

# Migrating from Splunk Using Falcon Platform Services

Accelerate your move from Splunk to Falcon Next-Gen SIEM — built to stop breaches, not just log them

## Splunk complexity slows teams down

Organizations running legacy SIEMs often struggle with rising costs, complex ingestion, and limited visibility across endpoint, identity, and cloud environments. As data volumes grow and threats span across domains, legacy architectures make it difficult to:

- Achieve end-to-end visibility across the entire security stack
- Control unpredictable licensing and infrastructure spend
- Obtain the full context needed for analysts to rapidly investigate and respond to threats

[CrowdStrike Falcon Platform Services for Next-Gen SIEM](#) ensures smooth transition from a legacy log management tool to an AI-native platform, purpose-built to stop breaches. Falcon Next-Gen SIEM delivers the engine for SOC transformation that collapses silos, eliminates ingestion complexity, and accelerates detection and response with adversary-driven precision — helping teams outpace modern threats from Day One. With the support of tailored services and deep security expertise, organizations can realize greater security ROI, operationalize tools more quickly, and confidently modernize their SOC for the AI era.

## Leading organizations transform their SOC with CrowdStrike

### Case Study 1: Global Food Manufacturer

#### From fragmented visibility to identity-driven detection and automated response

A Fortune 500 packaged foods manufacturer with ~14,000 employees operating globally was a heavy Splunk user but struggled with search performance and scalability. The company relied significantly on Active Directory (AD) and struggled with inconsistent identity visibility across regions.

#### Goals

- Accelerate identity-based detections
- Automate AD and Microsoft Entra ID response workflows
- Simplify onboarding of log sources

## Key benefits

### » Reduce time-to-value and accelerate ROI:

Quickly unlock the full power of the CrowdStrike Falcon® platform and Falcon Next-Gen SIEM with expert deployment, providing faster security impact and improved ROI.

### » Reduce deployment complexity: Let CrowdStrike assist with onboarding and setup so your team stays focused on security while the Falcon platform is seamlessly deployed.

### » Maximize protection: Enhance your security posture and optimize your protection with configuration based on best practices across thousands of customers.

### » Customize and tailor based on your needs: Expert teams focus on your goals to improve detection fidelity, streamline investigation, and automate response based on your environment, data, and risks.

#### CrowdStrike Delivered

- High-fidelity AD and identity detections to identify Kerberoasting, domain admin changes, and short-lived accounts
- SOAR-driven identity workflows such as token recycling and risky-user enforcement
- Rapid onboarding and unified identity and endpoint visibility

#### Outcome

- **50% cost savings** with reduced overages and improved budgeting from more predictable logging costs<sup>1</sup>
- **Efficiency:** Consolidated multiple tools with SIEM, SOAR, endpoint, identity, and threat intelligence in a single platform

## Case Study 2: Multinational Energy Provider

### Eliminating silos for comprehensive visibility that extends to the cloud

A global energy company spun off a division that needed to rebuild its SOC from the ground up with limited resources and headcount. It needed to move from Splunk to a more modern, agile solution that delivers value quickly.

#### Goals

- Unify visibility across vulnerability, identity, and cloud domains
- Simplify parsing and ingestion

#### CrowdStrike Delivered

- Significantly simplified ingestion using data from the Falcon platform and modules, including CrowdStrike Falcon® Exposure Management, CrowdStrike Falcon® Cloud Security, CrowdStrike Falcon® Adversary Intelligence, and Falcon Next-Gen SIEM
- Managed detection and response (MDR) with CrowdStrike Falcon® Complete Next-Gen MDR and managed threat hunting services with CrowdStrike Falcon® Adversary OverWatch™
- Parser creation and automation enablement

#### Outcome

- **Efficiency and ROI:** Projected benefits of over **\$6M** over the contract term by augmenting staff skills and expertise and increasing efficiency and efficacy<sup>2</sup>
- **Consolidation:** A unified platform with identity, cloud, and exposure management

---

<sup>1</sup> Results are based on metrics reported by a customer following deployment of CrowdStrike modules. Results may vary depending on customer environment and use case.

<sup>2</sup> These numbers are projected estimates of average benefit based on the company's own internal analysis and recorded metrics provided by customers during pre-sale 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.

## Case Study 3: Global Pharmaceutical Company

### Modernizing SecOps with advanced detections and SOAR playbooks

A global pharmaceutical organization with ~13,000 employees and a mature SOC faced significant complexity in its migration. Its Splunk environment included dozens of custom detections and complex SOAR enrichment workflows.

#### Goals

- Improve search performance
- Re-platform complex detection logic
- Modernize SOAR investigation and enrichment pipelines

#### CrowdStrike Delivered

- High-performance searching without prebuilt data models
- Recreated critical detection patterns in Falcon Next-Gen SIEM
- SOAR pipelines aligned to identity, threat intelligence, and endpoint activity

#### Outcome

- **SOC Transformation:** Strengthened detection posture by modernizing **60%** of legacy correlation rules<sup>3</sup>
- **Improved ROI:** Reduced logging costs by **20%** while expanding visibility<sup>4</sup>

## Best practices for a successful SIEM migration

### 1. Define your goals

Evaluate your existing SIEM to identify any pain points, such as performance issues, gaps in data coverage, or difficulties in threat detection and response. [Learn more](#) about strategic planning and key steps to prepare.

### 2. Inventory what is actually used today

Work within and across teams to understand which detections, dashboards, queries, and SOAR playbooks are used most often and carry the greatest security impact for the business.

### 3. Leverage platform data and pipelines

The Falcon platform already contains critical data like endpoint, cloud, identity, and more. Simplify ingestion from third-party tools with a data pipeline like [CrowdStrike Falcon® Onum](#).

### 4. Match the migration approach to SOC maturity

For customers with limited resources and expertise, leverage managed services like [Falcon Complete Next-Gen MDR](#) to get more value from your SIEM.

<sup>3</sup> Results are based on metrics reported by the customer following deployment of CrowdStrike modules. Results may vary depending on customer environment and use case.

<sup>4</sup> Results are based on metrics reported by the customer following deployment of CrowdStrike modules. Results may vary depending on customer environment and use case.

## Ready to learn more?

Talk to our experts to learn more about Splunk migration today.

Contact Us

## 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: [www.crowdstrike.com/services/](https://www.crowdstrike.com/services/)

Email: [services@crowdstrike.com](mailto:services@crowdstrike.com)

