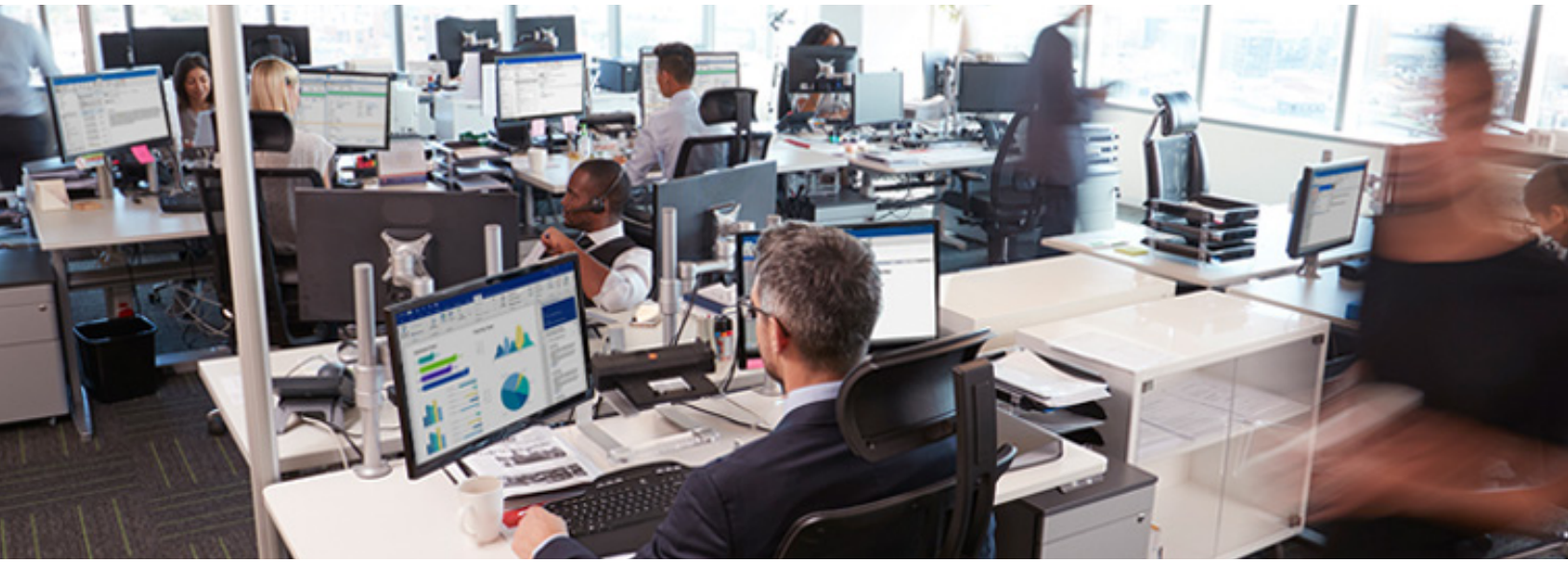
ARMIS + SPLUNK

CLOSE THE UNMANAGED DEVICE VISIBILITY & SECURITY GAP IN ANY ENVIRONMENT



MAKE YOUR EXISTING TOOLS WORK SMARTER

Busy security teams are always looking for ways to get more value out of the tools they already have, but most of these were built for traditional IT environments. Tools that rely on agents to inventory and monitor managed devices are left blind to unmanaged and IoT devices. They also won't work in operational technology (OT) or clinical settings because you can't put agents on these devices, and you can't scan them actively because it could cause them to crash.

The Armis® platform's integration with Splunk® extends unmanaged and IoT device visibility and security to Splunk's Data to Everything platform for a consolidated view of devices and risks that helps you keep your entire environment protected.

Identify and Classify Devices in Any Environment

Effective cybersecurity asset management requires visibility into every device in your environment. This broad scope is essential because bad actors see your environment as one interconnected attack surface.

Armis automatically discovers and generates a comprehensive inventory of all your assets. The Armis Device Knowledgebase of over 300 million device profiles provides you with a wealth of information about each device, like type, manufacturer, model, OS and version, location, reputation, applications used, and more. All of this information is made available right in Splunk, giving you all the information and context you need about devices in your environment.

KEY SOLUTION BENEFITS

- Extend your investment value in Splunk to unmanaged devices, including OT, medical, and IoT assets.
- Analyze device behavior for risks, threats, and attacks.
- Improve the efficiency of threat detection and incident investigation.

Manage Risk Effectively, Respond to Threats Efficiently

With so many devices in a typical enterprise environment, it's challenging to know which ones most vulnerable to an attack. And adding devices found in specialized environments like OT/ICS or cinical settings makes planning and prioritizing mitigation that much more difficult.

Armis automatically performs a security risk assessment for every device in your environment, including an overall device risk score along with detailed information about a device's risk profile. If a device's behavior is considered risky, Armis can block or quarantine the device automatically and generates an alert for your security team in your Splunk environment.

Comply with Security Frameworks

You likely model your security controls against one or more security frameworks. Armis is purpose-built to help you apply frameworks like CIS Critical Security Controls, NIST, and MITRE ATT&CK throughout your environment. In fact, our platform provides broad-spectrum coverage that supports 11 of 20 Critical Security Controls, and 16 of the NIST CSF controls across the Identify, Protect, Detect, and Respond categories. And Armis can help you audit your network connections to measure your network's integrity against the Purdue reference architecture.

> "The stories of Armis being able to plug in and work as advertised, without a whole lot of setup or configuration were true. We can see all our different layers from zero to five."
>
> **Nathan Singleton**
> Manager of Cybersecurity at Helmerich & Payne

Get Started Quickly

Armis deploys without installing any endpoint agents or additional hardware. It requires no learning period to start identifying devices or detecting threats, so you can get started seeing value right away. Integration with Splunk's Data to Everything platform is quick and easy too, using Armis connectors you can access from Splunkbase. Integration makes all of the rich information Armis provides available to your security team right in the SIEM interface they already know and use every day.

LEARN MORE:

armis.com/splunk

ARMIS

1.888.452.4011
armis.com

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 smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

20201118-2