Exaforce

CROWDSTRIKE

UNIFY CONTEXT. ACCELERATE RESPONSE.

Unified context and governed action across Endpoint, Identity, SaaS, Threat Intelligence within Falcon Next-Gen SIEM

SOLUTION BRIEF

The Challenge

The agentic era is raising the speed and scale of cyberattacks. According to the CrowdStrike 2026 Global Threat Report, attacks by AI-enabled adversaries increased 89% year over year in 2025, while 82% of detections were malware-free and the average eCrime breakout time fell to just 29 minutes.

Attackers increasingly exploit trusted identities, SaaS integrations, cloud services, and unmanaged devices, moving across domains while blending into normal activity. Security teams now have a much smaller window to connect the evidence, understand the attack, and respond.

The Solution

The CrowdStrike Falcon® platform delivers high-fidelity telemetry, threat context, detections, and native response controls. Exaforce integrates with CrowdStrike Falcon® Insight XDR, CrowdStrike Falcon® Next-Gen Identity Security, CrowdStrike Falcon® Shield, CrowdStrike Falcon® Next-Gen SIEM, and CrowdStrike Falcon® Adversary Intelligence, bringing Endpoint, Identity, SaaS, SIEM, and licensed threat intelligence into one investigation. Falcon Adversary Intelligence enriches findings with indicator and adversary context, while Exaforce connects signals and intelligence from the Falcon platform with the wider security ecosystem to reconstruct attacks, reach evidence-backed verdicts, and take governed action.

Exaforce applies four task-specific AI agents, called Exabots, across the security lifecycle: Detect, Triage, Investigate and Threat Hunt, and Respond. Working continuously, they show the evidence and reasoning behind every verdict, operate autonomously where policy allows, and request human approval for consequential actions. The Falcon platform remains the platform of record, while Exaforce adds cross-domain reasoning and governed execution.

KEY HIGHLIGHTS

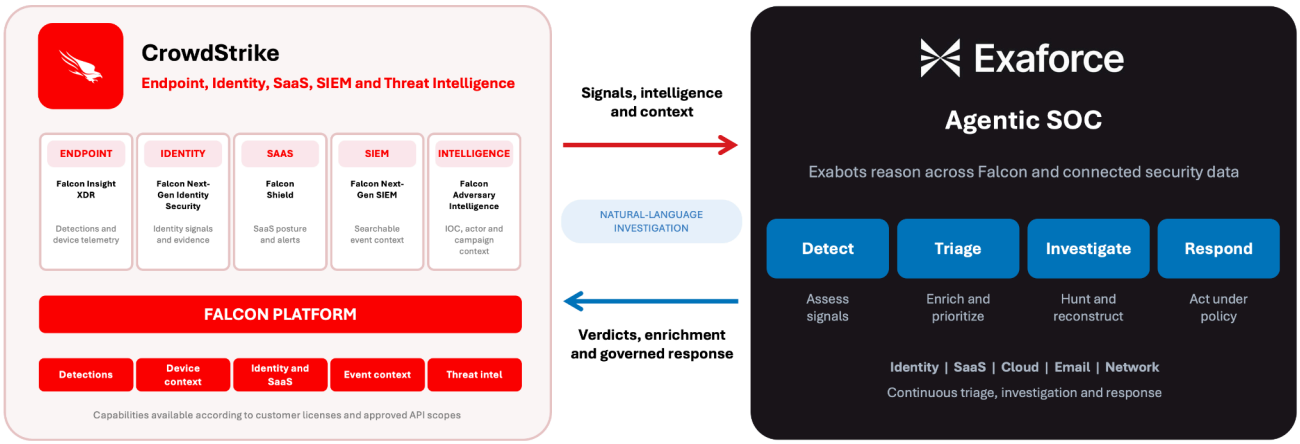
- **Connect activity across Endpoint, Identity, SaaS, and Falcon Next-Gen SIEM into one attack chain**
- **Triage every signal with full context from across your security ecosystem**
- **Hunt across data from the Falcon platform and your security ecosystem in natural language**
- **See the evidence and reasoning behind every verdict**
- **Contain threats through the Falcon platform and connected tools, automatically or with human approval**

Key Use Cases

USE CASE	JOINT MOTION	BUSINESS VALUE
Autonomous triage of Falcon detections	Exabot Triage evaluates detections from the Falcon platform, enriches them with Falcon Adversary Intelligence and cross-domain evidence, and separates benign activity from confirmed threats with clear rationale.	Reduce alert queues while giving every Falcon detection consistent, evidence-backed triage.
Natural-language threat hunting	When the Falcon platform flags a user or device, Exabot Investigate reconstructs what happened before, during, and after the detection across Endpoint, Identity, SaaS and third-party evidence. Analysts can ask: “What led to this detection, which users and devices were involved, and how did the activity spread?”	Scope incidents faster with one evidence-linked attack chain.
Governed containment and closed-loop response	Exabot Respond uses Falcon-native controls to contain devices, update alerts, and execute approved response actions. Policy guardrails and human approval govern consequential actions.	Accelerate containment and close the loop in Falcon without sacrificing human control.

How it works

One Falcon platform. One cross-domain investigation.



Operational Outcomes

24/7 COVERAGE Exabots work the investigation lifecycle around the clock.	**NATURAL LANGUAGE** Ask questions in plain language across all data sources.	**FASTER DECISIONS** Know what happened, why it matters, and what to do next.	**GOVERNED RESPONSE** Automate routine response, with approval for critical actions.

Once connected through a customer-created OAuth 2.0 API client with approved scopes, every signal from the Falcon platform enters a continuous Exaforce workflow. When Falcon Adversary Intelligence is licensed, Exaforce enriches findings with indicator, adversary, malware, kill-chain, and report context before correlating related users, devices, applications, and activity across Falcon and connected security sources into one evidence-backed attack chain. Analysts can then hunt and ask follow-up questions across this combined evidence in natural language, without writing complex queries.

Benign activity is resolved with a clear verdict and rationale. Confirmed threats arrive with evidence, timelines, root cause, blast radius, and recommended action. Verdicts, status updates, and enrichment can flow back to Falcon Next-Gen SIEM, while customer policy determines which responses run automatically and which require human approval.

The Integration in Action

An endpoint detection from the Falcon platform becomes one higher-confidence attack chain.

CrowdStrike and connected-source alerts combine while analysts remain in control.

2:47:00 **Detect.** Falcon Insight XDR flags suspicious PowerShell launched by a document on a managed endpoint.

Triage. Exaforce enriches the finding with related Falcon detections, device posture, user identity, and CrowdStrike adversary and indicator intelligence.

Correlate. Exaforce joins CrowdStrike detections with identity-provider, email, network, SaaS, and cloud alerts into one higher-fidelity attack chain.

Investigate. The timeline reconstructs the malicious email, stolen session activity, endpoint execution, persistence, and attempted lateral movement.

Verdict. Establish whether the activity is a real compromise, with root cause, affected user and device, blast radius, and an evidence-linked rationale.

Respond. Isolate the endpoint through the Falcon platform and coordinate session revocation and network blocks automatically or with human approval under policy.

2:52:00 **Ask.** In natural language, ask: “Which systems did this user and device access after initial execution?” Get an evidence-linked answer without a query.

Attackers don’t wait for business hours. Now your cloud defense doesn’t either.

Integration capabilities across the Falcon platform

Each integration uses the Falcon platform in a technically precise way while feeding the same Exaforce investigation and governance model.

FALCON CAPABILITY	INTEGRATED MOTION	BUSINESS OUTCOMES
Falcon Insight XDR	Collect detections, endpoint events, host inventory, incidents, and vulnerabilities. Endpoint process and network data can also classify AI applications in use. Optional scopes enable containment, Falcon Real Time Response, and alert updates.	A high-severity endpoint alert becomes an evidence-linked finding and a governed Falcon response.
Falcon Next-Gen Identity Security	Collect identity detections, correlate them with the identity provider and endpoint, and synchronize detection status. Identity remediation runs through the connected IdP.	An identity alert is matched to the user and sign-in history, auto-triaged, and resolved without unnecessary lockout.
Falcon Shield	Collect SaaS-security detections correlate them with the relevant SaaS and identity context.	A SaaS posture or identity signal becomes an investigated threat finding instead of an isolated alert.
Falcon Next-Gen SIEM	Use optional read access to search Falcon Next-Gen SIEM on demand.	Bring relevant event data into investigations for additional context and evidence.
Falcon Adversary Intelligence	With Falcon Adversary Intelligence, enrich findings with CrowdStrike indicators and related adversary, malware, kill-chain, and report context.	Prioritize findings faster with threat intelligence attached to the evidence, reducing manual IOC research.

About Exaforce

Exaforce delivers an agentic SOC platform that helps security teams detect, triage, investigate, hunt, and respond to threats with greater speed and consistency. Its task-specific Exabots operate on a shared reasoning foundation and a unified, real-time view of the environment, enabling transparent, evidence-linked decisions across the full SOC lifecycle. Exaforce is available as a SaaS platform. The platform is designed for strong tenant isolation and enterprise security requirements, with support for SOC 2, HITRUST, HIPAA, ISO 27001, PCI DSS, and GDPR compliance. Read our customer case studies, explore the platform, or learn more at exaforce.com.

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. Learn more at crowdstrike.com.

See the Exaforce + CrowdStrike integrations live

Meet Exaforce at Fal.Con 2026 to see Endpoint, identity, SaaS, Threat Intelligence, and Falcon Next-Gen SIEM workflows move from Falcon signal to evidence-backed, policy-governed action. Visit exaforce.com or scan the code to request a demo.

exaforce.com