ARMIS + CROWDSTRIKE

Unmatched visibility and security for managed and unmanaged assets

Gaps in your security strategy can be hard to find. Sometimes security protocols are just broken, sometimes it's the result of intentional circumvention, and sometimes you just didn't know a device even existed in the first place. Whatever the case, it's critical to know when these things happen, and to know as much as you can about the state of all devices in your environment so you can understand and mitigate the issue.

Together, Armis and CrowdStrike help to strengthen your security posture through real-time assurance that Falcon sensors are properly deployed, updated, and active. The Armis and CrowdStrike integration also improves your visibility, combining device details from Falcon sensors, with device details gathered by Armis from your other IT and security products, giving you a comprehensive view of every managed and unmanaged asset in your environment, including their potential risks.

Discover, classify, and maintain a complete inventory of all your assets

Bad actors see your environment as one interconnected attack surface, making comprehensive visibility into every device in your environment a critical need. Armis is agentless and passive. It discovers all devices in your environment—managed, unmanaged, OT, medical, and IoT—on or off your network and in your airspace.

Armis can identify the device type, manufacturer, model, IP and MAC address, OS, reputation, username, software, behavior, connections, risk factors, and more. And, leveraging the CrowdStrike Falcon sensor on a device, Armis can gather even more insights from your managed devices. This enriched device information is made available right in the Armis console and provides the most complete asset inventory available.

SOLUTION BENEFITS:

- Comprehensive managed and unmanaged device visibility across any environment: IT, ICS/OT, and healthcare
- Centralized source of truth for information about your assets
- Automatic, prioritized device vulnerability and risk assessments
- Enhanced threat detection and mitigation across all environments

Identify, assess, and respond to vulnerabilities and risks automatically

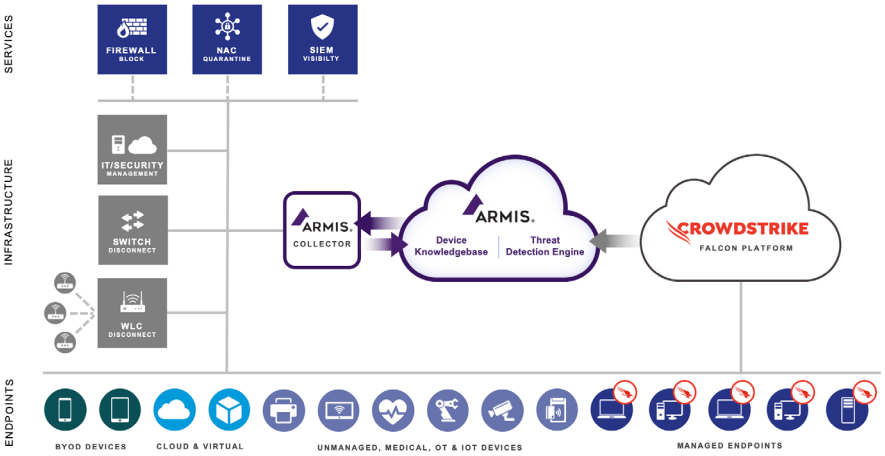
Busy security teams need to identify, prioritize, and mitigate vulnerabilities fast—not just for compliance with regulatory frameworks, but to thwart bad actors from using at-risk devices to stage an attack.

Armis uses device information from Armis' one-of-its-kind Device Knowledgebase (tracking 500M devices daily), along with details collected from CrowdStrike Falcon sensors and other IT and security products, to calculate risk scores for every device. These scores are based on factors like known vulnerabilities, known attack patterns, and device behavior.

Armis then uses this information to mitigate the risk of vulnerable or suspicious devices by triggering policy-based actions, such as blocking devices through integration with your network enforcement products.

Ensure compliance with IT/security policies for corporate devices

Enforcing corporate IT and security policies is an essential component of reducing your organization's attack surface. Armis can identify corporate devices that aren't actively running the CrowdStrike Falcon sensor. To help mitigate risk from any non-compliant or rogue endpoints, you can create policies in Armis that take automatic actions like opening cases with your ticketing system, alerting appropriate teams of a device's non-compliance status, or sending a notice to the user to reinstall a missing or misconfigured sensor.



ABOUT ARMIS

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged "smart" devices like video cameras, smart TVs, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on & off the network that connect and communicate via wired, Wi-Fi, Bluetooth, Zigbee, and many other common protocols that are invisible to legacy security systems. Armis continuously analyzes endpoint behavior to identify risks and attacks, to protect critical information and systems. Through integration with your switches and wireless LAN controllers, as well as your existing security enforcement points like Cisco and Palo Alto Networks firewalls or network access control (NAC) products, Armis can quarantine suspicious and malicious devices.

ABOUT CROWDSTRIKE

CrowdStrike is a global cybersecurity leader that has redefined modern security with an advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity, and data. Powered by the CrowdStrike Security Cloud, 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, the Falcon platform enables partners to rapidly build integrations to deliver customer-focused solutions that provide scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

20220222-1