CROWDSTRIKE

CrowdStrike Announces the Falcon Next-Gen SIEM ISV Ecosystem, Open to Integrating the Most Third-Party Data Sources to Power the AI-Native SOC

Ecosystem open to connecting data from AWS, Cloudflare, Cribl, ExtraHop, Okta, Rubrik, Zscaler and 500+ ISVs with Falcon platform data, AI and workflow automation to centralize insights and supercharge stopping breaches

AUSTIN, Texas--(BUSINESS WIRE)--May 7, 2024-- **RSA Conference 2024 – May 7, 2024** – CrowdStrike (NASDAQ: CRWD) today announced that CrowdStrike Falcon® Next-Gen SIEM now supports the largest ecosystem of ISV data sources of any pure-play cybersecurity vendor. Data from Amazon Web Services (AWS), Cloudflare, Cribl, ExtraHop, Okta, Rubrik, Zscaler and over 500 security and IT leaders can be seamlessly integrated with Falcon platform data, threat intelligence, AI and workflow automation to power the AI-native SOC and provide security teams with the centralized insights they need to stop breaches faster than ever before.

Security operations are a data problem. The growing number of security and IT solutions in enterprise environments makes it increasingly difficult to solve. Multiple agents, disparate consoles and piecemeal workflows create data silos which require excess human integration and operational investment. Legacy SIEMs attempted to stitch data together, serving as point-in-time relief from a chronic problem. In today's AI-powered enterprise, the legacy SIEM is no longer effective, creating blind spots, prolonging investigations and preventing security teams from matching adversary speeds. Legacy data schemas complicate ingesting ever-expanding data sources. Running modern security and IT operations requires a fundamentally different AI platform approach to ingestion, analytics and response orchestration. Most importantly, it requires the foundational ecosystem of data content from the tools used by enterprises across the globe.

The CrowdStrike Falcon Next-Gen SIEM ISV ecosystem allows security teams to seamlessly ingest, retain, search and analyze data from over 500 sources. This, combined with Falcon data, threat intelligence, AI and workflow automation, advances the AI-native SOC and provides security teams with unmatched speed and accuracy to stop breaches.

"CrowdStrike's customer base, more than 500 supported integrations and diverse partner base creates unparalleled data gravity, putting us in the driver's seat to create and lead the next-gen SIEM market," said Daniel Bernard, chief business officer, CrowdStrike. "The AI-powered Falcon XDR platform – which welcomes third-party data – differentiates our approach. Together with our hundreds of ISV partners, we're revolutionizing SIEM, combining an AI-native platform approach with the diverse data sources sought by the enterprise. The ability to bring any data in, instantly gain insight and automate orchestrated responses is the next-gen SIEM game changer today's enterprises need."

500+ data sources. Faster detection and response.

Falcon Next-Gen SIEM is open to supporting over 500 ISV data sources with integrations available through the CrowdStrike Marketplace and CrowdStrike Github. Historical and real-time data is correlated and enriched with massive amounts of Falcon data, threat intelligence, AI and workflow automation to provide security teams with the most comprehensive understanding of threat activity across environments and rapidly respond. The CrowdStrike ecosystem includes security and IT leaders spanning cloud, web, email, identity, network, OT and IT operations, including:

- **AI Computing:** Intel, NVIDIA
- **Asset Management/Patch Management:** Adaptiva, InfoSec Global, JumpCloud, Sevco Security
- **Cloud/Infrastructure**: Amazon Web Services (AWS), Citrix, Dell, Docker, Google Cloud, Kubernetes, Microsoft Azure, Nutanix, Red Hat, VMware
- **Compliance, Policy and Risk Management:** Cado Security, Discern Security, DTEX Systems, Elevate Security, Vanta, X-Analytics
- **Data Protection:** appNovi, Concentric AI, Forcepoint
- **Data Security/Data Management**: Cohesity, Dell EMC Data Domain, Rubrik, Tausight, Veritas
- **DevOps:** GitHub, Red Hat Ansible, Salt, Terraform by HashiCorp
- **DNS/DHCP:** Infoblox, Microsoft DNS/DHCP
- **Email Security**: Abnormal Security, Egress, Menlo Security, Mimecast, Perception Point, Proofpoint
- **Enterprise Browser:** Google Chrome Enterprise, Island, Talon by Palo Alto Networks
- **Firewall/Network**: Akamai Technologies, Axiomatics, Check Point Software, Cisco, F5 Networks, Fortinet, HPE Aruba Networking, Imperva, InfoExpress, Juniper Networks, Netgate, Palo Alto Networks, Trellix
- **Identity/SSO**: 1Password, Aembit, Beyond Identity, Cisco Duo, Cyberark, ForgeRock, Microsoft 365, Okta, OneIdentity, Ping Identity, Rezonate, StrongDM, TruU, Veza Technologies
- **IT/OT**: Armis, Asimily, Claroty, Dragos, Nozomi, Ordr, ServiceNow, Zoom
- **Microsegmentation:** Akamai, ForeScout, TrueFort
- **Mobile Security/Device Management:** Ivanti, Lookout
- **NDR/CDR**: Arista Networks, Corelight, Darktrace, ExtraHop, Gigamon, IronNet, Lumu, ThreatWarrior, Vectra AI
- **Observability and Data Management**: Chronosphere, Cribl, IBM Instana Observability
- **Operating Systems:** Apple MacOS, Google Chrome, Linux, Microsoft Windows
- **SaaS/Application Security:** Adaptive Shield, Airlock, AppOmni, Dazz, DoControl, Grip Security, Legit Security, Obsidian Security, Robust Intelligence, SafeGuard Cyber, Valence Security

- **Security Awareness Training and Testing:** KnowBe4, Prelude Security, Proofpoint, Right-Hand Cybersecurity
- **SSE/Web**: Apache HTTP Server, Axis Security, Broadcom Edge SWG, Cloudflare, HAProxy, iboss, Netskope, NGINX, Skyhigh Security, Squid Proxy, Technopath PowerApp, Zscaler
- **Threat Intelligence:** Centripetal, Cybersixgill, Cyware, DomainTools, Intsights, IPQualityScore, MixMode, OPSWAT, SecurityScorecard, SnapAttack, ThreatQuotient, Tidal Cyber, VirusTotal
- **Vulnerability Management:** Cisco Vulnerability Management, NopSec, RevealD, Safe Security, Silk Security (Armis), Vulcan Cyber

Supporting Quotes

“As modern attacks increase in complexity and sophistication, CISOs need increased visibility and control across their organization's environment to level the playing field for defenders,” said John Graham-Cumming, chief technology officer, Cloudflare. “The integration of Cloudflare’s robust zero trust capabilities, alongside CrowdStrike Falcon Next-Gen SIEM, allows organizations to gain a more holistic view of the threat landscape and take action to mitigate both internal and external risks posed by today’s security challenges.”

“We're partnering with CrowdStrike to help customers modernize their SOC and supercharge their SIEM. Plainly put, we're giving teams a single, unified view of their entire attack surface,” said Zac Kilpatrick, vice president of global channels and GTM alliances, Cribl. “Our efforts with Falcon Next-Gen SIEM bring choice, control and flexibility to the way organizations handle data. That way, they can make better decisions, faster.”

“With CrowdStrike, we’re setting the standard in data security,” said Mike Tornincasa, chief business officer, Rubrik. “Our integration with Falcon Next-Gen SIEM helps customers move away from legacy systems to an AI-native platform approach to more effectively secure the enterprise.”

“Zscaler and CrowdStrike offer true best-of-breed zero trust solutions that extend from endpoint to cloud that no other security platform can. We are extending this partnership further to drive improved threat detection and reduce complexity in security operations,” said Punit Minocha, executive vice president, business and corporate development, Zscaler. “Our collaboration with CrowdStrike and integration with Falcon Next-Gen SIEM is a testament to our joint commitment to providing SOC teams with the data and technology they need to stop threats.”

Falcon Next-Gen SIEM is generally available. For more information:

- Get a demo at RSA, booth #N-6144
- Register for the virtual AI-Native SOC Summit
- Visit the Falcon Next-Gen SIEM page or request a free virtual test drive
- Visit the Falcon Next-Gen SIEM partner page.

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 | Twitter | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

View source version on businesswire.com: https://www.businesswire.com/news/home/20240507307287/en/

Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike