LEARNING MADE EASY

Palo Alto Networks Custom Edition

Cloud Detection & Response (CDR)

for dummies®

A Wiley Brand

Understand cloud detection and response

Implement plans to prevent attacks

Detect, respond to, and remediate attacks

Brought to you by

paloalto® 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 Detection & Response (CDR)

Palo Alto Networks Custom Edition

by Dan Sullivan

for dummies®
A Wiley Brand

Cloud Detection & Response (CDR) For Dummies®, Palo Alto Networks Custom Edition

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

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 978-1-394-35437-5 (pbk); ISBN 978-1-394-35438-2 (ebk); ISBN 978-1-394-35440-5 (ebk)

Publisher's Acknowledgments

Editor: Elizabeth Kuball

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager: Cynthia Tweed

Production Editor: Bharaneedharan Murthy

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

Table of Contents

Introduction

Imagine a silent alarm trips in your company's digital vault. There's no loud siren, no flashing red lights — just a single, cryptic message in a log file that says a side door was opened with a key that hasn't been used in six months. Is it a janitor on the wrong shift? A software glitch? Or the beginning of a sophisticated heist?

In the cloud, this is what a modern break-in looks like. Attackers don't often use brute force anymore. They're subtle. They don't smash windows; they pick locks with stolen keys — a developer's credentials lifted from a public code repository. They don't run through the hallways; they move silently between systems, using the cloud's own legitimate tools to look like any other employee. The clues they leave behind are faint and scattered across a vast digital landscape.

That's where the real detective work begins. Cloud detection and response (CDR) is the discipline of taking that one cryptic clue and turning it into a full-blown investigation. It's about connecting the dots between an odd login in London, an unusual data access request on a server in Virginia, and a new user account being created in your sales application. It's the process of finding the story of an attack while it's still happening.

About This Book

Cloud Detection & Response (CDR) For Dummies, Palo Alto Networks Custom Edition, is your field guide to becoming a digital detective in the cloud. You don't need a trench coat or a magnifying glass — just a desire to understand how to protect your organization's most valuable assets. This book skips the dense, impenetrable jargon and focuses on what you actually need to know. In this book, you discover how to:

- **Think like the culprit.** Get inside the mind of a cloud attacker to understand their new playbook.
- **Find the fingerprints.** Learn where to look for evidence across your cloud environment.

- **Follow the leads.** Turn disjointed alerts into a clear attack path that shows you exactly what the attacker did.
- **Close the case.** Respond with speed and precision to neutralize the threat and restore security.

This book is designed to give you the foundational knowledge to build or contribute to a modern cloud security strategy, whether you're a security professional, a developer, or a manager who needs to understand the risks.

Foolish Assumptions

To write this book, I had to make a few assumptions about you, the reader:

- You understand that the cloud is more than just someone else's computer — it's a complex environment of services, identities, and data.
- You're working in a security, IT, or development role, or you're a leader who's responsible for the security of your organization.
- You're not looking for a book that will teach you how to write code. You're looking for a strategic guide to understand the concepts, processes, and tools involved in cloud defense.
- You know that perfect prevention is a myth, and you're interested in what to do when an attacker inevitably gets in.

Icons Used in This Book

Throughout this book, you'll see little pictures in the margins designed to draw your attention to specific kinds of information.


REMEMBER

The Remember icon points out information that's worth remembering long after you've finished the chapter. It's a foundational concept.

TIP

Tips are like shortcuts. The Tip icon highlights a piece of advice that can save you time, frustration, or a future security headache.

WARNING

The Warning icon points out a potential pitfall or a common mistake that you'll want to avoid.

Beyond the Book

There's only so much I can cover in this short book, so if you find yourself at the end of it wondering, "Where can I learn more?" go to `www.paloaltonetworks.com/cortex/cloud-detection-and-response`.

IN THIS CHAPTER

- Thinking like a cloud attacker
- Assembling a modern cloud defense team
- Getting a clear definition of cloud detection and response
- Figuring out how cloud detection and response fits in with a cloud-native application protection platform

Chapter 1
Introducing Cloud Detection and Response

The rapid expansion of the cloud creates both challenges and opportunities for security teams. But to understand how to defend the cloud, you first have to understand why it's such a tempting target. Traditional security tools — like those for endpoint or network detection — weren't designed for an environment where attackers can use the cloud's own features against it. A new approach is required, one that starts with understanding the attacker's playbook.

The Cloud Attacker's New Playbook

To a threat actor, the cloud isn't just a new place to attack — it's a gold rush. The same features that make the cloud powerful for your business also create powerful opportunities for them.

Instead of seeing a list of technical challenges, an attacker sees a field of open doors:

- **Misconfigurations are an open invitation.** An attacker doesn't need to be a master hacker to get in. They can just scan the internet for a single misconfigured storage bucket or an exposed database, like a burglar checking every house on the block for an unlocked window.
- **Identity is the master key.** Why bother writing malware when you can just steal the keys to the kingdom? Attackers hunt for developer credentials accidentally left in public code repositories. With one stolen identity, especially one with overly broad permissions, they can walk right in and look like a legitimate employee.
- **Vulnerabilities are a way in.** The code you deploy may have vulnerabilities that let attackers bypass your protective measures. A well-crafted malicious input, for example, can be the key to a successful injection attack that leaks sensitive data.
- **Automation is a superpower.** The tools you use to deploy applications and manage infrastructure at scale can be turned against you. Once inside, attackers use automation to spread through an environment at machine speed, far faster than a human security analyst can track.

Assembling Your Cloud Defense Team

Because attackers treat the cloud differently, you have to defend it differently. The old security model — where a security team works in a silo and throws tickets "over the wall" for developers to fix — is broken. Defending the cloud is a team sport, and you need a new kind of lineup:

- **The offense — developers and the development and operations (DevOps) team:** These are the builders. They have the deepest knowledge of the applications and are the only ones who can fix vulnerabilities at the source. In a modern defense, they're not just building features; they're building secure applications from the start.

- **The defense — cloud security architects:** These are the designers. They establish the overall security posture, set up the preventive controls, manage configurations, and ensure that the environment is architected to be resilient. They're the ones who try to lock the windows before the burglar arrives.
- **The special teams — the security operations (SecOps) team:** These are the incident responders. When an attacker gets past the initial defenses, these are the experts who hunt down the threat, contain the damage, and kick out the intruder.

A successful cloud detection and response (CDR) strategy gets all three groups working from the same playbook. It provides the visibility and tools that allow the security team, developers, and architects to collaborate in real time to shut down an attack.

Defining Cloud Detection and Response

CDR is a security discipline that focuses on finding and neutralizing threats actively operating within your cloud environment. It combines technology and processes to answer two fundamental questions during an attack: "What's happening?" and "What should we do about it?"

An effective CDR strategy moves beyond the capabilities of traditional security tools to address the threats unique to the cloud.

Detecting and protecting against threats in a new landscape

In a traditional on-premises environment, defenders often look for malware or unusual network traffic. Cloud detection is different. As you've seen, attackers often don't need malware when they can abuse legitimate cloud features to achieve their goals. Effective detection means spotting the subtle clues an attacker leaves as they move through your environment.

Security tools collect signals from every corner of your cloud. These signals come from your cloud provider's control

plane — like Amazon Web Services (AWS) CloudTrail or Microsoft Azure Activity Logs — and from your workloads, identities, and applications. A good detection program pieces these signals together to tell the story of an attack, enabling you to catch the intruder before they steal your data.

Protection complements detection to block the worst impacts of threats. Detection tools let you know when a threat is present, and protections like access controls and firewall rules prevent those threats from causing harm.

Responding with speed and precision

As soon as you've detected a threat, the clock is ticking. A truly effective response is about surgically removing the threat without disrupting your business operations.

For example, if an attacker compromises a single container in a Kubernetes cluster, you don't want to shut down the entire application. A precise response may involve isolating the compromised container for forensic analysis while the application continues to run. Modern CDR tools automate many of these response actions. Automation ensures that the response is not only fast but also consistent and free from human error during a high-stress incident.

Seeing How Cloud Detection and Response Relates to Cloud-Native Application Protection Platforms

The cloud security market is full of acronyms, but CNAPP is one you need to know. A cloud-native application protection platform (CNAPP) isn't a single tool — it's an integrated suite of security capabilities designed to protect cloud applications, from development through production.

CDR is a critical, action-oriented component of a CNAPP. Other parts of a CNAPP focus on preventing issues, but CDR is what you use when a threat is active in your environment. A CNAPP unifies two key security functions:

- **Cloud security posture management (CSPM)** tools scan your cloud environment for misconfigurations. A CSPM tool handles the prevention side of the equation.
- **Cloud workload protection platform (CWPP)** tools protect the actual running applications and servers — your virtual machines (VMs), containers, and serverless functions.

These components feed crucial context into the CDR solution. CDR stitches a CSPM alert about a new, risky user permission combined with a CWPP alert about suspicious code execution on a VM to give you an incredibly clear picture of an attack. The CNAPP's integrated nature allows you to move from detection to a targeted response within a single platform, drastically reducing the time it takes to neutralize a threat.

IN THIS CHAPTER

- Mapping your cloud attack surface
- Securing your cloud workloads at runtime
- Hunting for cloud vulnerabilities before attackers do
- Securing identities and data — the crown jewels
- Turning compliance mandates into security blueprints
- Putting it all together: The anatomy of a modern cloud defense

Chapter 2
Preventing Attacks

In the last chapter, you step into the mind of a cloud attacker. You see how they turn the cloud's own features — its scale, automation, and interconnectedness — into weapons. In this chapter, it's time to build your defense. An effective cloud detection and response (CDR) strategy isn't just about reacting to fires. It's about making your environment a much harder target in the first place. Prevention is the foundation of a strong response.

Thinking in Cloud Time: Responding at Scale

Before I dive into the specific controls, I need to talk about a fundamental shift in mindset. Responding to threats in the cloud isn't just a faster version of what you used to do in a data center — it's a completely different sport with a new set of rules. The speed and scale of the cloud demand a new philosophy.

Treating resources as cattle, not pets

This is the most important mental shift for any cloud security professional. In the old on-premises world, servers were like pets. We gave them names, we nurtured them, and when one got sick — or compromised — we would spend days carefully trying to clean it and nurse it back to health.

The cloud flips this model entirely. Cloud resources are cattle, not pets. They're numerous, they're identical, and most importantly, they're disposable. A modern cloud response isn't about "cleaning" a compromised virtual machine (VM). It's about terminating it without a second thought, confident that an automated process will instantly spin up a pristine, healthy replacement from a trusted template. This approach is faster and more reliable, and it eliminates the risk that some hidden piece of malware was left behind.

Automating your first responders

A human simply can't click fast enough to contain a threat that spreads at machine speed. By the time an analyst has logged in to investigate an alert, an automated attacker could already be exfiltrating your data. The goal of a modern CDR strategy is to have automated playbooks act as your tireless first responders.

When a high-confidence threat is detected — like a workload communicating with a known malicious server — an automated response should fire immediately. That response may isolate the workload from the network, revoke the credentials it was using, or take a forensic snapshot for later analysis. The immediate danger is contained in seconds, allowing your human experts to perform a deeper investigation on a threat that has already been neutralized.

Performing forensics on the fly

Investigating a cloud incident doesn't involve seizing a physical hard drive from a server rack. Cloud forensics is a remote, dynamic process. It involves taking live snapshots of virtual disks and memory, often from resources running in different geographic regions.

This evidence is then analyzed in a dedicated, clean forensic environment that you can spin up on demand, use for your

investigation, and then tear down when you're finished. Not only is this approach faster but it ensures that your investigation doesn't interfere with your production environment or contaminate your evidence.

Knowing What You Need to Protect

Before you can defend your cloud, you have to see it the way an attacker does — not as a list of servers and databases, but as a map of interconnected opportunities. If you were securing a physical building, you wouldn't just count the rooms. You'd map out every door, window, hallway, and access road to understand how an intruder could move through the space. The same principle applies to the cloud. You need a complete and continuously updated inventory of every asset.

REMEMBER

You can't protect what you can't see. The first step in preventing attacks is creating a comprehensive inventory of all your cloud assets.

Your cloud contains a diverse set of assets, each with its own risks:

- **Identities:** Both the people (developers, admins) and the nonhuman accounts (service roles, automation scripts) that have the keys to your kingdom
- **Data:** The databases, storage buckets, and caches that hold your sensitive information
- **Workloads:** The compute resources that run your business — VMs, containers, and serverless functions
- **Infrastructure:** The virtual networks, security groups, and configurations that form the digital landscape of your environment

Manually tracking these assets is impossible. The cloud changes too quickly. Developers spin up new resources, applications scale automatically, and configurations drift. You need an automated discovery process that constantly scans your environment through your cloud provider's application programming interfaces (APIs). A good CDR solution does this for you, giving you a live map of your attack surface.

Protecting Cloud Workloads

Your cloud workloads are the engines of your cloud applications. They're where your code executes and your data gets processed, making them a prime target for attackers. Protecting them requires more than just predeployment scans — it demands real-time security that operates while the workload is running.

Maintaining runtime security

Think of runtime security as an expert security guard inside your application while it's operating. This guard doesn't just check IDs at the door. They patrol the halls, know the normal patterns of activity, and can spot an intruder instantly. A CDR agent operating inside your workload does the same thing. It establishes a baseline of normal behavior — which processes should be running, which network connections are typical, which files are accessed — and immediately detects any deviation.

An attacker who bypasses your initial defenses or exploits a *zero-day vulnerability* (a flaw that hasn't been discovered by defenders yet) will be caught by the runtime agent. The agent can take immediate action, such as shutting down a compromised process or isolating the entire workload, while logging every detail for forensic analysis.

REMEMBER

Runtime protection isn't about scanning for known threats before you deploy. It's about actively defending your applications from malicious threats and behavior as they execute.

Detecting and mitigating cloud vulnerabilities

Vulnerabilities are the cracks and unlocked windows in your cloud environment. They can be found in operating systems, third-party libraries, or your own application code. Even more common are misconfigurations — like giving a user account far more permission than it needs or leaving a storage bucket open to the public internet. A robust prevention strategy involves hunting for these weaknesses before an attacker can find them.

Modern development practices use a CI/CD pipeline — short for continuous integration/continuous deployment — to automatically build, test, and deploy code. Security scanners can

be integrated directly into this pipeline. These tools check your application code and container images for known vulnerabilities, effectively preventing a compromised asset from ever being deployed to your production environment.

Securing Identities and Data: The Crown Jewels

Workloads are the engines, but identities and data are the crown jewels of your cloud kingdom. An attacker who compromises a workload may cause a disruption, but one who steals a powerful identity or exfiltrates sensitive data can cause a catastrophe. Protecting them requires a focused strategy.

Enforcing the principle of least privilege

The principle of least privilege is a simple but powerful concept — never grant more permission than is absolutely necessary. A developer may need to read from a database, but they probably don't need to delete it. An automated script may need to write logs to a storage bucket, but it certainly doesn't need access to your customer records.

Overly permissive identities are one of an attacker's favorite targets. By enforcing least privilege, you dramatically shrink the potential blast radius of a compromised account. A CDR solution can help by continuously analyzing permissions across your cloud and flagging accounts that have more access than they need or use.

Knowing what's in your data

You can't protect your sensitive data if you don't know where it is. Is that storage bucket holding public marketing images or a backup of your customer database? Data security posture management (DSPM) tools answer that question. They scan your datastores to discover and classify sensitive information — like personally identifiable information (PII), financial records, or intellectual property. When your sensitive data is mapped, the system can monitor for risky configurations or unusual access patterns, alerting you before a data breach occurs.

Ensuring compliance

Compliance frameworks like SOC 2 (short for System and Organization Controls 2), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) can feel like a bureaucratic chore, but they're actually powerful tools for prevention. These regulations provide a ready-made blueprint for a strong security posture. They tell you what you need to protect and the controls you need to implement.

A CDR platform helps automate the often-painful process of proving compliance. It provides continuous monitoring that can detect and inventory all cloud assets — including resources that were deployed outside of your standard procedures. The platform can also identify misconfigurations that violate your defined security policies. Instead of scrambling for evidence during an audit, you have a constantly updated record that demonstrates that your security controls are in place and operating effectively.

Protecting Web Applications and Application Programming Interfaces

Your web applications and APIs are the public-facing doors to your cloud. They're designed to be accessed from the internet, making them some of the most tempting targets for attackers.

Identifying threats to web applications

The Open Worldwide Application Security Project (OWASP) maintains a Top 10 list of the most critical web application security risks. Your CDR strategy should be designed to defend against these common attack vectors, which include *injection flaws* (where an attacker sends malicious data to your application) and *broken authentication* (where an attacker can bypass your login mechanisms to impersonate a legitimate user).


TIP

Familiarize yourself with the current OWASP Top 10 list at `https://owasp.org/Top10`. It's an essential resource for understanding the threats your applications face.

Assessing risk to application programming interface endpoints

APIs are the connective tissue of the modern cloud, allowing different services to communicate with each other. Their power and ubiquity also make them a significant risk. CDR helps prevent API-related incidents by addressing several key risks:

- **Broken authentication:** Enforcing strict authentication and authorization for every API call ensures that only legitimate users and services can make requests.
- **Shadow APIs:** Developers sometimes create temporary or undocumented APIs for testing that are forgotten and left running. A CDR solution can discover all APIs in your environment — not just the official ones — and ensure that they're managed and secured.
- **Insufficient rate limiting:** An attacker can try to overwhelm an API with a flood of requests. Rate limiting prevents this by capping the number of requests a user can make in a certain period, stopping denial-of-service (DoS) attacks before they can impact your application.

Putting It All Together: The Anatomy of a Modern Cloud Defense

The concepts in this chapter aren't just a checklist — they're layers in a deep, interconnected defense. Let's walk through a quick story to see how they work together to shut down an attack.

An attacker finds a developer's credentials accidentally posted on a public website. Their attack begins. They use the stolen credentials to access a VM, hoping to use it as a launchpad to find sensitive data.

But the moment they log in, the layers of defense activate:

- The **runtime security** agent on the VM detects an unfamiliar process — the attacker's reconnaissance script. Before the script can even finish scanning the local network, the VM is

instantly isolated from the rest of the network, cutting off the attacker's access.

- Simultaneously, the system analyzes the stolen credentials. Because you've enforced the **principle of least privilege,** the attacker discovers that the account has no permissions to access any production databases or sensitive storage buckets. It's a dead end.
- Your security team receives a single, high-context alert. The alert doesn't just say "suspicious process detected." It **shows them the entire attack chain** — the compromised identity, the workload it accessed, the malicious process it tried to run, and the automated containment action that was taken. A forensic snapshot of the isolated machine has already been taken for them to analyze.

The attack was over before a human analyst even had to open a ticket. That's the power of a modern, integrated cloud defense. It's not about stopping a single action — it's about creating a resilient environment where every control works together to make a successful attack nearly impossible.

IN THIS CHAPTER

- Collecting the right signals from a sea of noise
- Connecting the dots to find the story of an attack
- Building an attack timeline
- Understanding the attacker's playbook with MITRE ATT&CK

Chapter 3
Detecting and Investigating Cloud Threats

The last chapter focuses on prevention — building a modern defense to make an attacker's job as difficult as possible. But even with the strongest defenses, you have to operate with a simple assumption: Attackers will eventually find a way in. Your goal then is to spot the attackers the moment they get in and kick them out before they can do any real damage. Detection and investigation are where the action happens.

The Analyst's Superpower: Augmenting Humans with Machines

Before I dive into the mechanics of detection, let's talk about a new philosophy. The goal of a modern cloud detection and response (CDR) platform isn't to replace your security analysts — it's to give them a superpower.

Think of a traditional security analyst like a detective from a 1950s film. When a crime is reported, they have to manually sift through mountains of paperwork, interview dozens of witnesses, and connect the dots on a corkboard with pins and string. The work is slow and painstaking, and it's easy to miss a subtle clue buried in the noise.

A modern cloud security analyst is like that same detective, but with a high-tech artificial intelligence (AI) assistant. The moment a threat is detected, the assistant has already analyzed all the relevant logs, cross-referenced every piece of evidence, highlighted the key anomalies, and presented the detective with the three most likely attack paths. The analyst still uses their intuition and expertise to solve the case, but their work is accelerated from days to minutes. A modern CDR platform is that AI assistant — a powerful partnership between human and machine.

Visibility: Seeing Your Entire Cloud

You can't detect a threat you can't see. Effective detection begins with total visibility, which means collecting signals from every corner of your cloud environment. Think of your security team as investigators at a crime scene. They need to see everything — the security camera footage, the building entry logs, the fingerprints on the door — to piece together what happened. In the cloud, your logs and telemetry are that evidence.

Collecting signals from a sea of noise

The good news is that cloud environments generate a staggering amount of data. The bad news is that cloud environments generate a *staggering* amount of data. Your challenge isn't finding data. It's finding the right data and filtering out the noise. For a strong detection program, you need to collect and analyze signals from several key sources:

- **Cloud provider audit trails:** Every action taken in your cloud — from a developer launching a new server to an automated script changing a firewall rule — is logged by your cloud provider. Services like Amazon Web Services (AWS) CloudTrail, Google Cloud Audit Logs, and Microsoft Azure Activity Logs are the official record of who did what and when.

- **Network traffic logs:** These logs show you every connection made to, from, and within your cloud network. They're essential for spotting unusual traffic patterns, like a workload suddenly communicating with a server in a country you don't do business with.
- **Workload and operating system logs:** These are the signals coming from inside your running virtual machines (VMs) and containers. They provide crucial details about which processes are running and which actions they're taking at the workload level.
- **Identity logs:** These logs track every login attempt, permission change, and action tied to a specific user or role. They're critical for spotting compromised credentials or an attacker trying to escalate their privileges.

REMEMBER

In an ideal world, you'd collect every log from every source. In the real world, you have to prioritize. Focus on collecting the logs that give you the most security value for the cost.

Connecting the dots with context

A single log entry rarely tells you anything useful. A failed login could be an employee who forgot their password. A large data transfer could be a routine backup. By themselves, these events are just noise. The magic of detection happens when you correlate these individual data points to reveal the full context of an attack.

An effective CDR platform doesn't just collect logs — it weaves them together into a single, understandable story. It combines a failed login from your identity provider, with a network log showing that the login came from an unusual location, with a workload log showing that a suspicious command was run moments later. Suddenly, you don't have three separate pieces of noise — you have a clear signal of an attack in progress.

That's Not Normal: Investigating Incidents

After you've gathered and correlated your data, you can begin the hunt for suspicious activity. The core of modern threat detection is about understanding what's normal for your environment so you can instantly spot what isn't.

To detect something unusual, you first need a solid understanding of what's usual. A CDR platform does this by building a behavioral baseline for every user, role, and resource in your cloud. It learns the typical rhythm of your environment. It knows that your finance team usually accesses the billing database during business hours from the corporate network. It knows that a specific application service only ever communicates with one other database.

With this baseline in place, the system can detect suspicious deviations in real time:

- A user logging in from a new country at 3 a.m.
- A service account suddenly trying to access sensitive customer data it has never touched before.
- A developer account attempting to delete critical audit logs.


TIP

Your cloud environment is always changing, so your baseline of "normal" needs to change with it. A good CDR solution continuously updates its behavioral models to avoid flagging legitimate new activity as a threat.

The Investigator's Playbook: From Anomaly to Investigation

When your system detects a deviation from the baseline, it generates an alert. Now, the real investigation begins. The first step is triage — quickly determining if an alert is a real threat or just a false positive. World-class security analysts do this by asking a series of simple, powerful questions to instantly assess the risk:

- **What is the asset?** The first question is always about the target. An alert on a critical production database containing customer data is infinitely more urgent than an alert on a temporary test server. Understanding the importance of the asset involved tells you how quickly you need to act. A good CDR platform enriches alerts with this context automatically, telling you if an asset is business-critical or contains sensitive data.
- **Who is the user?** Next, you look at the identity involved. An unusual action taken by a cloud administrator with the keys

to the kingdom is a five-alarm fire. The same action taken by an intern with limited access may still be suspicious, but the potential for damage is much lower. Context about the user's role and privilege level is essential for prioritizing alerts.

- **Is this behavior *truly* anomalous?** The system flags behavior that deviates from the established baseline, but an analyst's job is to apply human logic. A developer accessing a new code repository for the first time is technically an anomaly, but it's likely a normal part of their job. That same developer suddenly trying to access the financial database is a major red flag. An analyst must distinguish between activity that is new and activity that is suspicious.
- **What is the "blast radius"?** Finally, you need to assess the potential impact. If an attacker has successfully compromised this asset, what could they do next? The answer to this question — the blast radius — determines the urgency of your response. An alert on a sandboxed test environment has a small blast radius. An alert on a server with broad network access and highly privileged credentials has a massive one.

Assembling the attack timeline

After you've confirmed a real incident, your goal is to understand the full story. The attack timeline is the definitive, chronological record of every action the attacker took, from their initial point of entry to their most recent activity. Building this timeline is one of the most critical parts of an investigation. It helps you understand how the attacker got in, where they've been, and what they're trying to achieve.

REMEMBER

A good timeline is the single source of truth for your entire incident response team. It keeps everyone on the same page and helps new team members get up to speed quickly.

Using the MITRE ATT&CK framework

As you analyze the attacker's actions, you'll want to map them to a standard framework. The MITRE ATT&CK framework is a globally accessible knowledge base of real-world adversary tactics and techniques. Think of it as the ultimate playbook for cyberattacks.

The framework is organized like a matrix. The columns represent tactics — the attacker's high-level goals, like "Initial Access," "Privilege Escalation," or "Exfiltration." The rows contain the specific techniques an attacker may use to achieve those goals, like "Phishing" or "Credential Dumping."

Mapping an incident to the MITRE ATT&CK framework is incredibly valuable. It helps you:

- **Understand the attacker's intent.** By identifying the tactics used, you can better understand what the attacker was trying to accomplish.
- **Identify defensive gaps.** If you see that an attacker successfully used a specific technique, you know you have a gap in your defenses that needs to be addressed.
- **Communicate clearly.** The framework provides a common language for security teams, threat intelligence providers, and executives to talk about threats.

IN THIS CHAPTER

- Acting as a security first responder
- Investigating a crime scene that can disappear
- Automating your response with playbooks
- Fixing the root cause so it never happens again

Chapter 4
Responding to Cloud Threats

In the last chapter, you put on your detective hat. You find the attacker, map out their every move, and understand what they're trying to accomplish. Now, it's time to kick them out and lock the door behind them. But a modern response isn't just about cleaning up a mess. It's about turning a negative event into a powerful opportunity to get stronger.

Turning Attackers into Your Best Pentesters

Here's a perspective that changes everything: Every attack is a free penetration test. An attacker has generously invested their own time and resources to give you a perfect, real-world report on the single weakest point in your defense. A *standard* response is to simply patch that one hole. A *standout* response is to treat the attacker's entire methodology as a gift of valuable data.

This chapter reframes the response process as a powerful feedback loop:

- **Containment is ending the test.** Your first response isn't just putting out a fire. It's stopping the "pentest" before it causes real damage.
- **Forensics is reading the report.** The analysis isn't just a postmortem. It's the process of carefully reading the detailed report the attacker unknowingly wrote for you.
- **Remediation is implementing the findings.** You don't just fix the one window the burglar broke. You analyze their path and realize you need to upgrade the locks on every door and window on that side of the house.

Isolating the Threat

Think of your security team like medical first responders arriving at an accident scene. Their first job isn't to perform complex surgery. It's to stop the bleeding. In cloud security, this is the containment phase. Your primary goal is to stop the attacker in their tracks and prevent them from doing any more harm.

When you have high confidence that a resource is compromised, you need to isolate it immediately. Your goal is to surgically remove the threat from your environment with minimal disruption to your business. A modern cloud detection and response (CDR) platform gives you several scalpels to do this:

- **Network-based isolation:** The quickest way to neutralize a threat is to cut off its network access. By changing a security group or firewall rule, you can instantly sever a compromised workload's connection to the internet and the rest of your cloud environment. This is like putting the attacker in a digital solitary confinement cell. They can't receive any new commands, and more important, they can't send any of your data out.
- **Compute-based isolation:** In the cloud, you can simply shut down or suspend a compromised virtual machine (VM) or container. Suspending a resource is often better than terminating it immediately because it preserves a perfect

snapshot of the machine's memory and disk for your forensic investigation — a crucial piece of evidence.

- **Identity-based isolation:** If you know an attacker has stolen a set of credentials, you can immediately revoke that user's permissions or disable their application programming interface (API) keys. This is like changing the locks the moment you know a key has been stolen, rendering the attacker's primary weapon useless.

REMEMBER

The goal of initial containment is speed. You want to have these actions preconfigured so you can execute them in seconds, not minutes.

Cloud Forensics: Investigating a Crime Scene

After you've contained an immediate threat, the deep investigation begins. In traditional security, this meant unplugging a server and physically taking the hard drive to a lab. In the cloud, the crime scene itself is virtual, and the evidence can vanish in an instant. Cloud forensics requires a completely new set of techniques.

The disappearing evidence

Many cloud resources — especially containers — are ephemeral. They're designed to be created, destroyed, and replaced automatically in seconds. If your response to a compromised container is to simply terminate it, you've also just destroyed all the evidence. It's like the attacker wrote their confession in disappearing ink.

This is why automated evidence collection is critical. A modern CDR playbook doesn't just terminate a suspicious workload. Its first step is to automatically take a forensic snapshot of the workload's memory and disk. The evidence is preserved *before* the resource is destroyed, giving your investigators a perfect copy to analyze.

The dedicated forensic environment

You would never conduct a forensic investigation in the middle of an active crime scene. The same is true in the cloud. You need a dedicated, isolated cloud account that acts as your sterile digital laboratory.

When a snapshot of a compromised machine is taken, it's copied into this clean forensic environment. Here, your analysts can safely "boot up" the compromised disk image, analyze the malware, and trace the attacker's steps without any risk of contaminating your production environment or tipping off the attacker.


TIP

Your forensic environment should be in a completely separate cloud account with its own strict access controls to ensure the integrity of your evidence and prevent cross contamination.

Automating Your Response with Playbooks

In a real incident, you don't want to be figuring out your response plan on the fly. You want to be executing a plan you've already created and practiced. In security, this prebuilt plan is called a *playbook.* A playbook is a detailed, step-by-step set of instructions for responding to a specific type of incident.

In a modern CDR strategy, these playbooks aren't just documents — they're automated workflows. When a specific type of threat is detected, the playbook can execute automatically, performing containment actions much faster and more reliably than any human could.

For example, a playbook for a malware infection may automatically:

1. Isolate the infected workload from the network.
2. Take a forensic snapshot of the memory and disk.
3. Terminate the compromised instance.
4. Send a notification to the security team with a summary of the incident and the actions taken.

Automation frees up your human analysts to focus on the more complex and strategic parts of the investigation, confident that the immediate threat has already been neutralized.

Remediating the Root Cause

Containment stops the attack, but it doesn't fix the vulnerability that allowed the attacker in. Remediation is the process of tracing the attack back to its source and fixing the underlying weakness. The attack path you mapped out in your investigation (see Chapter 3) is your guide. It will lead you directly to the root cause — a vulnerable library that needs to be patched, a misconfiguration that needs to be corrected, or an overly permissive identity that needs to be locked down.

Fixing these issues often involves issuing a *pull request* (PR), a formal request to change the source code or configuration file that contains the vulnerability. This ensures the fix is reviewed, tested, and deployed through your standard development pipeline, preventing the same vulnerability from being reintroduced later.

Proving You're In Shape: Demonstrating Compliance

One of the most powerful side effects of a good CDR program is that it makes proving compliance much easier. Regulations like SOC 2 (short for System and Organization Controls 2), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) require you to demonstrate that you have effective security controls in place. The detailed logs, incident timelines, and documented response actions you generate during your CDR activities are the perfect evidence to satisfy auditors.

Instead of scrambling to find proof that you're secure, you have a constantly updated record of your security posture. A modern CDR platform can even provide prebuilt reports and dashboards that are mapped directly to the requirements of specific regulations, turning a painful, months-long audit process into a simple matter of generating the right report.

IN THIS CHAPTER

- Aligning your security strategy with business goals
- Making your security tools work together
- Building a collaborative cloud defense team
- Following the Crawl, Walk, Run approach to implementation

Chapter 5
Getting Started with Cloud Detection and Response

In the last four chapters, I cover the entire lifecycle of a cloud threat — from prevention and detection to investigation and response. You have the playbook. Now, it's time to put that playbook into action. Getting started with cloud detection and response (CDR) isn't just about buying a new tool. It's about building the digital equivalent of a central nervous system for your cloud environment — a system that can sense, process, and react to threats in real time.

Think of your cloud environment as a living organism. A healthy organism needs a nervous system that can instantly detect when it touches something hot (a threat) and pull its hand away (a response) without having to consciously think about it. A modern CDR program is that nervous system. It provides the sensory input, the processing power, and the automated reflexes to keep your cloud safe. This chapter is your guide to building it.

Aligning with Business Requirements

Before you can build your nervous system, you need to know which parts of the body are most vital. A cut on the finger is a low priority; a threat to the heart is a crisis. In your business, your "crown jewels" — the critical applications and sensitive datastores — are those vital organs.

Your first step is to talk to your organization's leaders and understand their priorities. Are they most concerned with protecting customer data, ensuring the website never goes down, or meeting strict regulatory compliance rules? Knowing what matters most to the business allows you to design a nervous system that is hyperfocused on protecting your most critical assets.

Integrating Cloud Detection and Response with Your Existing Tools

Your new CDR platform isn't an island. It's the central processing unit (CPU) of your nervous system, and it's most powerful when it's connected to the rest of the body.

In Chapter 3, I introduce the "detective with an AI assistant" analogy. In this scenario, your security information and event management (SIEM) platform is the long-term memory, where all evidence is stored for deep analysis. Your security orchestration, automation, and response (SOAR) tool is the muscle memory, the system that executes automated actions. An effective CDR platform acts as the brain that supercharges both:

- **Enriching your SIEM:** Your CDR platform feeds a stream of high-quality, preprocessed signals to your SIEM. Instead of just raw sensory data, your SIEM gets intelligent insights, telling the story of an attack and dramatically reducing the noise.
- **Triggering your SOAR:** Your CDR platform can act as the reflex arc. When it detects a high-confidence threat, it can

automatically trigger a SOAR playbook to execute an immediate response — the digital equivalent of pulling your hand from the fire.

Understanding Roles and Responsibilities

Defending the cloud is a team sport. The old model where a siloed security team throws tickets "over the wall" to developers simply doesn't work. An effective CDR program requires tight collaboration between three key groups. Think of it like a fire department:

- **The fire marshals — cloud security:** This team designs the building codes. They're the architects who create the security policies, design the secure network layouts, and manage the overall security posture to prevent fires from starting.
- **The builders — developers and the development and operations (DevOps) team:** This team constructs the building. They're responsible for writing the code and building the infrastructure according to the fire code. They're the only ones who can fix a structural flaw at its source.
- **The firefighters — the security operations (SecOps) team:** This is your frontline response team. When the alarm rings, they're the ones who rush to the scene, put out the fire, and investigate the cause.

In a modern cloud defense, these three teams work from the same set of blueprints, communicating in real time to contain and remediate threats.

Implementing Best Practices: The Crawl, Walk, Run Approach

As you build out your CDR program, it's helpful to follow a phased approach. You don't need to do everything on day one. You build your capabilities in logical, progressive stages.

Crawl: Master the fundamentals

You can't defend what you can't see. The absolute first action is to gain comprehensive visibility across your entire cloud environment:

- **Create a complete asset inventory.** You need an automated way to know every single workload, identity, and datastore you have.
- **Collect the critical logs.** Start with the highest-value data sources — your cloud provider audit trails and identity logs.

Walk: Build your response muscle

When you can see your environment, you can start defending it:

- **Develop your first detection rules.** Focus on the most critical and obvious threats, like a storage bucket containing sensitive data being made public.
- **Build your first automated playbooks.** Start with simple, high-confidence actions. A great first playbook is one that automatically isolates a workload the moment it's seen communicating with a known malicious Internet Protocol (IP) address.

Run: Become proactive and resilient

With your foundational defenses in place, you can move to a more proactive posture:

- **Measure what matters.** Start tracking your mean time to detect (MTTD) and mean time to respond (MTTR). Your goal is to constantly drive these numbers down.
- **Start threat hunting.** Use the rich data you're collecting to proactively search for signs of threats that your automated rules may have missed.

REMEMBER

It's not just about having a burglar alarm (detection). It's about how fast the police show up after it goes off (response). Both are critical.

Fostering a Security Culture, Not Just a Security Team

Ultimately, the strongest defense is one where every citizen is part of the watch. The most effective way to secure the cloud is to make security a part of everyone's job. A truly mature organization doesn't just have a great security *team* — it has a great security *culture*.

This means empowering developers with the tools and training they need to write secure code from the start. It means conducting blameless postmortems after an incident, where the goal isn't to point fingers, but to understand what part of the *process* failed so it can be improved. And it means celebrating security wins — like when a developer finds and fixes a vulnerability *before* it ever gets to production. When security becomes a shared responsibility, your organization becomes exponentially more resilient.

IN THIS CHAPTER

- Asking the right questions before you buy
- Focusing on context, not just data
- Prioritizing speed and automation
- Ensuring that your tools empower your team

Chapter 6
Ten Things to Look for in a Cloud Detection and Response Solution

In this book, you learn to think like a cloud attacker, a security analyst, and a first responder. You have the strategic frameworks and the tactical knowledge to build a modern cloud defense. Now, it's time to choose your tools. An effective cloud detection and response (CDR) solution is the engine that powers everything covered in this book. This chapter gives you ten key evaluation criteria to keep in mind as you make your decision.

Does It Provide 100 Percent Visibility?

You can't protect what you can't see. A CDR solution is only as good as the data it can access. Your first question should be about the breadth and depth of its visibility. It needs to see every asset in your cloud environment — not just your virtual machines (VMs), but also your containers, serverless functions, identities, datastores, and the control plane itself.


TIP

Look for a solution that uses a combination of agentless scanning for broad coverage and optional agents for deep, real-time workload analysis.

Does It Turn Noise into Signal?

A platform that bombards your team with thousands of low-level, context-free alerts isn't helpful — it's a source of fatigue. A great CDR solution acts as an artificial intelligence (AI) assistant (see Chapter 3), giving your analysts superpowers. It should automatically correlate signals from multiple sources — a risky configuration, a vulnerable workload, and a suspicious identity — into a single, high-fidelity alert that tells the complete story of an attack.

Does It Think Like a Cloud Attacker?

Attackers in the cloud often don't use malware. They abuse legitimate cloud features and compromised identities to achieve their goals. A CDR solution that only looks for known malware signatures is fighting the last war.


TIP

Evaluate whether the platform is built to detect modern, cloud-native attack techniques — like an identity trying to escalate its privileges, a workload accessing sensitive data it has never touched before, or an attacker tampering with your audit logs.

Does It Map Risk to Your Business?

Not all alerts are created equal. A vulnerability on a public-facing server that has access to your customer database is infinitely more critical than a similar vulnerability on an isolated development machine. A standout CDR solution understands this. It should automatically enrich alerts with business context, telling you not just what the risk is, but why it matters.


TIP

Look for a platform that can identify your sensitive datastores and "crown jewel" applications and then prioritize risks based on their potential impact to the business.

Does It Enable a Response at Cloud Speed?

In the cloud, threats move at machine speed, and your response must do the same. This is where the "cattle, not pets" philosophy (see Chapter 2) becomes a technical requirement. Your CDR solution must have robust, flexible automation capabilities. You should be able to build playbooks that can take immediate containment actions — like isolating a workload, revoking credentials, or taking a forensic snapshot — the moment a high-confidence threat is detected.

Does It Help You Investigate a Disappearing Crime Scene?

Cloud evidence is ephemeral (see Chapter 4). A compromised container can be gone in seconds, taking all the forensic data with it. A CDR solution must be built for this reality. It should have built-in, automated capabilities to capture forensic artifacts — like disk and memory snapshots — *before* a compromised resource is terminated. It should also provide a secure, isolated environment for your team to conduct its analysis without contaminating your production environment.

Does It Unite Your Defense Team?

Defending the cloud is a team sport. Your CDR platform should be the common ground where your security architects, security operations (SecOps) team, and developers can collaborate. It should provide a single source of truth that all three teams can use to understand and remediate threats.

WARNING

A solution that forces your teams to work in separate, disconnected tools will only create friction and slow down your response.

Does It Speak the Language of Your Builders?

To truly fix a problem, you need to address its root cause. This often means fixing an issue in the source code or an infrastructure-as-code template. A CDR solution that just creates a ticket saying "vulnerability found" isn't enough.


TIP

Look for a platform that provides developer-friendly remediation guidance. The best solutions will pinpoint the exact line of code that needs to be fixed and even generate a pull request with the suggested change.

Does It Make Compliance an Everyday Activity?

Proving compliance shouldn't be a once-a-year fire drill. An effective CDR platform makes compliance a natural by-product of your daily security operations. It should be able to continuously monitor your environment against common regulatory frameworks — like SOC 2 (short for System and Organization Controls 2), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) — and provide prebuilt reports and dashboards that make it easy to demonstrate your security posture to auditors.

Does It Grow with You?

Your cloud environment and your security program will mature over time. The solution you choose should be able to support you through every stage of that journey. It should be easy to deploy and provide immediate value in the "Crawl" phase, with powerful, advanced features that you can grow into as you "Walk" and "Run" (see Chapter 5). A platform that requires a massive, months-long implementation project will be obsolete before it's even fully deployed.

Glossary

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

artificial intelligence (AI): The ability of a computer to interact with and learn from its environment and to automatically perform actions without being explicitly programmed.

attack surface: The sum total of the devices and connections that threat actors could potentially use to penetrate network defenses.

cloud detection and response (CDR): A security capability that provides real-time visibility, threat detection, and automated response across cloud environments.

cloud workload protection platform (CWPP): A unified cloud security solution that provides continuous threat monitoring and detection for cloud workloads.

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

CloudFormation: A service from Amazon Web Services (AWS) that allows users to model and manage their cloud infrastructure using code. It enables the creation, updating, and deletion of AWS resources in a consistent and automated manner.

compliance: The process of following laws, regulations, and industry standards related to how enterprises handle data, protect systems, and conduct business operations.

continuous integration/continuous deployment (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.

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

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).

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

endpoint detection and response (EDR): EDR focuses on identifying and addressing security threats at the endpoint level, such as laptops, desktops, and mobile devices. EDR solutions continuously monitor endpoint activities and analyze data to detect potential threats in real time.

extended detection and response (XDR): A security solution that uses multiple data sources such as endpoints, networks, identities, and cloud environments to detect and respond to cybersecurity threats.

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.

generative artificial intelligence (GenAI): Artificial intelligence (AI) technology that generates new content. The new content can include text, imagery, and more. New content created by GenAI is based on patterns learned from existing data using unsupervised machine learning (ML) algorithms. *See also* artificial intelligence (AI) and machine learning (ML).

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

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.

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.

indicators of compromise (IoCs): A network or operating system (OS) artifact that provides a high level of confidence that a computer security incident has occurred.

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

Instance Metadata Service Version 1 (IMDSv1): A service from Amazon Web Services (AWS) that helps code access metadata on an Elastic Compute Cloud (EC2) instance, including hostname, security group, hardware address, and more.

least-privilege principle: A principle by which a user or object is assigned only the minimum level of permissions needed to perform an authorized task.

machine learning (ML): A method of data analysis that enables computers to analyze a dataset and automatically perform actions based on the results without being explicitly programmed.

mean time to respond (MTTR): The average time it takes to respond after an incident is detected.

multicloud: 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). It is important to note that although all hybrid cloud environments are also multicloud environments, not all multicloud environments are necessarily hybrid cloud environments. *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 detection and response (NDR): NDR solutions identify and stop evasive network threats that can't be easily blocked using known attack patterns or signatures. NDR uses machine learning (ML) and behavioral analytics to monitor network traffic and develop a baseline of activity.

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.

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

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.

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.

server-side request forgery (SSRF): A web security vulnerability that allows an attacker to cause the application to make requests to an unintended location on the host server.

software composition analysis (SCA): A process used in software security to identify and manage risks associated with open-source components in software applications. SCA helps detect vulnerabilities, ensure license compliance, and generate a software bill of materials (SBOM) that lists all the components used in the software.

tactics, techniques, and procedures (TTPs): The specific methods or activities associated with a threat actor or adversary.

threat hunting: A formal process that attempts to proactively identify adversaries who have already breached defenses and found ways to establish a malicious presence in an organization's network.

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

virtual private network (VPN): An encrypted connection that secures data transmission between devices over the internet.

vulnerability management: The continuous process of identifying, evaluating, prioritizing, and remediating security weaknesses found in your infrastructure.

STOP CLOUD ATTACKS BEFORE THEY BECOME BREACHES

SECURE EVERYTHING RUNNING IN THE CLOUD

Don't wait for a breach to happen.
Outpace your adversary with Cortex® Cloud.

Best-in-class protection backed by 10K detectors and 2.4K+ ML models.

90% reduction in mean time to respond (MTTR)—from days to minutes.

75% reduction in analyst workload through AI-driven automation.

Industry-Leading Cloud Security. Analyst-Validated.

FORRESTER® WAVE LEADER 2024 Cloud Workload Security

Leader in The Forrester Wave™: Cloud Workload Security, Q1 2024 Report

2024 ENTERPRISE MITRE ATT&CK® Evaluations

100% Detection Score in MITRE ATT&CK® Evaluations — No Modifiers or Delayed Detections

GET READY TO PROTECT YOUR CLOUD

Take the interactive product tour:
http://bit.ly/3HnDnnM

Schedule a call with an expert:
https://bit.ly/3EwWFWC

paloalto NETWORKS | CORTEX® CLOUD

Protect your cloud resources

Cloud detection and response (CDR) enables your organization to prevent, detect, and respond to incidents using a comprehensive set of practices. CDR begins with prevention using policies to protect applications, workloads, and application programming interfaces (APIs). You can detect and investigate by combining information from multiple sources to build a picture of the attack, understand how the attack impacts your cloud applications, and identify the root cause or causes that need to be addressed. You can also use automated playbooks to respond to attacks and mitigate vulnerabilities.

Inside…

- Protect your cloud resources with a comprehensive strategy
- Begin by preventing security compromises
- Detect and investigate by integrating multiple sources and signals
- Respond with automated methods to isolate and remediate
- Reduce the time to remediate

paloalto 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.

ISBN: 978-1-394-35437-5
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.