CrowdStrike Products

Data Sheet

Falcon Adversary Intelligence

Optimize the effectiveness of your entire security stack through the power of AI and automation

Challenges

Adversaries have become faster and more sophisticated, consistently outpacing organizations and leaving them exposed to breaches. Being slower than the adversaries poses significant risks to your brand, reputation and financial standing.

Smaller organizations rely solely on their security tools for protection, while larger entities invest heavily in traditional security information and event management (SIEM) tools to detect and investigate attacks. Unfortunately, these legacy SIEMs aren't up to the task. An estimated 61% of legacy SIEMs generate more than 1,000 alerts daily,[1] overwhelming understaffed and underskilled SOC teams, leading to slower operations and missed threats.

Additionally, 80% of organizations limit their understanding of threat intelligence to known threats.[2] But intelligence must go beyond the basics, offering real-time insight into adversaries' methods and must be applied in organizations' environments and SIEMs. Automation is key to shortening the time from detecting to responding, enabling immediate deployment of countermeasures.

Solution

CrowdStrike Falcon® Adversary Intelligence optimizes effectiveness for the entire security stack through automated intelligence orchestration, contextual enrichment and AI-powered investigative tools.

Key benefits

- Falcon Adversary Intelligence **cuts response time from days to minutes** across your entire security stack with end-to-end intelligence automation.
- Out-of-the-box workflows ensure timely and precise **deployment of the right defenses, to the right tools, at the right time** across your entire security stack.
- Falcon Adversary Intelligence **disrupts adversaries with 24/7 monitoring and real-time alerts** to potentially malicious activity across the open, deep and dark web.

[1] Gurucul, SIEM Data Analytics Challenges Facing the SOC, 2023

[2] ESG Research

Falcon Adversary Intelligence delivers industry-leading threat intelligence into the CrowdStrike Falcon® platform, making all modules intelligence-aware on Day One. This integration provides the necessary context for confident decision-making delivered seamlessly into the daily workflow.

CrowdStrike customers can realize a reduction of up to 97% in research time on adversaries and threats, up to 80% decrease in malware analysis time and up to 79% decrease in threat triage efforts.[3]

Key capabilities

Streamline Your SOC Through Automation

Falcon Adversary Intelligence cuts response time from days to minutes across your entire security stack with end-to-end automation. Instantly submit potential threats to an advanced sandbox, extract indicators and deploy countermeasures — all while continuously monitoring for fraud and safeguarding your brand, employees and sensitive data.

- **Advanced malware sandbox:** Seamlessly integrated into your security operations, the sandbox automates file, email and command-line analyses within seconds, enables quick triage and provides essential context for informed next steps.
- **Brand and fraud monitoring:** Get enhanced threat visibility beyond your perimeter with real-time intelligence to uncover domain impersonations, exposed credentials and data leakages, and take action with automated takedowns and blocklist submissions.

Integrate Seamlessly with Third-Party Tools

Access a prebuilt library of incident response playbooks, empowering teams to orchestrate actions and automate defenses. Streamline response with pre-configured workflows, eliminating the need for complex integrations.

- **Out-of-the-box playbooks:** Scale response quality with standardized playbooks, and consistently deploy countermeasures to optimize protection.
- **Security operations APIs:** Accelerate threat response by pushing the right IOCs to the right tools at the right time. Seamlessly automate defenses across the security stack with CrowdStrike Falcon® Fusion security orchestration automation and response (SOAR) playbooks and prebuilt integrations.

Request a demo →

[3] Based on CrowdStrike Business Value Assessments (BVAs). CrowdStrike BVA numbers are projected estimates of average benefits based on aggregated business value assessments completed with customers 6+ months post deployment where they report realized process efficiencies compared to the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.

Expand Threat Hunting to External Sources

Falcon Adversary Intelligence prevents external threats that could compromise identities, steal sensitive data and destroy your organization's brand. Disrupt adversaries with 24/7 monitoring and real-time alerts to potentially malicious activity across the open, deep and dark web.

- **Attack surface reduction:** Get threat intelligence capabilities that include adversary profiles, credential monitoring, context-aware indicators and vulnerability intelligence.
- **Exposure of adversary infrastructure:** Utilize attack surface scans to explore and identify adversary-controlled domains and high-risk infrastructure accessed by your organization.
- **Automated threat modeling:** Effortlessly surface adversarial risk from the noise with CrowdStrike's automated threat modeling. Rapidly identify the most critical threats specific to your business and get tailored recommendations.

Attend a hands-on workshop →

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 | X | LinkedIn | Facebook | Instagram