CI/CD) pipelines.

One of the advantages of cloud-native architectures is that they allow you to take advantage of existing components and tools instead of requiring you to build every digital component from scratch. The downside of this advantage is that although open-source tools and other libraries can save you development time, they can be a source of vulnerabilities. Unpatched vulnerabilities

in open-source software can increase the fragility of your software supply chain.

Understanding the Shared Responsibility Model

A not-so-well-known thing about “the cloud” is that there is no one kind of cloud. There are public clouds that are created by businesses that make the cloud resources available to anyone — think: Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and more. On the other hand, there are private clouds that are limited to use by those who build and maintain those clouds. Add to the mix hybrid clouds, which combine the features of public and private clouds. Now you have a sense of the variety pack of cloud types you may be dealing with.

Recognizing that different types of clouds bring different kinds of responsibility

As any superhero will tell you, with great power comes great responsibility. This idea applies to clouds as well, but you are not alone in shouldering that responsibility.

Clouds come in different shapes and sizes:

- » **Infrastructure as a service (IaaS):** This is the DIY version of clouds. You get access to VMs, containers, bare-metal servers, and other core infrastructure components.
- » **Platform as a service (PaaS):** In this version, providers manage the infrastructure for you, so you don't have to. PaaS customers get access to a software platform for building services while leaving the infrastructure management to someone else.
- » **Software as a service (SaaS):** In this version, cloud providers offer fully functional applications and services without the need for their customers to have to manage infrastructure or think about deploying applications.

With so many ways of configuring cloud services, how are you supposed to know who's responsible for protecting what?

When you think about shared responsibility for security, it may bring to mind a number of different groups within your organization — including the network team, security team, apps team, and compliance team. Each of these teams is definitely part of the picture, but cloud security is also a shared responsibility between the cloud vendor and your organization.

Consider an organization that has deployed cloud platforms internally for its own use. The organization is responsible for all aspects of security for its private cloud because the cloud is hosted within its own data centers. The organization is responsible for protecting the physical network; securing infrastructure components such as hypervisors, virtual networks, operating systems, and firewalls; as well as service configurations, identity and access management (IAM), and data protection services. With private clouds, you're in a "you own it all" mode of operation.

Public clouds providing IaaS — like AWS, GCP, and Microsoft Azure — require a different approach to cloud security. In these clouds, you share responsibility for security with the cloud vendor. The cloud vendor is responsible for protecting the physical infrastructure of the cloud, such as data centers, racks of servers, and physical network and storage devices. This is good, because you as a cloud customer have no control over these things. Your organization takes responsibility for defining and implementing security controls to protect its workloads, applications, data, and user identities.

When you use a SaaS version, you get a lot of help with security. The SaaS vendors take care of the security of their platform, which includes physical security, infrastructure, and application security. Now, these vendors don't own your data, so you're still responsible for protecting your customer data.

As companies make more use of public cloud or SaaS applications, the operational burden for securing the underlying infrastructure components and managing platform services shifts to the vendor (see Figure 2-1). Regardless of the platform used, the enterprise will always be responsible for ensuring the security and privacy of its own data.

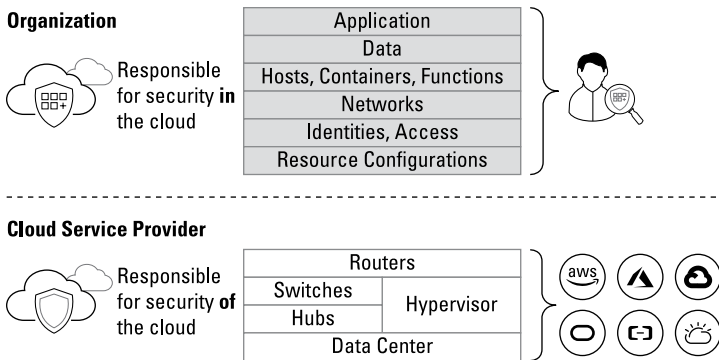


FIGURE 2-1: Cloud security is a shared responsibility.



Your data is your responsibility.

If you want to keep your applications and data secure (and you do), you must clearly understand where your cloud vendors' security responsibilities end and where yours begin. And by the way, you also need to have the right tools.

Ideally, your organization's security teams will have tools that keep them informed about activity within the cloud application, details on who is using which resources, as well as help detecting and preventing data loss and compliance violations. You also need context-aware policy controls that help enforce and address security issues when they occur. You'll also want real-time threat intelligence so you can prevent attackers from exploiting them.

Attacking using tried-and-true methods

If it ain't broke, don't fix it as the saying goes. Malicious attackers embrace this kind of thinking when they use a variety of well-known attack types. These are attacks that target user identities and the roles and privileges users have; they include trying to get information about infrastructure from cloud instance metadata APIs, which most cloud service providers support and have details about your VMs. Other identity and access attack paths include exploiting improperly secured credentials (for example, usernames and passwords stored in a file or on a sticky note).

Malicious actors may go after sensitive data in online data services such as Amazon Simple Storage Service (S3) and Azure Storage, as well as SaaS platforms like Microsoft 365 and Google Workspace.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Sensitive data may be stolen from the cloud by sharing or syncing the data with another cloud account controlled by the attacker or by creating a backup of the cloud environment. Bad guys can also turn to destroying data in attacks.

Identifying emerging AI attack vectors

Just when the security team in your organization thought it had enough to deal with, along comes AI, bringing with it new attack vectors. These include the disclosure of sensitive information, such as personally identifiable information (PII) that may be exposed in large language models (LLMs). Malicious actors can manipulate prompts to alter the behavior or output of an LLM, potentially causing the model to generate harmful content or allow unauthorized access, among other negative outcomes.

Here are some other examples of attacks against AI:

- » **Data poisoning:** An attacker injects carefully crafted samples into training data, causing an AI model to learn biased or malicious patterns.
- » **Adversarial attacks:** Subtle disturbances to the input data misleads the AI system into making incorrect predictions or decisions, potentially with severe consequences.
- » **Model extraction:** A threat actor attempts to steal an organization's proprietary AI model through unauthorized access or by probing the model's outputs to reconstruct its internal parameters.

In the Age of AI, you have to contend with both long-understood attack methods and new types of AI-specific attacks that are emerging along with the adoption of AI.

Implementing Security from Code to Cloud to Security Operations

Your security teams are facing increasing complexity as they defend your cloud resources from advanced cloud-based threats. Too often organizational silos divide application security (AppSec), cloud security (CloudSec), and security operations (SecOps) teams. In many cases, each of these groups works with separate tools,

workflows, and data sources. This situation can lead to barriers between them, which hinders cross-team collaboration. That, in turn, can delay incident response.

Consider an example of how this may happen: Imagine a CloudSec team detects a vulnerability in cloud infrastructure. They know something is up but lack the runtime context to determine exactly how the attack is proceeding. This can happen when SecOps analyst may be monitoring alerts without visibility into the cloud services and applications they're protecting. Meanwhile, AppSec teams are trying to protect the enterprise's cloud-native applications but lack observability into those applications, so they remain disconnected from risks that can materialize in production.

In such environments, attackers can move between cloud infrastructure, enterprise systems, and application layers without much concern for anyone having a complete picture of their activity. Now consider that 80 percent of medium, high, and critical exposures occur in cloud environments, and you'll see why manual workflows and disconnected security tools are liabilities to modern enterprises using cloud resources.

Throwing more siloed tools at these security issues is not going to solve the picture problem of security. Instead, you must rethink security and break down longstanding barriers between application development, cloud security, and operations.

Organizations need a new approach to security that breaks down artificial barriers and delivers comprehensive security from code to cloud to security operations center (SOC), as shown in Figure 2-2.

Forget silos, you want to unify data, automate workflows, and leverage AI-driven insights in a consolidated, integrated platform. Think teams that can share information, identify misconfigurations, identify real attack patterns, and automate responses across cloud and traditional infrastructure. Now that's how you deal with today's cloud security threats.

In order to address modern security challenges in the cloud, enterprises need to optimize security processes across multiple areas.

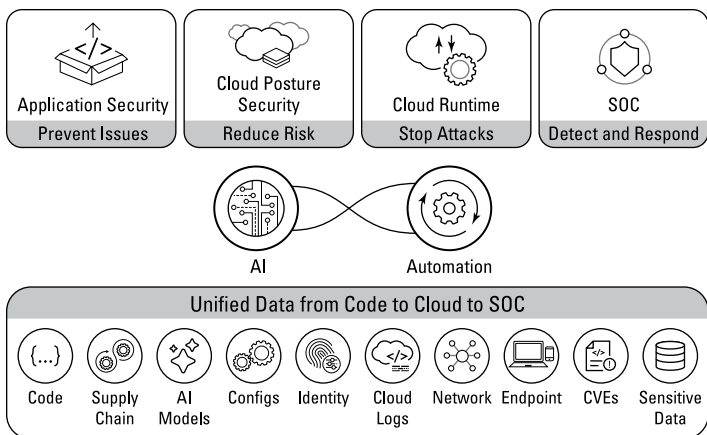


FIGURE 2-2: Full-context security from code to cloud to SOC.

With regards to application security, you need to:

- » Strengthen contextual awareness of vulnerabilities as they progress from development to runtime.
- » Improve cross-team visibility by integrating application security insights with runtime data for more accurate prioritization.
- » Enhance guardrails to adapt dynamically to evolving threat patterns during development.

For posture management, it is important to:

- » Deepen integration of posture management tools with runtime threat indicators to better prioritize risks.
- » Address gaps in misconfiguration remediation workflows to prevent operational delays.
- » Strengthen the connection between posture enforcement and real-time threat visibility.

And just as important, you need to consider how you protect runtime security with the ability to:

- » Improve detection capabilities by correlating runtime signals with upstream application and cloud data to uncover complex attack chains.

- » Bridge the gap between cloud runtime threat detection and automated, ecosystem-wide remediation.
- » Expand visibility into hybrid environments, capturing interactions between cloud-native resources and traditional infrastructure.



REMEMBER

Cloud-native applications are different from their legacy counterparts. They're built from the ground up to run in the cloud. Any next-generation security strategy needs to be holistic in scope and focused on *securing* 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 lifecycle. This includes creating secure code and a secure infrastructure for it to run on, across multiple clouds.

Using AI to Eliminate Security Risks

Many security threats begin with code vulnerabilities. Data, AI, and automation present an opportunity to transform how you respond to these threats. This is ideal because you want to shift from reactive defense practices to having a more proactive, adaptive protection operation.

An AI-driven security operations solution helps improve your security game. By collecting and analyzing data across code, cloud, and security operations, AI can help you identify attack paths, prioritize critical risks, and recommend precise remediation actions.

When an incident occurs, you want to move fast. AI can correlate signals across the environment to show the complete attack story — from initial code vulnerability through cloud exploitation to broader impact. More important, AI can predict potential attack paths before attackers exploit them.

Instead of simply responding to incidents, organizations can prevent attacks, automatically identifying and fixing their most critical vulnerabilities.

AI can continuously learn from each incident, and improve its ability to predict and prevent attacks. It's also ideal for automating routine security workflows across cloud and security operations. This represents just one of the transformative capabilities that only a unified, AI-driven approach can deliver.

IRON MOUNTAIN SHIFTS LEFT WITH CNAPP

Iron Mountain is the global leader in storage and information management services. Trusted by 225,000+ organizations and 90 percent of the Fortune 1000, Iron Mountain stores and protects billions of valued assets, including critical business information, highly sensitive data, and cultural/historical artifacts.

As the company set out to develop Iron Mountain InSight DXP — a cloud-native application that uses AI to classify, extract, and enrich both digital and physical content — its InfoSec team sought to resolve multi-console complexity with a single solution for visibility across its entire cloud surface.

Challenge

- **Gain visibility** into the cloud-native InSight DXP application (and all cloud-native workloads) in AWS, GCP, Microsoft Azure, and beyond.
- **Maintain the highest level of security** in a complex and evolving multicloud environment with a lean InfoSec team.
- **Ensure compliance** with a range of cybersecurity frameworks and government regulations around the globe.

Solution

When Iron Mountain set out to build Iron Mountain InSight DXP, it needed an upgrade from its cloud service providers' native security tools. "With all three major clouds and six or seven tools, whenever there was an issue, it was a pain to try to figure out which cloud or vendor it was," explains Information Security Officer David Williams. More tools resulted in more complexity, redundancy, confusion, and labor.

Already a Palo Alto Networks client, Iron Mountain selected Palo Alto Networks Cloud Security Solution to resolve its multi-console problems.

Seeing everything, down to the grain

According to Williams, the solution “made InSight DXP possible.” Support for workloads across AWS, GCP, and Azure streamlined the security team’s operations with end-to-end visibility into Iron Mountain’s security and compliance posture. Specifically, Iron Mountain can now see which particular policy or rule is being violated from a compliance standpoint, as well as where that violation falls in terms of impact or remediation priority.

Consolidation changes the game

Before Palo Alto Networks Cloud Security Solution, closing security gaps required a series of time-consuming and duplicative tasks. Cloud security engineers and analysts would log in to each cloud, look up Common Vulnerabilities and Exposures (CVE) in the global CVE database, find the criticality levels, conduct remediation, and mark the task as finished. Now, everything can be viewed in one place.

Distilling alerts down to their essence

Iron Mountain was no stranger to alert overload, and with identical workloads across clouds, redundancy was a major pain point. Before Palo Alto Networks Cloud Security Solution, if there was an issue within Kubernetes in GCP, the same alert would signal in AWS and Azure Kubernetes, too. Then those three alerts would get multiplied by the number of Kubernetes instances — as many as 100 — resulting in 300 alerts for a single issue. Palo Alto’s CNAPP platform consolidates all 300 alerts into one, dramatically reducing the signal-to-noise ratio for Williams and his team.

Bringing security into the code

Another significant benefit of Palo Alto Networks Cloud Security Solution is its ability to empower DevOps with security capabilities, which has been transformative at a company with hundreds of developers and only a handful of InfoSec personnel. “I was able to turn our developers into junior security engineers because they’re

(continued)

(continued)

now policing our code in real time,” Williams reports. Misconfigurations are much easier to catch and fix, too, giving Iron Mountain the ability to be preemptive and proactive instead of reactive.

Baked-in support for global compliance

As a protector of cultural, historical, business, and government assets, Iron Mountain has to adhere to a wide variety of demanding regulations. To demonstrate compliance, Williams’s team can simply print a report from the CNAPP solution. “It will show all our highs, criticals, and lows and tell us if they’ve been remediated within the necessary time frame,” Williams explains. CVEs are also baked into Palo Alto Networks Cloud Security Solution. Additionally, as regulations evolve, Palo Alto Networks stays at the forefront of the changes. “When NIST SP 800-53 went from Rev. 4 to Rev. 5, it was right there in the solution,” Williams remembers.

Reporting that shows and tells

The reporting capabilities in Palo Alto Networks Cloud Security Solution — especially the one-click feature — are also responsible for big leaps in efficiency. Williams can pull from hundreds of out-of-the-box reports, customizing them to meet the needs of individual regulations or customers. When auditors want to observe the security tools in action, Williams does a live screen-share. “We show the green check marks and allow the auditor to take screenshots, showing exactly what we’re doing, how we’re doing it, and how efficient we are.”

Results

- **Thirty percent increase in efficiency** across cloud InfoSec operations
- **Two-hour reduction in time** to gather evidence for compliance audits
- **Seven cybersecurity tools** consolidated into one for a single, unified view

IN THIS CHAPTER

- » Addressing cloud misconfigurations
- » Ensuring cloud workload protection
- » Managing identities and access
- » Safeguarding sensitive data
- » Protecting AI systems

Chapter 3

Defining Core Security Controls

Modern cloud environments require modern security tools. Let's take a look at a set of services that together provide comprehensive controls for your cloud workloads. Get ready for a long list. Locking down cloud assets takes a village of tools, including:

- » Cloud security posture management (CSPM)
- » Cloud workload protection platforms (CWPPs)
- » Cloud infrastructure entitlement management (CIEM)
- » Data security posture management (DSPM)
- » Artificial intelligence security posture management (AI-SPM)
- » Attack surface management (ASM)
- » Cloud-native application protection platforms (CNAPPs)

This chapter isn't just a laundry list of tools. I also look at how you can implement security from cloud to code to security operations center (SOC).

Securing Clouds

When you think of cloud assets, some things probably come to mind right away: workloads, compute resources, configurations, identities, data stores, and other more specialized types of resources and components that make up your ensemble of assets. Just as a musical ensemble can include a variety of instruments, cloud security ensembles include different types of security tools that address different challenges and help you address particular types of attacks or vulnerabilities. In the following sections, I cover what your cloud security ensemble should include.

Cloud security posture management

CSPM tools and practices are designed to help you find and correct misconfigurations. CSPM gives you visibility into all your cloud resources and helps you keep them in compliance with your organization's policies. This is especially important when you're dealing with the rapid pace of change that is typical in enterprise cloud environments.

Small cloud misconfigurations can lead to big problems. Even things that seem inconsequential, like making an object storage bucket publicly accessible or giving a user or service account a few extra permissions, can enable significant breaches and data loss.

CSPM includes tools to discover assets in your cloud, deliver visibility into their configurations, monitor and alert about misconfigurations, and automatically remediate issues it finds.

Cloud workload protection platform

You need to protect the applications and services running in the cloud. Looking to a working environment analogy, CWPP is employed to help protect the people working in an office building while CSPM is intended to protect the office building itself.

A CWPP addresses several different kinds of issues, including the following:

- » The need to apply policies consistently across a variety of applications and service types

- »» The ephemeral nature of some workloads that can spin up and execute quickly and then terminate
- »» The need to monitor applications and their dependencies for vulnerabilities that can be exploited by attackers, resulting in data breaches and compromised systems
- »» The need to monitor and protect the runtime environment of workloads because executing applications are exposed to threats like malware and zero-day exploits

Perhaps the most important set of controls provided by a CWPP is the runtime protections that provide

- »» Allow lists that define legitimate processes, files, and network connections used by the workload
- »» Anomaly detection based on behavior analysis
- »» Memory protection and integrity checking to block exploits and malware
- »» File integrity monitoring to identify and alert on changes to critical system files

A CWPP also helps with detection and response activities. It gives you a combination of security benefits, ranging from reducing the attack surface of workloads to improving DevOps security practices and enabling greater visibility into the state of workloads.

Cloud infrastructure entitlement management

Managing which identities can access what cloud infrastructure is tricky because there are not just people, but also machines, apps, and services (also known as *nonhuman identities*). The majority of the time, identities have excessive permissions, opening the door for attackers to abuse compromised identities with privilege escalation and lateral movement to crown-jewel assets like sensitive data.

CIEM is a core cloud security control that addresses identity and access risks by:

- »» Giving organizations visibility into cloud identities and their permissions, easily identifying who has access to what cloud service

- » Learning the access behaviors of cloud identities to detect unused or excessive permissions that increase risk
- » Recommending new cloud entitlements based on the principle of least privilege

CIEM helps stop attack techniques like *privilege escalation* (where attackers gain higher access than they should) and *insider threats* (where someone misuses their permissions).

Data security posture management

If you want to protect your sensitive data, you need to know where that sensitive data is, who has access to it, how it's being used, and what access controls are in place for it.

DSPM systems are designed to help you discover, classify, and secure sensitive data in the cloud, whether it's in databases, data lakes, or object storage buckets.

DSPM systems are especially helpful when data is spread out across multiple data stores, including unmanaged or unknown repositories. These systems can also help identify incorrectly classified data or data that lacks sufficient access controls. By constantly monitoring different data stores in your cloud, DSPM can discover new data, verify that its classification and access controls are correct, and remediate issues that leave sensitive data exposed to leaks or tampering.

Artificial intelligence security posture management

Artificial intelligence (AI) is a rapidly emerging technology with a wide range of applications. Organizations are rolling out new services and capabilities based on AI along with other workloads.

Generative AI, including large language models (LLMs) and large reasoning models (LRMs), are complex systems with access to vast amounts of information. Their behaviors can be difficult to anticipate when exposed to unexpected inputs, which can lead to AI-specific types of attacks.

Predictive AI depends on a development pipeline that includes data collection and transformation, processing, training, validation, and deployment. Any of the stages of the pipeline could

be compromised to alter the behavior of machine learning (ML) models in unwanted and difficult-to-detect ways.

AI-SPM can help you build a comprehensive inventory of generative AI and ML assets, scan for bias in generative and predictive AI outputs, and test for susceptibility to attacks, such as prompt injection.

Attack surface management

Wouldn't it help to have a map of your cloud environment developed by a security cartographer who could show you the entire terrain of your cloud that is exposed to threats? That's what ASM platforms are designed for.

You can think of an attack surface as the set of all assets and endpoints that are exposed to would-be attackers. Like so much in the cloud, the attack surface is in constant flux as infrastructures, applications, and workloads change. ASM helps you with inventorying assets and identifying potential points of attack in vendor or business partner services.

ASM probes to discover assets within an enterprise's cloud and then looks for open ports, known vulnerabilities and other ways of exploiting weaknesses.

Implementing Security from Code to Cloud to Operations with Cloud-Native Application Protection Platforms

The previous section offers a significant list of tools and technologies needed to protect cloud assets. Each of these tools, by itself, is an important element of protecting enterprise cloud environments, but they're all fairly specialized in the type of protections they provide. CNAPPs can combine the capabilities of systems like CSPM and CWPP and avoid the problems that commonly plague siloed security tools.

CNAPPs help security teams address the problem of security tool sprawl. With too many tools, each generating its own reports and alerts, it's easy to get overwhelmed and miss critical information.

CNAPPs can help reduce reporting and alerting complexity and prioritize information so security teams can focus on the most important issues.

Consider how silos of security tools can work as expected and still miss crucial information: A CSPM can detect a misconfigured subnet in a virtual private cloud, and a CWPP in the same environment can spot a vulnerability in a workload, but neither of these tools is capable of recognizing the misconfigured network that exposes the workload vulnerability to attackers on the public internet. What's lacking is a comprehensive view of a cloud's exposure.

Now imagine if you had a tool that could build a comprehensive picture of security in your cloud with:

- » Scans of the cloud to find assets and misconfigurations, like those found with CSPMs
- » Details about workload vulnerabilities, unhardened configurations, and runtime exposures, like those detected by CWPPs
- » Information on users and service accounts with excessive privileges, such as found by CIEMs

Building on the consolidation of information by CNAPPs, you can realize even more benefits than if you relied on a collection of siloed security tools. CNAPPs enable you to reduce the complexity of security operations (as well as the costs of those operations) while improving your ability to identify and prioritize threats.

Another thing I need to point out about CNAPPs is that they operate across the lifecycle of cloud applications and services. For example, you can use the tools to scan code repositories and IaC templates for vulnerabilities and misconfigurations in the development phase. When you're building and deploying, you can use CNAPP capabilities to scan images for vulnerabilities and prevent the release of vulnerable application code. At runtime, CNAPP can help protect workloads, monitor configurations, and detect threats in real time.

Cloud environments are inherently complex, blending diverse elements like compute, networking, and IAM. This complexity, combined with the rapid, constant change from modern

development, hinders visibility into service interactions. The result is a proliferation of misconfigurations and vulnerabilities across the architecture, creating a greater risk surface.

Typically, the policies will map to an industry best practice framework. Examples include the Center for Internet Security (CIS) Benchmarks and MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). They may also map to regulatory compliance frameworks such as the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), or General Data Protection Regulation (GDPR).

IN THIS CHAPTER

- » Understanding the risks of siloed tools
- » Defining a CNAPP
- » Exploring the core capabilities of a CNAPP
- » Reviewing the key advantages of a platform approach

Chapter 4

Digging Deeper into CNAPP: The Platform Approach to Cloud Security

Imagine your cloud security program. You can use a collection of separate, specialist tools, or adopt a single, unified platform that keeps the essentials together. In cloud security, a cloud-native application protection platform (CNAPP) is that unified tool. In this chapter, I walk you through what a CNAPP is, why it matters, and what it can do for you.

Understanding the Risks of Siloed Tools

When tools don't share context, gaps appear — and that's where attackers move. Relying on a collection of siloed security tools creates dangerous blind spots. A posture management tool may spot a misconfigured network, while a workload protection tool flags a vulnerable application, but neither one can connect the

dots to see the immediate danger. Each tool gives you a single puzzle piece, leaving your team to guess what the final picture looks like.

This approach creates several significant problems:

- » **Lack of context:** An alert about an open network port is just noise. It becomes critical only when you know it connects to a workload with a known vulnerability and access to sensitive data.
- » **Alert fatigue:** When analysts are bombarded with thousands of low-priority alerts from a dozen different tools, the critical warnings get lost in the noise.
- » **Operational complexity:** Managing a mix of separate tools is a job in itself. Each system has its own dashboard and rules, leading to inconsistent policies and heavy management overhead.
- » **Slower incident response:** During an attack, analysts are forced to jump between dashboards to piece together the story. This “swivel-chair” analysis slows investigations, giving attackers more time to do damage.



WARNING

Too many siloed tools don't just slow down your team — they give attackers more room to maneuver.

Defining the Cloud-Native Application Protection Platform

A CNAPP is a unified security solution built for modern cloud complexity. It consolidates multiple security tools into a single platform, enabling them to share information and provide insight that separate toolkits never could.



REMEMBER

Think of a CNAPP as a unified command center for cloud security — everything you need in one place, working together.

CNAPP brings previously separate controls into one place so signals can be correlated, prioritized, and acted on. A true CNAPP integrates the capabilities of multiple tools into one cohesive system. Most CNAPPs provide a core set of capabilities, including the following:

- » **Application security posture management (ASPM):** End-to-end app risk view
- » **Software supply chain security:** Third-party/open-source hygiene
- » **Cloud security posture management (CSPM):** Misconfiguration and posture checks
- » **Cloud infrastructure entitlement management (CIEM):** Least-privilege and entitlements
- » **Data security posture management (DSPM):** Sensitive data discovery/control
- » **AI security posture management (AI-SPM):** Model/data lifecycle security
- » **Cloud workload protection (CWP):** Runtime threat detection/defense
- » **Web application and API Security (WAAS):** Web/application programming interface (API) protection and abuse
- » **Cloud detection and response (CDR):** Correlated detection and response



Each of these tools existed before CNAPP. The difference is how a platform unifies them, allowing context to flow between capabilities.

Table 4-1 shows how a siloed stack compares with a unified CNAPP.

TABLE 4-1 Siloed Tools versus CNAPP

Capability	Siloed Tools	CNAPP
Visibility	Fragmented views per service/layer	Unified, full-lifecycle visibility
Risk context	Limited to isolated issues	End-to-end attack paths and data context
Coverage	Point-in-time checks	Continuous coverage, dev to runtime
Remediation	Manual alert triage and handoff	Automated remediation with security operations center (SOC)-ready incidents
Team alignment	Siloed among cloud, AppSec, SOC	Shared context across teams

Seeing Why the Platform Approach Matters

Beyond just integrating tools, a CNAPP provides key advantages for modern security:

- » **Unified visibility across clouds:** You get a single, consistent security view across Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and beyond.
- » **Shared context to unify teams:** Developers, security analysts, and operations can all work from one source of truth.
- » **AI-powered risk correlation:** You find hidden patterns and toxic combinations that represent real attack paths.
- » **Prioritizing risks that matter:** It moves teams from chasing thousands of alerts to fixing the few that really matter.
- » **End-to-end lifecycle coverage:** Security is embedded from the first line of code to runtime detection and SOC operations.
- » **Automated remediation at scale:** It converts raw alerts into a handful of SOC-ready incidents, many remediated automatically.



TIP

Think of CNAPP as cutting through the clutter: one place, one context, one action plan.

With a CNAPP, teams move faster with fewer blind spots — because context, priorities, and actions live in one place.

IN THIS CHAPTER

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

Chapter 5

Looking at Regulatory Compliance in the Cloud

If you work in an enterprise, you've probably seen the impact of regulations from both governments and industry organizations. There are too many regulations to cover them all in depth, but I've chosen a couple to review so you can see what you'll encounter when working in cloud security. This chapter takes a look at the European Union's General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directive.

Navigating the Regulatory Landscape

It's probably not news to you, but the regulatory landscape is constantly evolving. There is an ever-increasing number of laws and statutes mandating information security and data protection requirements worldwide. Some regulations you may have encountered include the U.S. Health Insurance Portability and Accountability Act (HIPAA), the U.S. Gramm-Leach-Bliley Act (GLBA), Society for Worldwide Interbank

Financial Telecommunication (SWIFT) data protection policies, the Payment Card Industry Data Security Standard (PCI DSS), and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). In the European Union, the GDPR and NIS Directive (EU 2016/1148) have important implications for organizations operating in the cloud. Here's an in-depth exploration of two of the most onerous compliance frameworks you're likely to encounter.



REMEMBER

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).

General Data Protection Regulation

GDPR applies to enterprises and other organizations that process or store personal data on individuals located in the European Union (EU). As far as the GDPR is concerned, *personal data* is defined as any information relating to an individual that is identified or identifiable. For example:

- » Data that identifies you or can be used to identify you (for example, name, email address, date of birth, user ID)
- » Data that identifies a unique device used by a single person, like your Internet Protocol (IP) address or unique device ID
- » Data that reflects or represents a person's behavior or activity (for example, your location, the applications you downloaded, or the websites you visited)

The GDPR is much stricter than previous data protection laws. And if you think you're off the hook because your company isn't in the EU, think again. Companies outside the EU that have EU customers are covered by GDPR.

Here are some key points about GDPR that will shape how you plan your compliance practices:

- » **The GDPR has mandatory notification requirements for breaches that involve personal data.** For starters, you'll need to notify supervisory authorities within 72 hours. This is a must if personal data is lost, stolen, or otherwise compromised. In some cases, you'll have to notify individuals as well.

Notifications aren't just short apologies or a quick "Sorry, my bad." They have to describe 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.

» **The GDPR stipulates administrative fines.** The penalties for noncompliance are meant to deter, so they're going to hurt. Your organization could face potential maximum fines of the following (and more):

- Four percent of annual global revenue (or maximum €20,000,000, whichever is higher) for noncompliance with its data processing and data management obligations
- Two percent (or maximum €10,000,000, whichever is higher) for security and data breach notification-related obligations

Personal data protection is now a board-level concern for many reasons, including the potential reputational harm of data breaches, the GDPR's mandatory notification mandate, the possibility of regulators' investigations, and significant administrative fines.



WARNING

Watch out for the scope of work ahead with GDPR. It requires substantial technology, personnel investments, and business process controls for companies to achieve compliance. The GDPR impacts 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. You've been warned.

If your organization is subject to GDPR, you're going to want to understand the risks of collecting personal information, so be sure to protect your systems with the appropriate security. This may require a shift in thinking in your organization.

If you're lucky enough to get the opportunity to read the details of GDPR requirements, you'll find they center around data management — namely, data collection and processing. There are a variety pack of obligations. You have to provide notice when collecting personal data, you can't allow unauthorized data processing, you have to be a good steward and maintain records of data processing activities, you have a duty to appoint a data protection officer (DPO) in certain instances, and there are rules regarding transfer of personal data to third parties and third countries, amongst others.

GDPR has specific security-related language, as described in Table 5-1, including protecting personal data from exfiltration by cyber-adversaries and from internal leakage. So, as you and your organization work toward GDPR compliance, it's important to keep sight of the need to complement investments in compliance activities with needed investments in cybersecurity.

TABLE 5-1 Summary of Relevant Provisions from the GDPR

Topic	Summary of Provisions
<p>Security of data processing</p>	<p>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]</p> <p>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]</p> <p>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]</p>
<p>Data breach notification</p>	<p>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]</p>
<p>Administrative fines</p>	<p>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]</p>



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, are not going cut it when you need 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. This is a good time to understand the benefits of modern cloud security tools such as CSPM, CWPP, and CNAPP and how they can help streamline compliance efforts.

Network and Information Security 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 so they can keep the proverbial lights on. They do this by establishing security and incident notification obligations for various organizations that offer essential and digital services.



REMEMBER

The NIS Directive isn't your typical regulation. It's actually a set of objectives and policies that members of the EU should work toward through legislation.

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 organizations also have to 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. If you're unfortunate enough to have a significant security incident, you'll be reporting to the appropriate national authorities.

Recognizing the Importance of Automated, Continuous Monitoring

Security and compliance are shared responsibilities in the public cloud. It's your data at the end of the day, and if there is a breach or compliance violation, your company will be accountable.

Sure, your cloud provider delivers a service, but the security of your workloads and your data is your responsibility. It's also your revenue, reputation, and customer relationships that are at stake.

So, what are you to do? 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. Enterprises operating in the cloud should be focusing their security operation efforts around tools that can provide continuous monitoring, assessment, and prioritization of risks, and automated remediation.

How do you know you're in compliance on any given day? Because you are constantly measuring security and compliance. 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 solution 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.

If you follow these guidelines you will be able 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 (ML) and analytics — without requiring human interaction.
- »» Monitor compliance throughout the entire development lifecycle.
- »» 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.

Continuous monitoring and compliance automation is a common good for your organization; both compliance and application development teams will benefit. For example, your compliance team can significantly reduce time spent on third-party security audits. Over in the application development department, 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 Catchup” Trap

Do you work in an organization where compliance is a never-ending cycle of audits, reactionary efforts to correct audit discrepancies, and an inevitable drift from the compliant state over time? That must hurt. 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.

Fortunately, new cloud security tools are designed to end the frustration, repetition, and drudgery by 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 will help your organization get into shape:

1. Monitoring.

The cloud environment is changing continuously. These changes can be normal, routine activities of DevOps or IT

teams. 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.

Implementing a Proactive Approach with DevSecOps

One thing that shows the increasing need for cross collaboration and ending silos is the rise of the DevSecOps engineer. The role of the DevSecOps engineer touches the entire IT stack including network, server, host, container, and cloud and application security. It also includes the entire software development lifecycle. Over on the development side of the world, the primary focus is on identifying and preventing vulnerabilities. In operations,

the focus shifts to monitoring and defending against both inside and outside attacks while maintaining compliance.

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:** Unit testing is the first opportunity to test a piece of code against its functionality. It's where you catch the low-hanging fruit of buggy software.
- » **Dependency scanning:** Dependency scanning checks dependencies like libraries for vulnerabilities, which helps you catch any libraries that are not safe to use.
- » **Dynamic application security testing (DAST):** DAST tests for vulnerabilities without analyzing the code in this phase. This is also known as *black-box testing*. Examples include APIs, Structured Query Language (SQL) injections, cross-site scripting, and other external methods sending input parameters to the application.
- » **Static application security testing (SAST):** SAST focuses on analyzing code, making it possible to find vulnerabilities earlier in the development stage without exercising the code.
- » **Container scanning:** Container scanning helps detect vulnerabilities, malware, and other security measures in images 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.

Your organization can address the inherent risk-related challenges by employing a security platform built for the cloud — in particular, one that leverages automation to provide continuous monitoring, analysis, prevention, and remediation for cloud security and compliance.

This is a new model that provides comprehensive protection in the cloud. As your organization continues to rely on public clouds to drive both day-to-day business activities and innovation, it 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 suggest focusing 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.
- » **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 demonstrate your security and compliance posture at the push of a button.

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 6

Building an Organizational Culture around Security

If you've read the previous chapters, you have a good understanding of what's involved with cloud security and compliance. That often leads to the question, "Okay, so I know what I need to do — how do I get started?" This chapter answers that question.

Managing Cybersecurity in the Modern Era

Enterprise security isn't easy (as if you didn't know that already). The speed at which enterprises are moving today to innovate and deliver digital services compounds the challenges you already face. To succeed at building and maintaining secure cloud operations, enterprises must have the processes, the technology, and the people in place to keep systems adequately secured.

Cybersecurity isn't just technology; it's people and culture. A company's cybersecurity culture is shaped by the attitude, knowledge, assumptions, norms, and values of the workforce, as well as 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.

It's critical for you to foster an environment where employees have the knowledge and instinct to both identify and immediately respond to cyber-threats. In the following sections, I look at how you can foster a culture that promotes security awareness and adoption of best practices.

Creating an effective cybersecurity team

If you want to create an effective cybersecurity team, begin with an assessment of your organizational needs. Identify teams that you may need to create, as well as the skills you want.

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

How many cybersecurity professionals leave the office at the end of the day thinking, "That was a good day — I got it all done." Probably as close to zero as you can get. 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 that gap.

From the cyber-defender's perspective, there are three ways automation can help an organization:

- » **Turn threat detection into threat prevention.** Don't spend any time manually preventing known threats. 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 should set policies based on the context of what should be protected: users, data, and applications. Context-based policies are designed to adapt to business changes without requiring constant updates.
- » **Accelerate the pace of investigations using analytics and machine learning (ML).** Artificial intelligence (AI) and analytics provide insights and context around exploits and techniques. They allow security teams to detect, assess, prioritize, and respond much more rapidly than they could if they had only manual procedures.



TIP

A security vendor that offers automation essentially gives you time back to focus on more valuable, business-critical work. Automation 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. What can your team do with this time? How about train on the latest concepts, tools, and methods around security and application deployment?

Assessing security effectiveness

It's essential to understand what success looks like for the security team. This is why we need key performance indicators (KPIs), which can help the team continuously assess its effectiveness in protecting the organization's cloud assets.

Here are some potential KPIs that can help security teams assess the effectiveness of security practices:

- » 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

If you already use automation extensively in your cybersecurity processes, you probably understand the value of automation in avoiding configuration errors and enabling rapid security response actions when threats are detected. You want to bring that level of effectiveness to the cloud, but it will require different tools than you may have used in other environments.

Whether a business is in the cloud implementation phase or is more focused on cloud optimization, automation becomes increasingly important as they increase cloud usage and operations in the cloud. With automation, these organizations can successfully scale their cybersecurity operations and reduce the risk of error across the organization's entire cloud footprint.



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

The need to adapt your security practices to the demands of dynamic cloud environments is expanding the group of stakeholders in security decisions and operations. In the past, developers

may not have focused on the broader security picture, but now they play a more significant role in the conversation. Developers are assuming more responsibility for cloud security with the “shift left” mindset.

Clearly, you need to consider how you integrate cloud security tools and practices into the developer workflow. However, 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. This demands that organizations include efforts to develop DevSecOps skills within their developer teams.

Continuous cybersecurity skills training and enhancement

If you want to successfully implement security essentials, your 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

That’s a lot, but it’s an achievable goal if you have appropriate cross-training and security training. Your organization should have training in place for 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).



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 are not an add-on feature. They 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 (QA) phase or, worse, in production. Stay secure and compliant with 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 lifecycle.

Executive leadership

Don't forget to talk to the top brass. Get with your chief information officer (CIO) or chief information security officer (CISO) and explain what it takes to build a security-aware DevOps team. Leadership support is the determining factor to whether you'll succeed. Successfully building a secure DevOps organization requires leadership that will help to drive and instill security culture and processes.

Automation

If it 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.

Cultivating the collaborative mindset

The spirit of DevOps is twofold:

- » To break down the silos between developers, operations teams, IT leadership, QA, and security.

»» To 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 other teams is essential. Everyone on your teams needs to understand their role, as well as the challenges faced by others in the organizations. 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 collaboration in security, 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.



REMEMBER

Silos bad, collaboration good.

Security accountability

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

IN THIS CHAPTER

- » Knowing your responsibilities
- » Working with other stakeholders
- » Adopting a cloud-centric approach
- » Unifying your data
- » Mapping context across tools
- » Leveraging automation
- » Understanding your potential exposure
- » Implementing least-privilege access
- » Evaluating your options
- » Minimizing your attack surface

Chapter 7

Ten Cloud Security Recommendations

This chapter offers a quick, rapid-fire look at ten best-practices recommendations to help you protect your data and applications in the cloud.

Understand the Shared Security Model

You are not alone in the cloud. Public cloud providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure can't be expected to know who should have write access to specific data in your environment any more than you're expected to protect the physical buildings that house cloud servers. In the shared security environment, the cloud provider is responsible for ensuring that the platform is always on, available, and up to date. But you, the customer, are responsible for

protecting your own applications and data running within the public cloud.

You're in complete control of what security to implement within your arena of responsibility, and you must take steps to safeguard your content, whether it's 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.

Involve Cross-Functional Teams

Whether you're building or updating your cloud security program, the cloud security team is not an isolated island in your enterprise. You need to communicate with stakeholders in development, DevOps, AppSec, IT, and the security operations center (SOC). The goal of those kinds of efforts is to:

- » Understand their initiative and road-map priorities for the cloud.
- » Gain alignment on cloud security and processes.
- » Identify gaps or areas of overlap with other teams.
- » Determine where and how to standardize on security tools and data collection to improve collaboration.

Take a Cloud-Centric Approach

When you're in the cloud, you get to address business challenges with an agile, scalable approach. To take full advantage of this, you need to apply the concepts of the modern data center to your cloud deployment architecture. Leaving behind the traditional constructs and practices that worked well with monolithic applications running on-premises will serve you well — it'll enable your organization to achieve high availability and scalability organically.

Unify Data

Keep an eye on the big picture. Bring cloud security context from different sources into a shared data lake, including configurations, audit trails, and logs across cloud providers. This makes it easier to correlate findings from different sources and enhance visibility.



TIP

Be sure to standardize on storage formats and implement comprehensive data lifecycle management policies for the data lake. Your future self will thank you.

Implement a Context-First Mindset

The cloud is a complex environment, and your responsibilities are complicated enough without adding to your cognitive load with fragmented tools and multiple data silos. Do you really want to deal with a variety pack of security tools such as cloud security posture management (CSPM), cloud infrastructure entitlement management (CIEM), and cloud workload protection platform (CWPP)? No, so map context across these tool domains to reveal high-severity issues.

Use Automation to Eliminate Bottlenecks

Wherever you look in the cloud, you'll find automation. And no wonder — change is constant in the cloud. If you go to all the trouble to develop comprehensive policies and practices, don't bog them down with manual implementations.



TIP

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



REMEMBER

It's difficult for teams to analyze and address every issue manually. Automating processes can eliminate bottlenecks.

Know Your Potential Exposure

Let's be honest: One of the reasons you like public clouds so much is that you can easily spin 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, make sure you are

- » **Monitoring cloud usage:** Keep an eye on how much your organization is spending on the cloud and what you're spending it on. A few well-placed tags and labels on cloud resources can go a long way toward helping you track your spend and identify anomalous resources.
- » **Ensuring 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.
- » **Identifying data store and network-based exposures:** Don't forget to include other potential internet exposure, such as data store- and network-based exposures in your cloud environment.
- » **Requiring 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.
- » **Locking 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.

Minimize Access Permissions

If you want to make it easy for attackers to get into your systems, then be sure to have compromised assets with excessive permissions readily available. That will make it easy for those malicious actors to move laterally through your infrastructure to get to the crown-jewel assets like sensitive data. Monitoring cloud infrastructure access and limiting permissions can reduce your blast radius, preventing attacks from becoming disasters. Be sure to monitor both identities of humans as well as nonhuman identities (service accounts).

Prepare for Incident Response

Congratulations on all the preventive measures you've taken and all the carefully crafted security controls you've implemented! Unfortunately, they aren't enough. You also need to plan for successful malicious attacks or other kinds of incidents. Be sure to understand how you would detect and be alerted to an incident, what data you would need to understand the context of an attack, and how you would respond to isolate assets and correct the root cause(s) that enabled the attack.

Evaluate Your Security and Compliance Options

There are several security options to choose from when moving to the cloud, including the following:

- » **Native security services:** Cloud service providers (CSPs) offer native security services, which are a good starting point. These include security groups, web application firewalls (WAFs), configuration monitoring, and many more. Look to

supplement these with enterprise-grade security offerings to address shortcomings.

For example, security groups and port-based firewalls are essentially port-based access control lists (ACLs), 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.

- » **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 or readily communicate with each other. They also require specialized skills to operate and manage. Automation becomes difficult, if not impossible, to achieve.
- » **Cloud-native application protection platforms (CNAPPs):** Unlike the disparate tools that create security silos, a CNAPP provides a cohesive, purpose-built platform for the modern cloud. By integrating multiple security controls (such as posture management, workload protection, and entitlement governance) into a single system, a CNAPP automatically correlates signals across the entire cloud-native lifecycle. This unified approach eliminates tool sprawl, enhances contextual visibility, and allows teams to prioritize and act on true risk without the burden of complex, manual integration.
- » **DIY security:** Some organizations choose a DIY approach to securing cloud workloads, using custom scripts and open-source projects to protect deployments. The disadvantages of this strategy are obvious. The only open question is which of the challenges of DIY security will sink you first: the burden of improving and deploying custom tools, the lack of expertise available to manage the security implementation and operations, or the nonexistent support in the event of a security breach?

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.



WARNING

Glossary

AI: *See* artificial intelligence (AI).

API: *See* application programming interface (API).

application programming interface (API): A set of protocols, routines and tools used to develop and integrate applications.

artificial intelligence (AI): The branch of computer science focused on enabling machines to perform actions that typically require human intelligence such as reasoning, planning, and problem solving.

attack surface: The devices and connections that malicious actors could potentially use to penetrate your network defenses.

black-box testing: *See* dynamic application security testing (DAST).

Center for Internet Security (CIS) Benchmarks: A set of globally recognized and consensus-driven best practices to help security practitioners implement and manage their cybersecurity defenses. Specific CIS Benchmarks are published for various technologies, operating systems, and public cloud environments.

CI/CD: *See* continuous integration/continuous delivery (CI/CD).

CIEM: *See* cloud infrastructure entitlement management (CIEM).

CIS Benchmarks: *See* Center for Internet Security (CIS) Benchmarks.

cloud infrastructure entitlement management (CIEM): The process of managing identities and privileges in cloud environments. The purpose of CIEM is to understand which access entitlements exist across cloud and multicloud environments, and then identify and mitigate risks resulting from entitlements that grant a higher level of access than they should.

Cloud Instance Metadata API: A service provided to running virtual instances that allows applications to access information about the running virtual instance. Available information generally includes name, security group, and additional metadata including sensitive data such as credentials and UserData scripts that may contain additional secrets. *See also* application programming interface (API).

cloud security posture management (CSPM): The practice of controlling public cloud infrastructure risk. CSPM tools automate the detection and remediation of misconfigurations across cloud resources.

cloud workload protection platform (CWPP): A security solution engineered to protect workloads in cloud environments. Workloads can be hosted on a range of infrastructures, from traditional VMs to modern containers and serverless functions, across public, private, and hybrid clouds. CWPPs preserve the confidentiality, integrity, and availability of workloads. *See also* virtual machine (VM), container, serverless function, public cloud, private cloud, *and* hybrid cloud.

cloud-native application protection platform (CNAPP): A unified security solution designed to address the entire lifecycle of cloud-native applications from development to production.

CNAPP: *See* cloud-native application protection platform (CNAPP).

Common Vulnerabilities and Exposures (CVE): A catalog of publicly disclosed security flaws (that is, vulnerabilities) maintained by the MITRE Corporation.

container: A lightweight, portable, and self-sufficient unit that packages an application along with its dependencies, libraries, and runtime environment. Containers enable applications to run consistently across different computing environments, simplifying development, testing, and deployment processes. They isolate applications from the underlying system, ensuring that each application runs in a dedicated user space.

continuous integration/continuous delivery (CI/CD): A DevOps environment supported by automation such that changes to application source code and infrastructure configuration are built, integrated, and deployed automatically. *See also* DevOps.

cross-site scripting (XSS): A client-side code injection vulnerability that enables untrusted scripts to execute in a user's browser within the context of a trusted web application. The application reflects or stores attacker-controlled input and delivers it without proper encoding or sanitization.

CSPM: *See* cloud security posture management (CSPM).

CVE: See Common Vulnerabilities and Exposures (CVE).

CWPP: See cloud workload protection platform (CWPP).

DAST: See dynamic application security testing (DAST).

data detection and response (DDR): A technology solution designed to detect and respond to data-related security threats in real time. It focuses on monitoring data at its source and allows organizations to spot threats that may not be detected by traditional infrastructure-focused security solutions.

data loss prevention (DLP): An application or device used to detect the unauthorized storage or transmission of sensitive data.

data protection officer (DPO): Under the GDPR, the DPO is the individual responsible for overseeing an organization's data protection strategy and implementation. *See also* General Data Protection Regulation (GDPR).

data security posture management (DSPM): A comprehensive approach to safeguarding an organization's sensitive data from unauthorized access, disclosure, alteration, or destruction. DSPM encompasses various security measures, including data classification, data encryption, access control, data loss prevention (DLP), and monitoring. *See also* data loss prevention (DLP).

DDoS: See distributed denial-of-service (DDoS).

DDR: See data detection and response (DDR).

DevOps: The culture and practice of improved collaboration between software developers and IT operations.

DevSecOps: An approach that extends the DevOps model by integrating security into the CI/CD pipeline through automated checks, ensuring close collaboration between development, IT, and security teams. *See also* DevOps *and* continuous integration/continuous delivery (CI/CD).

distributed denial-of-service (DDoS): A type of cyberattack in which extremely high volumes of network traffic are sent to the target victim's network to make their network and systems unavailable or unusable.

DLP: See data loss prevention (DLP).

DPO: See data protection officer (DPO).

DSPM: See data security posture management (DSPM).

dynamic application security testing (DAST): A security testing method that simulates real-world attacks on a web application while it is running. Also known as *black-box testing*.

FaaS: See functions as a service (FaaS).

functions as a service (FaaS): A cloud computing service that allows customers to run code in response to events, without managing the complex infrastructure typically associated with building and launching cloud applications.

GDPR: See General Data Protection Regulation (GDPR).

General Data Protection Regulation (GDPR): A data privacy law that strengthens data protection requirements for European Union (EU) residents and addresses the export of personal data outside the EU.

GLBA: See Gramm-Leach-Bliley Act (GLBA).

Gramm-Leach-Bliley Act (GLBA): A U.S. law that requires financial institutions to implement privacy and information-security policies to protect the nonpublic personal information of clients and consumers.

Health Insurance Portability and Accountability Act (HIPAA): A U.S. federal act that addresses security and privacy requirements for medical systems and information.

HIPAA: See Health Insurance Portability and Accountability Act (HIPAA).

hybrid cloud: An environment consisting of resources from multiple public and/or private clouds that provide application and data portability across clouds. See *also* private cloud *and* public cloud.

hypervisor: In a virtualized environment, the supervisory program that controls allocation of resources and access to communications and peripheral devices.

IaaS: See infrastructure as a service (IaaS).

IaC: See infrastructure as code (IaC).

IAM: See identity and access management (IAM).

identity and access management (IAM): A software service or framework that allows organizations to define user or group identities within software environments and then associate permissions with them.

infrastructure as a service (IaaS): A cloud computing service model in which customers can provision processing, storage, networks, and other

computing resources and deploy and run operating systems and applications.

infrastructure as code (IaC): A DevOps process in which developers or IT operations teams can programmatically provision and manage the infrastructure stack for an application in software. *See also* virtual machine (VM) *and* DevOps.

large language model (LLM): A category of AI models trained on enormous amounts of data, making them capable of understanding and generating natural language and other types of content to perform a wide variety of tasks. *See also* artificial intelligence (AI).

least privilege: A security principle in which only the permission or access rights necessary to perform an authorized task are granted.

LLM: *See* large language model (LLM).

machine learning (ML): A method of data analysis that enables computers to analyze a data set and predict labels and classifications, as well as numeric values, such as the predicted selling price of a stock.

MFA: *See* multifactor authentication (MFA).

microsegmentation: An approach to security that involves dividing a network into segments and applying security controls to each segment based on the segment's requirements. These granular segments, or secure zones, isolate workloads, securing them individually with custom, workload-specific policies.

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK): A knowledge base of adversary tactics and techniques, derived from real-world observations and maintained by MITRE Corporation, used to map, detect, and mitigate post-compromise behavior across enterprise, cloud, mobile, and industrial control system environments.

MITRE ATT&CK: *See* MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

ML: *See* machine learning (ML).

multi-cloud: An environment consisting of resources from multiple public and/or private clouds, but that does not necessarily provide application and data portability across clouds (that is, the different cloud environments may operate as siloed clouds). *See also* hybrid cloud, private cloud, *and* public cloud.

multifactor authentication (MFA): An authentication mechanism that requires two or more of the following factors: something you know,

something you have, or something you are. For example, a user may authenticate with their username and password (something you know) and a one-time passcode sent to an authenticator app on their mobile phone (something you have).

Network and Information Security (NIS) Directive (EU) 2016/1148: Adopted in 2016 and intended to boost the overall cybersecurity level for critical infrastructure in the European Union (EU), NIS Directive (EU) 2016/114 was the first cybersecurity law to cover the entire EU.

NIS Directive (EU) 2016/1148: See Network and Information Security (NIS) Directive (EU) 2016/1148.

PaaS: See platform as a service (PaaS).

Payment Card Industry Data Security Standard (PCI DSS): A standard set of requirements developed for the protection of personal data related to credit, debit, and cash card transactions.

PCI DSS: See Payment Card Industry Data Security Standard (PCI DSS).

Personal Information Protection and Electronic Documents Act (PIPEDA): A Canadian privacy law that defines individual rights with respect to the privacy of their personal information and governs how private-sector organizations collect, use, and disclose personal information in the course of business.

personally identifiable information (PII): Information such as name, address, Social Security number, birth date, and place of employment, that can be used on its own or with other information to identify, contact, or locate a person.

PII: See personally identifiable information (PII).

PIPEDA: See Personal Information Protection and Electronic Documents Act (PIPEDA).

platform as a service (PaaS): A cloud computing service model in which customers can deploy supported applications onto the provider's cloud infrastructure but doesn't have to manage or control the underlying cloud infrastructure.

private cloud: A cloud computing deployment model that consists of a cloud infrastructure that is used exclusively by a single organization.

public cloud: A cloud computing deployment model that consists of a cloud infrastructure that is open to use by the general public.

Remote Desktop Protocol (RDP): A proprietary Microsoft protocol that provides remote access to a computer. RDP uses TCP port 3389 and

UDP port 3389 by default. *See also* Transmission Control Protocol (TCP) *and* User Datagram Protocol (UDP).

SaaS: *See* software as a service (SaaS).

SAST: *See* static application security testing (SAST).

SDLC: *See* software development lifecycle (SDLC).

Secure Shell (SSH): A cryptographic network protocol that provides secure access to a remote computer.

security information and event management (SIEM): A set of tools and services offering a holistic view of an organization's information security, using predetermined rules to help security teams define threats and generate alerts.

security orchestration, automation, and response (SOAR): Technology that helps coordinate, execute, and automate tasks between various people and tools, allowing companies to respond quickly to cybersecurity attacks and improve their overall security posture.

serverless function: A cloud-native development model in cloud computing that allows developers to build and run applications and services without needing to manage infrastructure or server-side IT. Applications in the serverless model rely on a combination of managed cloud services and FaaS that abstract away the need to manage, patch, and secure infrastructure and VMs. *See also* functions as a service (FaaS) *and* virtual machine (VM).

SIEM: *See* security information and event management (SIEM).

SOAR: *See* security orchestration, automation, and response (SOAR).

Society for Worldwide Interbank Financial Telecommunication (SWIFT): A global network that facilitates secure and efficient financial transactions between banks and other institutions.

software as a service (SaaS): A cloud computing service model in which the customer is provided access to a hosted application that is maintained by the service provider.

software development lifecycle (SDLC): A structured process used by software developers to plan, design, develop, test, and maintain software applications.

SSH: *See* Secure Shell (SSH).

static application security testing (SAST): A security testing method that analyzes source code to find security vulnerabilities before the code is compiled. Also known as *white-box testing*.

SWIFT: *See* Society for Worldwide Interbank Financial Telecommunication (SWIFT).

TCP: *See* Transmission Control Protocol (TCP).

Transmission Control Protocol (TCP): A connection-oriented protocol responsible for establishing a connection between two hosts and guaranteeing the delivery of data and packets in the correct order.

UDP: *See* User Datagram Protocol (UDP).

UEBA: *See* user and entity behavior analytics (UEBA).

User Datagram Protocol (UDP): A connectionless protocol (in which a direct connection between network devices is not established before datagrams are transferred) that provides best-effort delivery (received datagrams are not acknowledged, and missing or corrupted datagrams are not requested) of data.

user and entity behavior analytics (UEBA): A type of cybersecurity solution or feature that discovers threats by identifying activity that deviates from a normal baseline.

virtual machine (VM): An instantiation of an operating system running within a hypervisor. *See also* hypervisor.

VM: *See* virtual machine (VM).

WAF: *See* web application firewall (WAF).

WAAP: *See* web application and API protection (WAAP).

web application and API protection (WAAP): The evolution of cloud WAF services that were designed to protect internet-facing web applications and web APIs, including API management capabilities, that enable organizations to discover and protect web APIs, enforce their usage policies, and control access. *See also* web application firewall (WAF) *and* application programming interface (API).

web application firewall (WAF): A type of firewall that protects web applications and APIs by filtering, monitoring and blocking malicious web traffic and application-layer attacks — such as DDoS, SQL injection, cookie manipulation, XSS, cross-site forgery and file inclusion. *See also* application programming interface (API), distributed denial-of-service (DDoS), *and* cross-site scripting (XSS).

white-box testing: *See* static application security testing (SAST).

XSS: *See* cross-site scripting (XSS).

Stop chasing alerts, start preventing breaches

Organizations are rapidly migrating critical applications and data to the cloud while increasingly adopting a multi-cloud strategy. An advantage of migrating applications to the cloud is speed of delivery and innovation. However, legacy security tools, policies, and processes designed for traditional data centers and IT operations cannot adapt to address SaaS applications or the continuous deployment model and pace of change in the cloud. In this book, you'll learn how to properly manage cloud risk without slowing down deployment with a consistent approach to security and compliance that spans the cloud application life cycle stages of code, build, deploy, and run.

Inside...

- Unify your stack with a single platform
- Stop chasing alerts and find real attack paths
- Ship secure code faster
- Eliminate blind spots across your entire cloud
- Master continuous, audit-ready compliance

 **CORTEX® CLOUD**
BY PALO ALTO NETWORKS

Dan Sullivan is a cloud architect, instructor, and author with decades of experience developing, deploying, and maintaining production applications. His roles have included designing for security and supporting security operations.

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

ISBN: 978-1-394-35659-1

Not For Resale



for
dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

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