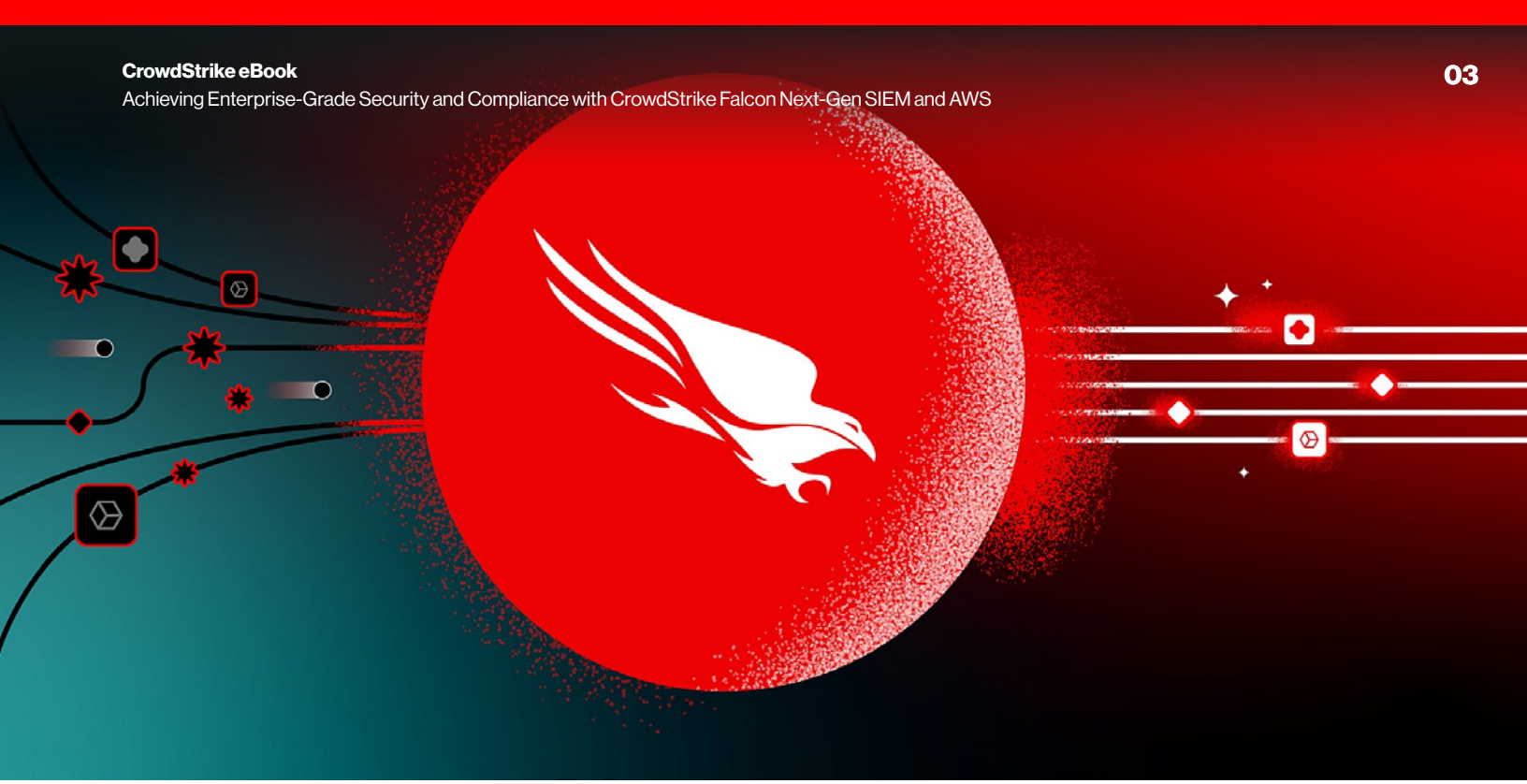
eBook

CROWDSTRIKE

Achieving Enterprise-Grade Security and Compliance with CrowdStrike Falcon Next-Gen SIEM and AWS

Centralize security data to automate threat detection, manage log retention for audits, and simplify compliance across your entire data estate.

Table of Contents



CHAPTER 1

Overcoming visibility gaps and growth barriers in modern security operations

With an average eCrime adversary breakout time of just 29 minutes in 2025,[1] you need a solution that can identify and contain threats before they escalate. But the complexity of cloud footprints can create blind spots, making it challenging to be certain you have the complete picture of your environment. Reducing these risks in organizations that use Amazon Web Services (AWS) with multiple subaccounts demands a visibility layer that updates automatically as you grow.

Traditional security information and event management (SIEM) solutions were built for static, on-premises data. Modern cloud-native security is designed to keep pace with the dynamic speed and high-fidelity telemetry of AWS environments. Failing to account for the dynamic nature of enterprise workloads results in a loss of visibility and a risky security posture that lacks context.

[1] CrowdStrike 2026 Global Threat Report.

CHAPTER 2

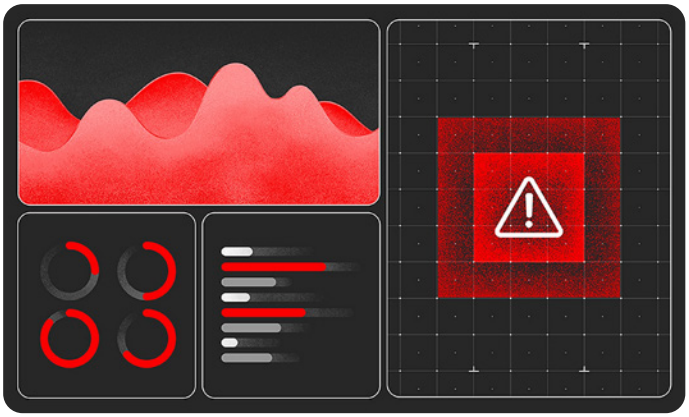
The shift to an outcome-based security platform

To maintain a resilient defense, organizations must understand the fundamental difference between a logging tool and an outcome-based security platform.

While legacy SIEMs focused on manually collecting and storing logs, an outcome-based platform delivers immediate value and visibility into high-value data sources.

When data is siloed, it is nearly impossible to gain a comprehensive view of your security posture or easily address critical compliance questions.

Without a centralized view — and centralized data — your team is left with a collection of noisy alerts, but no clear understanding of how an adversary is operating within your environment.



Modern adversaries outpace legacy SIEMs

29mins

Average eCrime breakout time in 2025[1]

241days

Average time to identify and contain a data breach[2]

2,922

Security alerts received per day by enterprise SOC practitioners and cybersecurity professionals in 2025[3]

2.5hours

Average time per day defenders spend triaging alerts, while 41% of teams spend over 3 hours a day[3]

63%

Percentage of security alerts received that go unaddressed[3]

[1] CrowdStrike 2026 Global Threat Report.
[2] IBM Cost of a Data Breach Report 2025.
[3] Vectra AI 2026 State of Threat Detection and Response Report.

CHAPTER 3

Transitioning to modern security operations

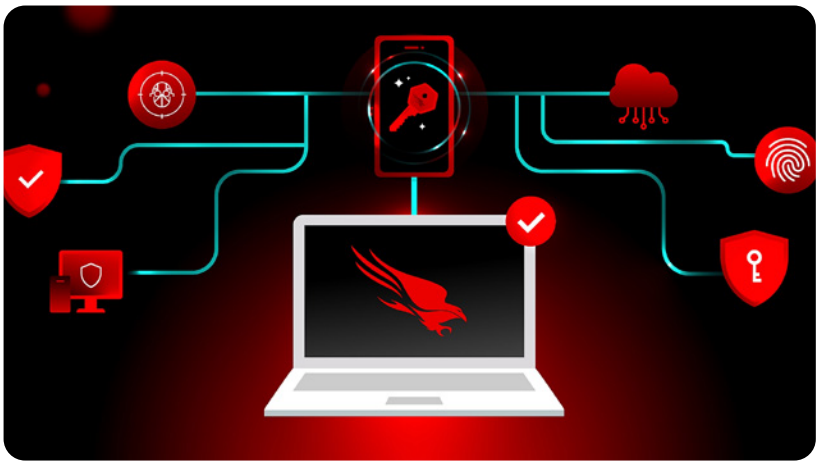
To build a proactive defense, organizations must move beyond passive log archives and adopt a unified approach to security operations. Legacy systems act as passive archives, often requiring manual query writing and hours of data normalization before an analyst can see a clear picture. In contrast, modern operations leverage the speed of index-free search to surface threats in real time.

A unified platform gives you the visibility you need to effectively identify incidents such as stolen credentials, unauthorized resource access, and identity and access management (IAM) privilege escalation.

It allows your team to answer fundamental security questions that legacy tools overlook, such as "How did the attacker move laterally?"

This shift moves beyond simple correlation to automatically enriching events with context. Instead of an analyst receiving three separate, disconnected alerts for a suspicious login — a new process on an EC2 instance and an unusual outbound connection, for example — a unified platform automatically combines these events into a single, chronological story.

By centralizing all telemetry in your environment, you can correlate your AWS data with identity telemetry, firewalls, endpoints, and web proxies to stop an adversary's lateral movement before it can cause harm. Rather than simply logging a security event after the fact, this unified visibility enables your team to detect indicators of attack (IOAs) and disrupt a breach before it results in the exfiltration of intellectual property or sensitive customer data held for ransom.



CHAPTER 4

Ingest and detect: Accelerating the security lifecycle

Modern security operations require a foundation built on real-time visibility and detection. This process begins by combining cross-domain data across your environment into a unified telemetry layer powered by an index-free architecture. By bridging the gap between raw data collection and AI-native analytics, CrowdStrike Falcon® Next-Gen SIEM transforms disparate AWS findings into actionable security context, delivering enterprise-level protection for organizations of any size.

Frictionless data ingestion at scale

A security platform's effectiveness starts with high-throughput ingestion that removes technical friction. While legacy SIEMs often struggle with ingestion bottlenecks, Falcon Next-Gen SIEM offers a one-click deployment experience. This deeply integrated workflow with AWS eliminates the need for manual data engineering or bespoke API configuration.

High-fidelity telemetry from your AWS environment — including AWS CloudTrail, AWS Security Hub, and Amazon GuardDuty — is enabled via native, one-click configuration, making data available for analysis with subsecond latency from the moment it is generated.

Streamline data onboarding

A modern security operations center (SOC) requires a unified view that extends beyond cloud-native findings. Falcon Next-Gen SIEM simplifies this by providing enterprise-grade connectors that bridge the gap between AWS and the rest of your technology stack.

While your AWS telemetry is onboarded via a one-click configuration, the CrowdStrike Falcon® platform also streamlines the ingestion of third-party sources, including firewalls, web proxies, and identity telemetry. Your team no longer needs to build custom connectors, allowing you to achieve unified visibility across your endpoints, identities, and cloud infrastructure through a single, AI-native SOC platform.

Immediate visibility and detection on Day One

Once data is ingested, Falcon Next-Gen SIEM moves on to detection. An effective SIEM is measured not only by the volume of data it can handle, but by its mean time to detect (MTTD). While legacy tools often require months of manual rule tuning, CrowdStrike provides immediate visibility on Day One.

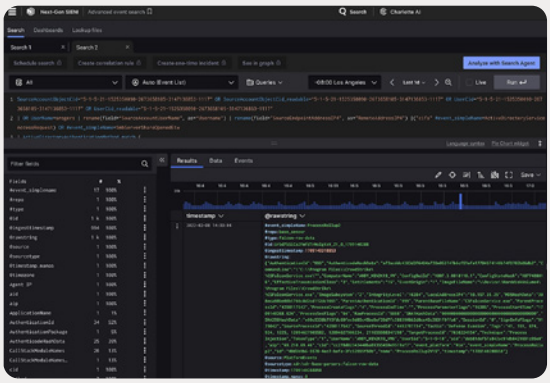
You gain an instant advantage by using the curated list of over 200 AWS-specific templates — prebuilt detections specifically designed to surface complex adversary activity like compromised credentials and credential misuse — selected from CrowdStrike's library of over 1,200 correlation rule templates.

CHAPTER 5

Accelerating investigation with AI-powered visualization

Detection is only half the battle. Beating the 29-minute average eCrime adversary breakout window means lean security teams must move beyond manual triage and fragmented analysis. With cross-domain telemetry unified within the Falcon platform, the focus shifts to investigation, the critical phase where an analyst must quickly understand the scope and intent of a threat.

Transforming flat logs into graph-based content



When an alert is triggered, every second counts. Traditional SIEMs often present a flat list of logs, forcing analysts to piece together a narrative from thousands of lines of raw data. This manual process creates a visibility gap that adversaries exploit to hide their lateral movement.

Falcon Next-Gen SIEM eliminates this friction by leveraging graph-based context to visualize investigations in a unified analyst workbench automatically. Instead of searching through silos, your team sees a visual representation of the incident that illustrates the relationships among associated hosts, identities, and AWS assets.

Root-cause analysis through automated context

By visualizing the attack path, your team can instantly perform root-cause analysis without the need for complex, manual query writing. The platform automatically stitches together disparate signals, such as a suspicious login and a new process on an EC2 instance, into a single, chronological story.

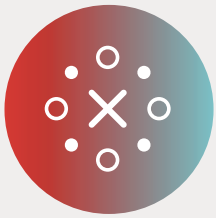
This automated context is further accelerated by the CrowdStrike® Charlotte AI™ agentic security analyst. Charlotte AI reasons through natural-language detections, helping your team summarize complex incidents, generate Falcon platform-native CQL queries, and bridge the gap from initial signal to a definitive response decision in seconds.

CHAPTER 6

Achieving rapid containment with automated response

For smaller security teams, manual intervention for every alert is an unaffordable luxury. Falcon Next-Gen SIEM serves as a force multiplier by integrating CrowdStrike Falcon® Fusion SOAR (security orchestration, automation, and response) directly into the investigation workflow.

Instead of reactive firefighting, your team can deploy no-code, prebuilt SOAR workflows designed to handle common AWS-directed attacks, such as privilege escalation. These automated playbooks can be configured to:

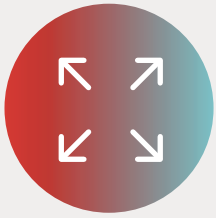


Neutralize compromised credentials

Automatically disable a user's access across AWS and identity providers such as Okta and Microsoft Entra ID if suspicious activity is detected.

Contain unauthorized resource changes

Trigger immediate remediation actions if critical AWS configurations are altered without authorization.



Scale response without adding headcount

Leveraging curated templates to automate repetitive tasks, your team can achieve up to 150x faster search performance thanks to the platform's index-free architecture.[4]

By combining AI-powered visualization with automated response, Falcon Next-Gen SIEM lets you see the attack faster — and stop it before it can move laterally through your environment.

[4] Results are from a customer case study. Individual results may vary.

CHAPTER 7

Supporting compliance through centralized retention

Falcon Next-Gen SIEM leverages a single, AI-native interface to manage both your security operations and your cross-domain telemetry. By consolidating diverse data streams into a single, searchable location, the platform eliminates the historical and operational blind spots that often allow adversaries to remain undetected.

Sustaining long-term audit readiness

Legacy logging tools often fail to provide the long-term visibility required for modern compliance because they are disconnected from the data source. For example, many applications only retain activity logs for 90 days. If an adversary lingers in your environment — or if a regulatory audit requires a look-back at the previous quarter — those 90 days are insufficient.

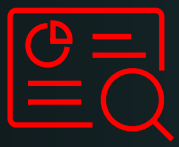
Falcon Next-Gen SIEM closes these historical and operational blind spots by consolidating diverse data streams into a single, searchable location. This unified telemetry enables your team to investigate incidents that occurred months ago, not just weeks ago, helping address stringent log retention requirements for auditors.

By centralizing these high-fidelity sources alongside your AWS telemetry, you move beyond fragmented, siloed logs to a comprehensive posture that helps satisfy both your threat hunters and your auditors.

Key use cases

Identity and access management

Continuous monitoring of providers such as Okta and Microsoft Entra ID helps catch credential theft early.



Productivity suites

Full visibility into platforms such as Slack, Microsoft 365, and Google Workspace enables tracking of data movement.

Compliance monitoring

Out-of-the-box dashboards simplify compliance monitoring, including frameworks like FISMA, GDPR, HIPAA, ISO 27001:2022, NERC CIP, NIST SP 800-53, PCI DSS v4.0.1, and SOX.

CHAPTER 8

Realizing a future-ready security posture

True security resilience requires a platform that scales as fast as your business grows. For rapidly growing organizations, the challenge isn't just managing current data; it's maintaining visibility as you add new AWS services and accounts.

By consolidating your AWS environment and security operations within Falcon Next-Gen SIEM, you can reduce the risks that come with fragmented data and build a foundation for sustainable, long-term growth.

Eliminating complexity

As organizations scale, they often get trapped by fragmentation, creating multiple AWS accounts and deploying niche security tools for each new project. This exponentially increases complexity and exposes visibility gaps, allowing adversaries to exploit the 29-minute average breakout window. You can't protect what you can't see, and a disjointed defense forces analysts to pivot between consoles while adversaries hide their lateral movement in unmonitored accounts.

Automated asset discovery and ingestion

Falcon Next-Gen SIEM solves this fragmentation problem through automated discovery. Designed for the dynamic nature of the cloud, the platform automatically identifies new AWS resources and accounts across your organization as they are created.

Instead of manual onboarding, which is prone to human error and creates risky security delays, Falcon Next-Gen SIEM uses a unified telemetry layer to automatically add and monitor new data sources the moment they go live. This enables your security posture to keep pace with your infrastructure, providing continuous visibility across your expanding digital estate. By replacing a collection of siloed tools with a unified operation, your team can secure your rapid growth without missing a beat.

Next-gen performance, unbeatable value

UP TO **150x**
Faster search to supercharge investigations and hunting[5]

UP TO **70%**
Faster incident response[6]

UP TO **5x**
Faster data streaming[6]

Zero
Upfront costs and pay-as-you-go pricing

[5] Results are from a customer case study. Individual results may vary.
[6] These numbers are projected estimates of average benefit based on the company's own internal analysis and recorded metrics provided by customers during presale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the customer's module deployment and environment.

CHAPTER 9

Achieving operational readiness in minutes

For smaller businesses, the barriers to enterprise-grade security historically have been complexity and cost. Falcon Next-Gen SIEM, available on AWS Marketplace, eliminates these hurdles. You no longer must choose between monitoring a new application and staying within budget.

By leveraging frictionless procurement and CrowdStrike's pay-as-you-go model, the Falcon platform supports enterprise-grade security that is accessible today and sustainable tomorrow.

Falcon Next-Gen SIEM is architected for speed, taking you from procurement to protection in minutes. Leveraging deeply integrated workflows between AWS and CrowdStrike and a "one-click" deployment experience, you can quickly configure and deploy the Falcon platform without complex manual configuration or a pre-existing endpoint sensor.

Data from your AWS deployment — including AWS CloudTrail, AWS Security Hub, and Amazon GuardDuty — is ingested automatically, enabling your organization to get up and running on a platform that easily scales as your business grows.

Falcon Next-Gen SIEM meets you where you are, eliminating upfront costs with pay-as-you-go pricing without long-term contracts. This means you can address your security needs without breaking your budget — regardless of your current toolset — and deploy enterprise-grade connectors without a large security team to oversee them.

Get started today

Falcon Next-Gen SIEM is architected to deliver immediate ROI.

CrowdStrike's 30-day free trial offer and fast, easy deployment — without the need to talk to a salesperson — means you can quickly move from procurement to protection.

Ready to take control of your security and your budget?
Check out the CrowdStrike Falcon Next-Gen SIEM 30-day free trial offer on AWS Marketplace today.

Learn more→

About CrowdStrike
CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/
Follow us: Blog | X | LinkedIn | Instagram
Start a free trial today: https://www.crowdstrike.com/trial