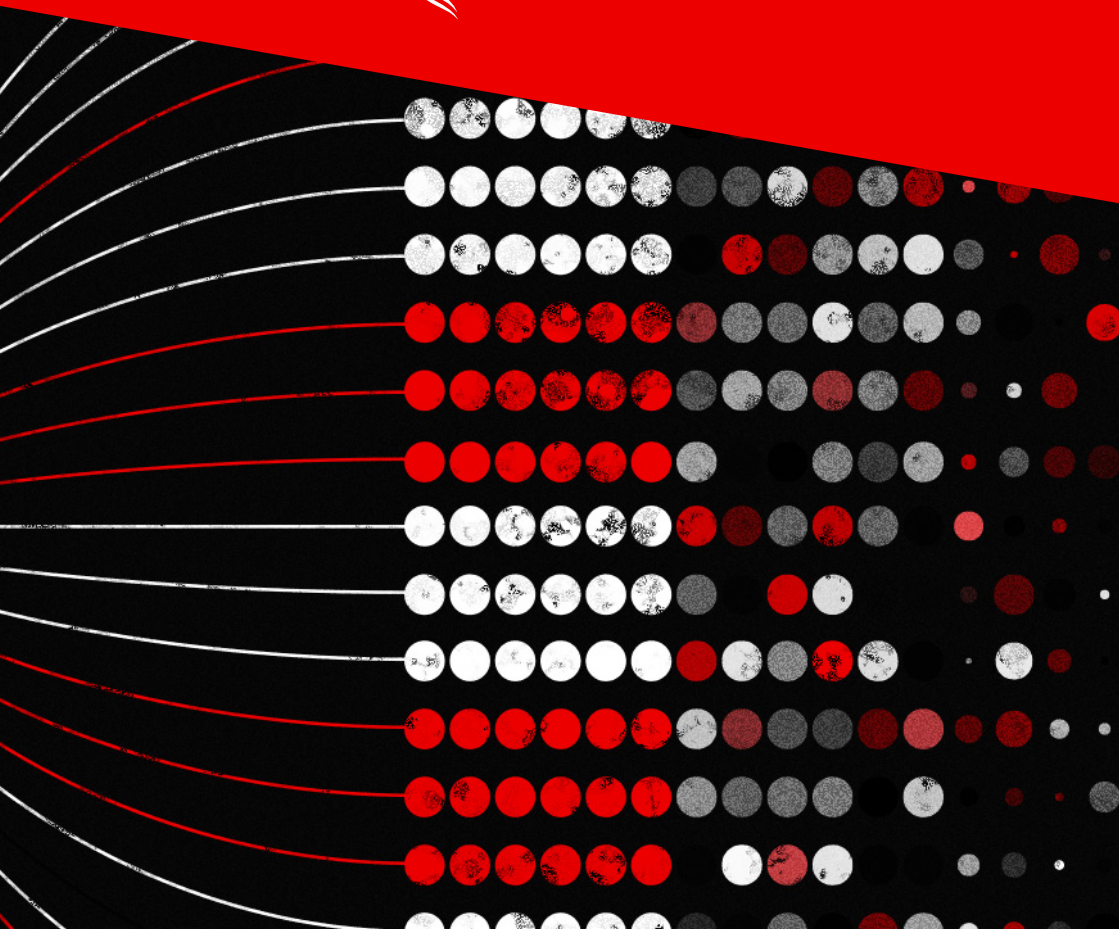
The Complete Guide to Next-Gen SIEM

CROWDSTRIKE



What You'll Learn in This Guide

The Complete Guide to Next-Gen SIEM is your essential resource for understanding security information and event management (SIEM) solutions.

Within these pages, you'll gain insights into how SIEM technologies work and their pivotal role in a SOC. We'll trace the evolution of SIEM from legacy models to next-generation innovations and explore how shifts such as platform consolidation, federated architectures, and the rise of the AI SOC are reshaping core security workflows.

By reading this guide, you'll learn how to:

- **Evaluate the capabilities that matter** as security operations evolve for greater speed, scale, and outcomes engineered for the AI era
- **Prepare your SOC for AI** by understanding how data, automation, and AI agents must come together
- **Choose the right foundation** for modernizing your SOC and supporting what comes next

Read on to see what defines next-gen SIEM — and what it takes to build a modern SOC around it.

Table of Contents

Chapter 1: Legacy SIEM Can't Keep Pace with Modern Adversaries 4

Chapter 2: The Forces Reshaping Security Operations 8

Chapter 3: How to Choose Your Next SIEM 12

Chapter 4: Falcon Next-Gen SIEM Powers SOC Transformation 15

Chapter 1

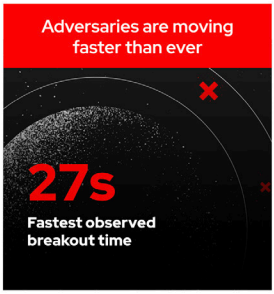
Legacy SIEM Can't Keep Pace with Modern Adversaries

The AI-Accelerated Adversary

Today's attackers are executing increasingly stealthy, high-speed campaigns across a rapidly expanding attack surface, leaving teams using legacy logging tools lagging behind. AI has completely upended how modern threat actors operate, driving an 89% increase in attacks from AI-enabled adversaries in 2025.[1] Adversaries are using AI to accelerate phishing, automate credential-based attacks, and compress the time from initial access to impact, and they are exploiting trusted authentication flows to bypass traditional defenses. Siloed point tools and legacy logging tools miss key pieces of an attack, leaving teams without the critical visibility they need to respond.

AI-accelerated adversaries have pushed the SOC to a breaking point.







[1] CrowdStrike 2026 Global Threat Report

SIEM Evolution

AI is driving today's SOC transformation, but this shift has been building for decades. To understand why a next-gen SIEM represents a paradigm shift rather than just an upgrade, we need to look at how the market has evolved. Exploring this history reveals the limits of past tools and shows why an AI-native approach is the only way to keep pace with today's adversaries.

Phase 1: Early Log Management

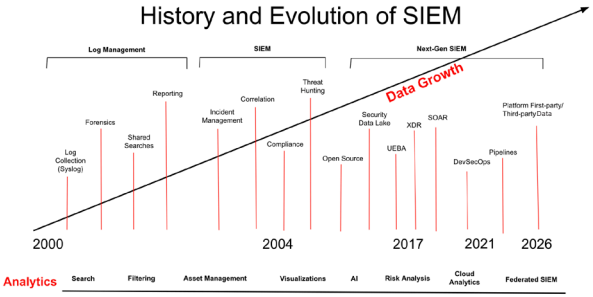
Early SIEM platforms emerged from the need for basic log management. Focused on collecting and indexing logs on-premises via relational databases, these tools were largely used for compliance use cases. They helped organizations meet foundational standards like NIST frameworks and retain data needed for audit or occasional forensic analysis. However, typically deployed on-premises, they faced significant scalability challenges and lacked the advanced correlation needed to detect complex threats.

Phase 2: Scalability and Analytics

As data volumes grew, this phase introduced NoSQL databases to handle increased scale. SIEMs started to become core to the SOC's everyday workflows. Teams also adopted emerging technologies like user and entity behavior analytics (UEBA) and early security orchestration, automation, and response (SOAR). While this era moved SIEMs beyond simple log management toward key threat detection, investigation, and response (TDIR) workflows, these tools still struggled to fully bridge the gaps between disjointed security products.

Phase 3: AI-Native Platforms and Consolidation

Today, SIEM is becoming the foundation of the AI-native SOC. Cloud-native platforms bring together security data and workflows across endpoint, identity, cloud, exposure management, and other domains, replacing fragmented tools with shared context. AI and security agents can then use this context to accelerate investigation and response across the SOC. The result is a SIEM that goes far beyond log management, supporting faster, more coordinated detection, investigation, and response.



Despite major technological leaps in SIEM, the modern SOC is buckling under the weight of fragmented, legacy-driven operations.

Overburdened SOC Teams

The SIEM has long served as the backbone for the SOC, but legacy solutions struggle to keep pace with escalating data volumes and sophisticated threats in modern environments. Key challenges include:

Poor Scalability

Over the last decade, data volumes have surged, a trend further accelerated with AI. Beyond sheer volume, data sources are also increasing in diversity and complexity. Traditional SIEMs, built on rigid, on-premises architectures and legacy indexing, struggle to normalize and correlate these disparate, rapidly changing data streams. These legacy architectures effectively stifle real-time analysis and delay the threat detection that modern environments demand.

Manual, Slow Investigations

Siloed tools bury analysts under a deluge of alerts in their SIEM. Triaging noisy alerts and chasing false positives burns precious analyst time. Pivoting across tools creates "swivel chair syndrome," which contributes to analyst fatigue and often yields inconsistent processes. Sluggish search speeds further delay investigations, turning critical workflows into time-consuming tasks.

27 sec
fastest recorded eCrime breakout time in 2025[2]

2,992
average security alerts received per day in 2025[3]

63%
of security alerts go unaddressed[3]

69%
of organizations use more than 10 detection and response tools[3]

[2] CrowdStrike 2026 Global Threat Report
[3] Vectra 2026 State of Threat Detection

Rising Costs and Complexity

Complexity is the enemy of security. Tool sprawl and exploding data volumes in the SOC have forced teams to adopt convoluted architectures riddled with blind spots. Fragmented data lakes, data duplication, and cloud-attached storage add even further complexity. Meanwhile, security leaders constantly balance trade-offs between cost and visibility.

These challenges have created a breaking point that the modern SOC can no longer ignore.

Chapter 2
The Forces Reshaping Security Operations

Platform consolidation, flexible data architectures, and agentic AI are redefining how security teams collect data, detect threats, and operate the SOC. These shifts are setting a new baseline for what next-gen SIEM must deliver.

From Point Products to Platforms

Over a decade of research by CrowdStrike's frontline teams shows adversaries adapt as defenses evolve. Historically, adversaries often started by attacking the endpoint. As the SOC developed stronger protections, adversaries pivoted from file-based malware drops to stealing credentials. As critical workloads migrated, attackers pivoted again to compromise new cloud infrastructure. Today's attacks are cross-domain, and adversaries live in the gaps between siloed tools.

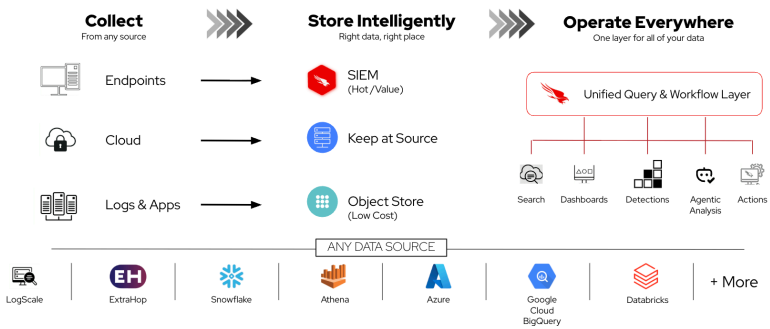
Each tactical shift prompted a new wave of tooling in the SOC, leaving security teams to manage a fragmented ecosystem of point tools. To integrate these in a SIEM, security teams would spend months configuring connectors, mapping schemas, and building custom parsers just to get data flowing.

Cue the rise of integrated SOC platforms. This latest generation of SIEM solutions integrates cross-domain protection for endpoint, identity, cloud, and beyond. In these platforms, key telemetry is available natively, at full fidelity, without incurring any charge for ingestion. When sensors, collectors, detections, and analytics share a common foundation, security data is operational on Day One.

From Centralized Data to Federated Architecture

However, consolidation does not mean centralizing all of your data. The SIEM market is also seeing a fundamental shift in how security data is collected, stored, and accessed. Rather than forcing every dataset into a single repository, modern architectures give teams the flexibility to place data where it makes the most sense based on its value, cost, and use case while maintaining a unified way to search, analyze, and act across it. This creates a distributed data foundation where the SIEM, external storage, and data kept at its source can work together as part of the same security operation.

Federated SIEM Architecture



Organizations are increasingly adopting data pipelines for greater control and precision over ingestion. Before data ever hits the SIEM, teams can decide where to send it based on use case.

- **High-value data:** Ingest into SIEM for active investigations
- **High-volume data:** Keep at the source and retain in a data lake or cloud object storage for later use

SIEMs with federated search capabilities allow analysts to query data as needed, greatly simplifying retention for forensics, audit, or compliance use cases. Together, pipelines and federated search give teams more control over what data they ingest, where they retain it, and how they access it, without requiring every dataset to be centralized in the SIEM.

Pipelines further unlock new possibilities for data architecture. The same pipeline can also route data to multiple destinations based on use case. For example, organizations can leverage one pipeline to send security-relevant telemetry to the SIEM while simultaneously routing data to long-term storage, analytics, or other downstream systems. In the modern SOC, pipelines can detect upstream or on the “edge” with simple analytics for matches on single events or indicators of compromise (IOCs). Teams can filter pass-through alerts and verbose fields to reserve the SIEM for more complex correlation across diverse log sources and/or anomaly detection. Pipelines help SOC teams achieve earlier, faster detection to match adversary speed while effectively managing costs.

From a System of Record to Agentic Security Operations

Transformation does not come from adding stand-alone AI SOC tools to your security stack. Enter the agentic SOC — an essential operating model, not just another product.

Flexible architecture and a consolidated platform lay the foundation for agentic security operations. When integrated with a unified platform, agents can triage detections with greater precision and coordinate multi-domain investigations in parallel. They can even recommend data sources to onboard and automate the process while accessing data in distributed environments via federated connection.

Rather than replacing human analysts, the agentic SOC scales human expertise. Human analysts stay at the center of operations by supervising, evaluating, approving, and orchestrating agent actions, including response. This allows security teams to gain leverage over AI-scale alert volumes without expanding headcount.

Consolidate security context. Architect data for flexibility. Scale expertise with agents.

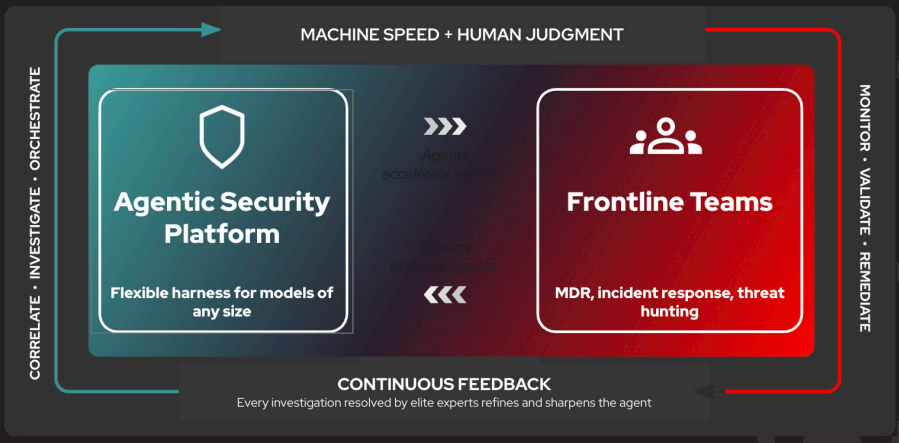
Beyond General-Purpose Models: Why Specialized Intelligence Matters

Raw model size and powerful frontier large language models (LLMs) do not guarantee cybersecurity accuracy. In a high-stakes SOC environment, accurate agentic outcomes require domain-specific precision while maintaining flexibility:

- **Expert-trained intelligence:** Rather than relying on generic model tuning, agents must be trained on validated adversary tradecraft and investigation decisions from top threat experts.
- **Agentic harness:** True agentic operations also demand model flexibility. For instance, small language models (SLMs) are often better suited for narrowly scoped, repetitive tasks common in the SOC, allowing teams to effectively govern agents, manage token spend, and optimize costs by bringing the right tool to every job.

Technology Alone Does Not Transform the SOC

Expert-trained intelligence powers the platform



Chapter 3
How to Choose Your Next SIEM

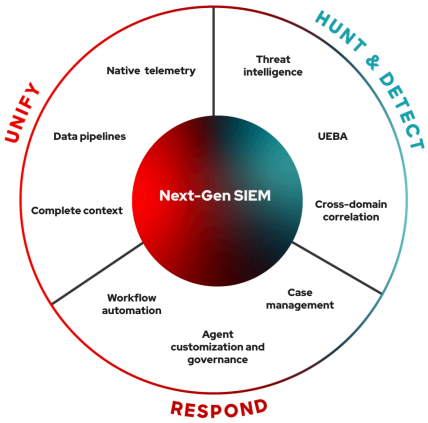
Choosing a SIEM is no longer simply a matter of comparing ingestion costs or ticking the box on individual features. As SIEM shifts beyond a logging solution to the foundation for your agentic SOC, teams need to consider the total value of the platform, cost of ownership, and ROI on security outcomes.

Look for Converged Capabilities

We've already discussed the importance of consolidated, cross-domain telemetry and context. However, it is also critical to understand how to unify workflows across tools throughout the incident life cycle.

Each step of incident response, from triage to remediation, should flow seamlessly into the next. Look for SIEMs that natively combine multiple capabilities: threat intelligence for enrichment, anomaly detection and behavioral analytics for complex attacks, and case management for tracking service-level agreements (SLAs) and assigning work.

As SIEM evolves into the control plane for AI agents, your automation strategy becomes a critical part of choosing the right platform. While some stand-alone SOAR tools offer powerful integrations, SIEM and SOAR increasingly need to come together on a common foundation that can build, manage, and govern AI agents alongside traditional deterministic workflows. As your agentic SOC matures, your team may require additional customization and flexibility, such as the ability to bring your own AI models or bidirectional MCP support.



Use Outcomes to Evaluate Detection and Data Management

Many SIEM evaluations still focus on the wrong measures: more correlation rules, more integrations, more content. Talk to your SIEM engineer to understand the full content life cycle — from migration to building and deploying rules — as well as overhead related to management and maintenance.

For detections, the buying criteria should shift from how many rules a vendor provides to how quickly and reliably new adversary behavior becomes actionable detection content. Look for vendors that continuously translate frontline threat intelligence, hunting, managed detection and response (MDR), and incident response insights into production-ready rules. Some vendors continuously validate and deploy detections automatically in your environment for protection against emerging threats instead of publishing rule templates that the customer must enable themselves.

For data onboarding, recall the importance of pipelines from the previous chapter. Pipelines can drastically simplify onboarding new data sources, but poor integration with the SIEM can introduce new operational overhead. Get ahead of issues with parsers and schema consistency with SIEM solutions that offer a library of certified pipelines with prebuilt, pre-tested data flows by data source and vendor. Look beyond initial setup to how these pipelines are maintained as source formats change so that downstream parsers, detections, and workflows continue to receive the data they expect.

TRADITIONAL BUYING CRITERIA		NEXT-GEN SIEM CRITERIA
How many rules?	→	Who owns keeping them effective?
Do you have threat intel?	→	How quickly does that intelligence become detection content?
Can I customize detections?	→	How much tuning and maintenance falls back on my team?
Do you support this data source?	→	Who keeps the parser and pipeline working when that source changes?

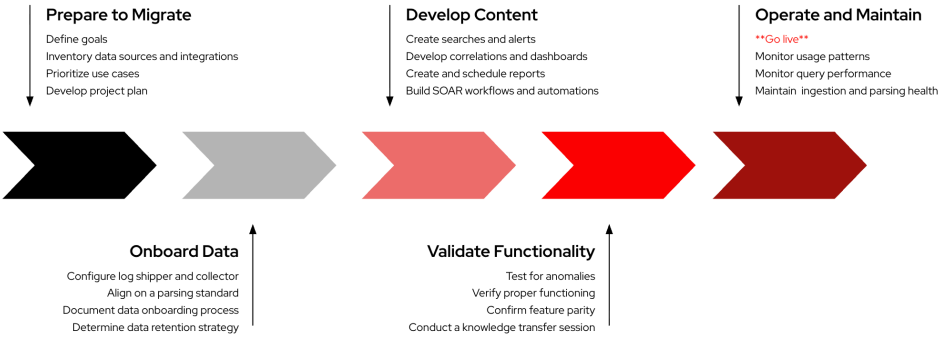
Assess Services and Expertise to Operationalize Your SIEM

SIEM migration, detection tuning, and workflow optimization often stretch internal resources thin. Migration projects extend well beyond moving data. Teams must preserve detections, rebuild workflows, validate functionality, and maintain the environment after cutover.

Learn how services can accelerate deployment and set your SIEM up for success. Some vendors offer dedicated migration services or work with an ecosystem of partners who specialize in SOC transformation. These partners often boast significant experience and expertise across verticals and geographies, and they can look beyond your SIEM to strategize across your whole security stack.

Some SIEM solutions are also paired with managed services for MDR or threat hunting. These services can extend internal teams with 24/7 monitoring, threat hunting, and response. As discussed previously, your SIEM platform is the foundation for workflows across the SOC, including these service providers. When evaluating managed services, ensure you are investing in not just an overlay but a team of experts that is well-versed in the underlying technology.

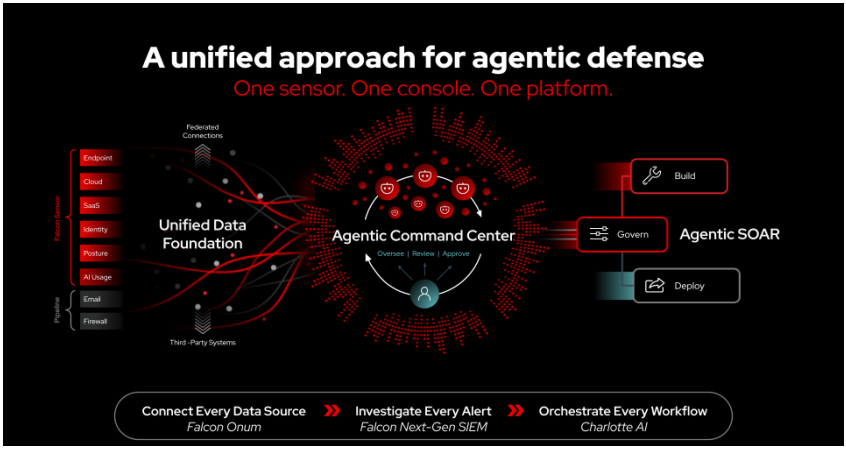
SIEM Migration Best Practices



Ultimately, choosing a next-gen SIEM means evaluating far more than the technology itself. Architecture, economics, detection efficacy, ecosystem, and services all shape whether a platform can deliver meaningful SOC transformation. The right choice should reduce complexity today while giving the organization a foundation that can evolve with the SOC.

Chapter 4
Falcon Next-Gen SIEM Powers SOC Transformation

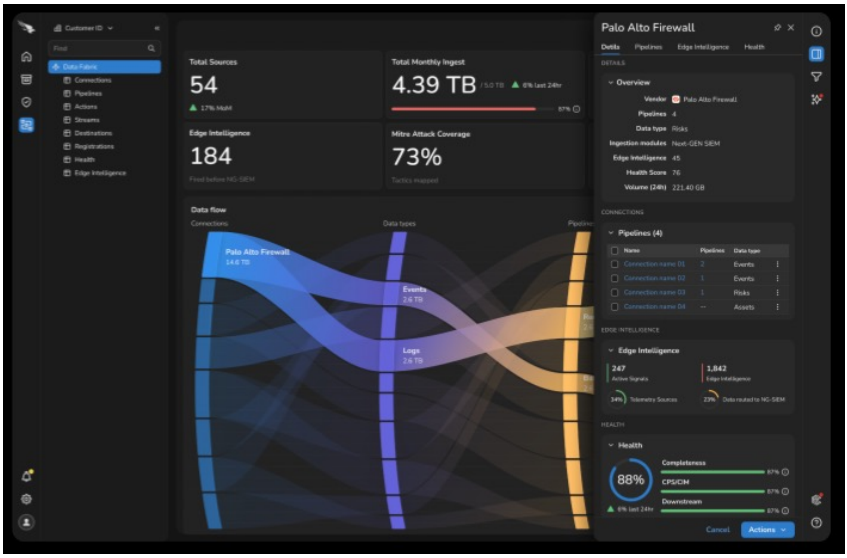
The Foundation for the Agentic SOC



We've established what modern security operations require: unified data and context, flexible data architecture, and AI that can reason and act across your environment. We've also talked about how to refresh your SIEM buying criteria to set you up for success with a next-gen SIEM.

CrowdStrike brings these elements together on the CrowdStrike Falcon® platform. CrowdStrike Falcon® Next-Gen SIEM is the engine of the agentic SOC, connecting security data, detections, investigations, and response on a common foundation built to stop breaches — not simply log them.

Connect Every Data Source



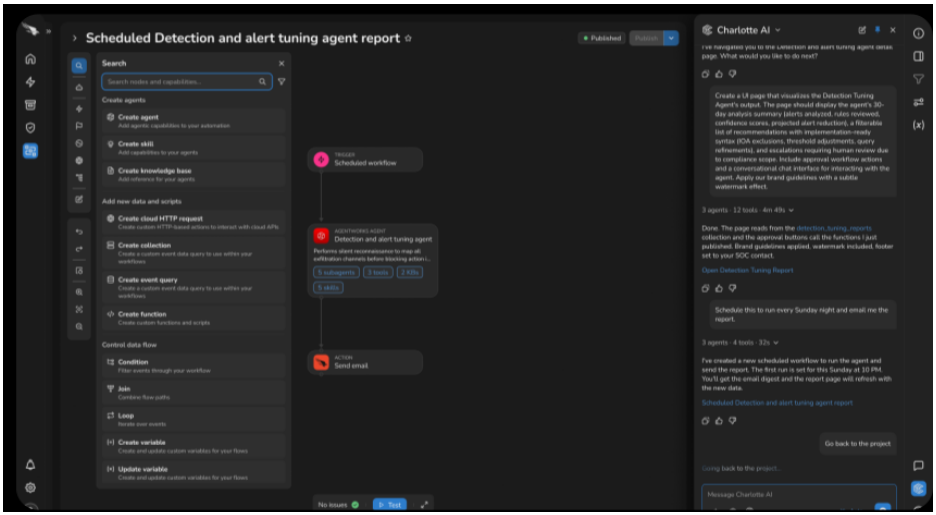
- **Ingest telemetry seamlessly:** Falcon platform data is already available natively in Falcon Next-Gen SIEM, eliminating the ingestion and integration work traditionally required to operationalize core security telemetry.
- **Extend visibility with real-time pipelines:** CrowdStrike Falcon® Onum extends this foundation with real-time pipelines to collect and route third-party data, giving teams greater control over how telemetry flows into Falcon Next-Gen SIEM and other destinations.
- **Access distributed data via federated search:** Federated search gives teams access to data in CrowdStrike Falcon® LogScale™ and external stores such as S3 and Snowflake without requiring every dataset to be centralized. This gives teams flexibility to keep data in the storage tier that makes sense for the use case while preserving access for investigation and hunting.
- **Unify third-party security telemetry:** Bring telemetry from third-party security tools into Falcon Next-Gen SIEM alongside native Falcon platform data to correlate activity and investigate threats across a heterogeneous environment.

Investigate Every Alert



- **Correlate signals across domains:** Adversary-driven detection content correlates signals across endpoint, cloud, identity, network, and third-party data to uncover cross-domain attacks.
- **Accelerate investigations with expert agents:** Expert agents — the same used by CrowdStrike Falcon® Complete — work in parallel across domains. These agents build on shared context to converge on a unified verdict, with accuracy that sharpens as they learn your environment.
- **Automatically assemble complete context:** See the full attack path, search across petabytes of data, and bring related detections into a single case for faster, more confident decisions.

Orchestrate Every Workflow



- **Unify your automation canvas:** CrowdStrike® Charlotte Agentic SOAR brings apps, deterministic workflows, and agents onto the same foundation as detection and investigation.
- **Build and govern custom agents:** CrowdStrike® Charlotte AI™ AgentWorks lets teams create, test, and deploy agents for their own SOC use cases, with controls for governance and scale.
- **Choose the right model for the task:** Expanded model optionality lets teams use supported OpenAI and Anthropic models.
- **Connect agents across your stack:** Bidirectional MCP support lets third-party agents access Falcon platform tools while AgentWorks agents connect to external tools and data.
- **Scale response across the ecosystem:** Prebuilt playbooks and thousands of response actions extend automation across security and IT tools, helping teams contain threats and orchestrate response without starting from scratch.

Transform with Confidence

- **Simplify migration and implementation:** CrowdStrike Services helps teams migrate from legacy SIEMs, onboard data, and operationalize new workflows.
- **Extend your team with 24/7 protection:** Falcon Complete provides MDR and full-cycle remediation for organizations that need additional operational capacity.

Step into the Future of Security Operations

> "We're on the precipice of another major leap with [Falcon Next-Gen SIEM]. It's at least ten times faster than what we had before. The performance improvements have been game-changing, allowing us to instantly ingest Falcon platform data and third-party data for the ultimate visibility and threat hunting."
>
> — Steve McIntosh, Director of Threat Management and Response at Aflac

Put the Agentic SOC into Action

You've seen what it takes to build the foundation for modern, AI-powered security operations. Now experience it firsthand.

Join an Agentic SOC hands-on workshop to see how CrowdStrike unifies security data, accelerates investigation with AI, and orchestrates response at machine speed — while keeping humans in control.

Join a Hands-on Workshop

Want to see how this could work in your environment?

Request a Demo

150x
Faster search speeds vs. legacy SIEMs[4]

15+
Point tools consolidated over time[5]

95%
Reduction in false positives[6]

[4] Results are from a case study. Individual results may vary.
[5] Results from an individual customer
[6] Results from an individual customer

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/

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

© 2026 CrowdStrike, Inc. All rights reserved.