

Falcon Next-Gen SIEM: Take the Next Step to Transform Your SOC

One platform to stop breaches

If you currently use CrowdStrike Falcon® Insight XDR, you can easily apply the power of the leading CrowdStrike Falcon® platform to all data sources with CrowdStrike Falcon® Next-Gen SIEM. Key Falcon data from endpoint, threat intelligence, identity, cloud, and more can be readily correlated with data from third-party tools for unparalleled visibility across your entire environment. Break down data silos and eliminate blind spots by unifying your security data with the Falcon platform. When the vast majority of data needed for SIEM use cases comes from CrowdStrike, why send it anywhere else?

Step into the future of security today

Falcon Next-Gen SIEM delivers unmatched security and operational efficiency, making it the ideal choice for CrowdStrike Falcon users. Here's what you'll gain:

- **Seamless data onboarding** with your Falcon data already in the platform
- **Rapid deployment** up to 3x faster than other solutions, further accelerated by expert services¹
- **AI-led investigations** including incident summaries, real-time collaboration, and incident visualization
- **Blazing-fast search** up to 150x faster than legacy SIEMs¹
- **24/7 expert protection and full-cycle remediation** with Falcon Complete Next-Gen MDR
- **Up to 80% cost savings** compared to siloed solutions²

**Get Started Today
with 10GB/day of
Free Third-Party
Data Ingestion**

All Falcon Insight XDR customers have 10GB/day of free third-party data ingestion. Broaden your visibility, streamline operations, and drive better security outcomes — all at no additional cost.

[Get started now](#)

¹ Results are from a customer. Individual results may vary.

² This is the projected estimate of average benefit based on recorded metrics provided by customers.

Extend beyond Falcon Insight XDR with Falcon Next-Gen SIEM

	Falcon Insight XDR	Falcon Next-Gen SIEM
Log Management and Ingestion		
Comprehensive endpoint telemetry collection	✓	✓
Third-party data ingestion	✓ Up to 10GB/day	✓
Prebuilt connectors and parsers	✓ Up to 10GB/day	✓
AI-generated parsers	✓	✓
Data pipeline	-	With Falcon Onum ³
Data retention	✓ 7 days	✓ Up to 5 years ³
Security Monitoring and Detections		
Security alerts	✓	✓ Extends to third-party data
Dashboards and visualizations	✓	✓ Extends to third-party data
Machine learning-powered detections	✓	✓ Extends to third-party data
Correlation rules to detect cross-domain attacks	✓	✓ Extends to third-party data
Behavioral indicators	✓	✓ Includes identity risk factors
Entity enrichment	✓ Host context only	✓ Host and user context
Search and Investigation		
Scalable, highly efficient search	✓	✓ Extends to third-party data
Visualization and case management in Workbench	✓	✓ Extends to third-party data
AI-powered incident summaries	With Charlotte AI ³	✓ Includes free monthly Charlotte AI entitlements

³ Add-on available for additional purchase.

	Falcon Insight XDR	Falcon Next-Gen SIEM
Prevention and Automated Response		
Real-time response actions on the endpoint (e.g., network isolation, quarantine, etc.)	✓	✓
Automated workflow actions and playbook templates	✓ Applicable to first-party and utility/ITSM tools (100+ actions)	✓ Extends to third-party tools (2,500+ additional actions)
Custom app creation with Falcon Foundry	✓ Up to 1 app	✓ Includes fixed number of apps ³
LLM-to-Fusion actions in Falcon Fusion SOAR workflows	With Charlotte AI ³	✓ Includes free monthly Charlotte AI entitlements
Charlotte AI Agents		
Turnkey AI agents for data transformation, search analysis, correlation rule generation, Falcon Foundry app generation, and more	With Charlotte AI ³	✓ Includes free monthly Charlotte AI entitlements
Add-on Expert Services³		
Managed threat hunting with CrowdStrike Falcon® Adversary OverWatch™	✓ For endpoint, identity, and cloud	✓ Extends to third-party data
Managed detection and response (MDR) with CrowdStrike Falcon® Complete Next-Gen MDR	✓ For endpoint, identity, and cloud	✓ Extends to third-party data
Operational Support Objective-based support for deployment, configuration, content development, and operationalization of Falcon Next-Gen SIEM	✓ For endpoint, identity, and cloud	✓ Options include fixed number of log sources and queries
Resident Engineers Time-based staff augmentation that leads the deployment, configuration, and support for Falcon Next-Gen SIEM	-	✓ Options include fixed number of log sources and queries
Resident Responder Time-based staff augmentation that assists your SOC, intelligence, and threat hunting teams using Falcon Next-Gen SIEM	-	✓ Options include fixed number of log sources and queries

³ Add-on available for additional purchase.

"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. We've had a lot of success pulling our data together."

– Steve McIntosh, Director of Threat Management and Response at Aflac

Ready to take the next step?

Learn how to get started with Falcon Next-Gen SIEM today and enjoy 10GB/day of free third-party data ingestion for all Falcon Insight XDR customers, at no additional cost. For higher data volumes and retention periods, talk to your account team to explore an upgrade to a full Falcon Next-Gen SIEM subscription.

[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.

