vijilan
IT Security: Enabled

ARCSIGHT VS. FALCON NEXT-GEN SIEM COMPARISON

A Head-to-Head Analysis Across 12 Key Security Criteria

Organizations modernizing their security operations often compare ArcSight with Falcon Next-Gen SIEM. Both platforms provide SIEM capabilities for threat detection, log analytics, and security monitoring. However, they differ significantly in architecture, deployment model, operational complexity, and integration with modern security ecosystems.

This comparison evaluates how each platform performs across 12 key criteria including pricing, performance, deployment, AI capabilities, XDR integration, and managed service readiness.

AT-A-GLANCE COMPARISON

Criteria	ArcSight	Falcon Next-Gen SIEM
Architecture	Traditional SIEM platform designed for enterprise environments	Cloud-native platform built on the CrowdStrike Security Cloud
Primary Focus	Log management, compliance monitoring, and threat detection	Security-first SIEM with deep endpoint telemetry
Deployment	Supports on-premise, hybrid, and cloud deployments	Fully SaaS-based deployment
Data Ingestion	Extensive log ingestion across network devices, servers, and applications	Optimized ingestion from Falcon telemetry and integrations
Performance	Mature correlation engine designed for large enterprise environments	High-speed threat detection powered by native telemetry
AI & Detection	Rule-based correlation and analytics capabilities	AI-driven behavioral detection with integrated threat intelligence
Threat Detection	Advanced correlation rules across multiple data sources	Detection powered by Falcon intelligence and endpoint visibility
XDR Integration	Integrates with various third-party security tools	Native integration across Falcon security modules
Scalability	Built for large enterprise infrastructures	Highly scalable cloud-native architecture
Pricing Model	Often based on event volume, infrastructure, and licensing	Flexible pricing aligned with Falcon platform usage
Security Ecosystem	Integrations across traditional enterprise security environments	Deep integration within the Falcon ecosystem
Managed Service Compatibility	Often supported by MSSPs or internal SOC teams	Frequently paired with managed SOC and MDR services

Key Takeaways

ArcSight

Best suited for organizations that need:

- A mature enterprise SIEM platform
- Flexible deployment options including on-premise environments
- Strong correlation capabilities across large infrastructures

Falcon Next-Gen SIEM

Best suited for organizations that want:

- A cloud-native SIEM platform with faster deployment
- AI-driven detection powered by endpoint telemetry
- Tight integration with a unified security platform

Effective Security Requires More Than a SIEM Platform

Even advanced SIEM platforms require ongoing expertise to maintain effective protection. Organizations must ensure:

- Continuous security monitoring
- Expert threat investigation
- Rapid incident response
- Continuous tuning of detection rules and analytics

Without dedicated security operations resources, many organizations struggle to fully maximize the value of their SIEM investments.

Strengthen Your SIEM with Expert SOC Support

Vijilan Security helps organizations maximize their SIEM investments through 24/7 monitoring, expert threat analysis, and rapid incident response.

Our team helps organizations deploy, manage, and optimize modern SIEM platforms while maintaining continuous visibility into evolving cyber threats.

MODERNIZE YOUR SIEM STRATEGY WITH EXPERT GUIDANCE

Whether you are evaluating ArcSight, Falcon Next-Gen SIEM, or planning a SIEM modernization initiative, expert guidance can help ensure your security operations remain effective and resilient.

TALK TO A SECURITY EXPERT TODAY

Discover how Vijilan Security can help you evaluate, deploy, and optimize your SIEM strategy.

SCHEDULE A CONSULTATION

info@vijilan.com www.vijilan.com +1 (954) 334-9988

AICPA SOC
ISO 27001
A-LIGN