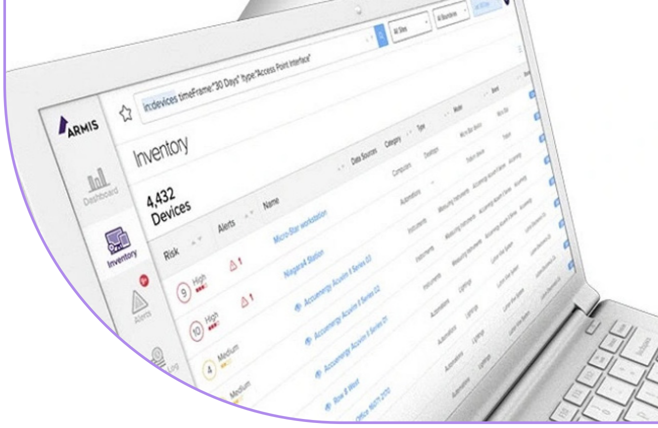
SALT


ARMIS
in:devices timeFrame:"30 Days" type:"Access Point Interface"
Inventory
4,432 Devices
Dashboard
Inventory
Alerts
Log
Risk
Alerts
Name
Data Sources
Category
Type
Micro-Star workstation
Niagara4 Station
Accuenergy Acuvim II Series 03
Accuenergy Acuvim II Series 02
Accuenergy Acuvim II Series 01
Row 8 West
High
Medium

Armis

CASE STUDY

Armis provides an agentless, enterprise-class device security platform designed to address the threat landscape of unmanaged and IoT devices. Customers use the company's real-time and continuous protection to see and control all managed, unmanaged, and IoT devices – from traditional devices such as laptops and smartphones to new smart devices including smart TVs, webcams, printers, HVAC systems, industrial control systems, and medical devices. Armis provides passive asset inventory, risk management, and detection and response to help organizations understand and mitigate their risk.

Monitoring this broad range of devices depends on Armis building integrations for them – integrations that are all API driven. Prior to the COVID-19 pandemic, the Armis team was able to manually document, test, manage, and secure all these APIs. When the pandemic hit and Armis' customers all started having employees working from home, those customers suddenly needed Armis to build integrations with an untold number of new devices.

"We spun up more than 100 new integrations in just the first few months of the pandemic – across different technologies, products, and vendors – and all of that is happening over APIs," says Curtis Simpson, CISO at Armis. "We went from 10s of APIs to 100s of APIs in weeks – there was no way we could keep up with creating and updating Swagger files for documentation and pen testing every new API."

Simpson knew he needed automation for discovering, monitoring, and protecting this exponential growth in APIs. After evaluating multiple solutions, the company settled on Salt Security.

Armis leverages the Salt platform to automatically and continuously discover all of its APIs, capturing granular details about them to eliminate blind spots and assess risk. The platform also automatically baselines typical API behavior patterns and identifies anomalies, further inspecting them to distinguish user mistakes or changes in APIs from malicious behavior. Salt surfaces only the attack patterns, reducing alert fatigue and enabling Armis to respond quickly or to automate the shutdown of the attack.

ARMIS®

Armis provides an agentless, enterprise-class device security platform for protecting unmanaged and IoT devices.

Headquarters
Palo Alto, CA

Founded 2015

Infrastructure
Mirrored API traffic from CloudFlare WAF and NGINX, on AWS cloud

www.armis.com

"Our integration team is also using Salt to track how our APIs are used. We can see which ones are being consumed and what functions are being used," says Simpson. "Without Salt, they would have had to build all that monitoring capability themselves for all these new APIs, but with Salt doing that work, they can instead build new integrations. That's a huge added value.

"We've also been able to use Salt for compliance and FedRAMP [Federal Risk and Authorization Management Program]," Simpson continues. "We were able to submit the full catalog of all our APIs and where sensitive data was involved to FedRAMP right out of the Salt platform."

Simpson also appreciates the "shift left" capabilities of Salt. With remediation details, the DevOps teams can immediately update the coding of the APIs to improve security. "With Salt, we're deploying API runtime security, so we get immediate and ongoing value for APIs, even as we rapidly build new ones," says Simpson. "Improving dev practices is super valuable, but you can't shift everything left at once. You're changing the culture along with introducing a bunch of new technology into the pipeline. So with Salt, you get protected right now, and then you can focus on getting developers the remediation insights."

Top use cases for Armis:

- **attack prevention:** Armis has been introducing so many new APIs so fast that the company needs Salt to monitor them for exploitation.
- **dynamic API discovery:** As Armis releases new APIs weekly, Salt creates a continuous inventory of all the APIs and shows where they expose sensitive data.
- **remediation insights:** Armis taps Salt to send details about how APIs can be strengthened directly to the right dev teams.
- **compliance:** Armis can leverage the dynamic reporting in Salt to provide reporting on its full set of APIs and sensitive data for compliance and to demonstrate FedRAMP adherence.

> **With Salt, we're getting API security in runtime, so we can rapidly build and release new APIs and know we're fully protected."**
>
> **– Curtis Simpson, CISO**

SALT