CASE STUDY

Armis Helps State Legislature Tighten Up Security Gaps and Save Time for IT Staff

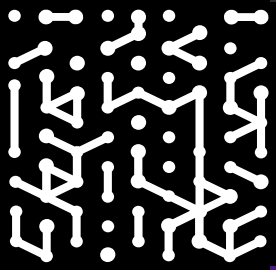
Daily security tasks go faster with a single view and single source of truth

Industry

Government

IT Environment

State government department with 350 employees and approximately 1,500 devices monitored, including BYOD and guest devices on public Wi-Fi.



Introduction

With data streaming in from multiple sources in the security stack, the IT team at this state government department was finding itself having to constantly correlate multiple data sets to track down device discrepancies.

The manual process was time-consuming and inefficient. Armis integrated various systems and sources of data to provide a single source of truth. The team now has a shared, consolidated dashboard that greatly speeds up everyday tasks, prioritizes vulnerabilities, and tightens security gaps before they become a problem.

With 350 total staff members, this U.S. state government department has a team of 15 people dedicated to providing IT services in the state capital building. The security team monitors approximately 1,500 devices. The team's security analyst has been with the department for 18 years and is responsible for security, wireless network access controls, firewalls, and networking. As a relatively small and agile department, the IT team is constantly evaluating new technologies that could potentially be a good fit for its needs.

Manual comparison and correlation of data was “wildly inefficient”

The team needed a solution that would provide them with a single pane of glass that tied in the data they collected from their many disparate security-related tools. For example, the endpoint team used CrowdStrike for endpoint protection, detection, and response; the server team used Microsoft System Center Configuration Manager (SCCM) for endpoint management; and the networking team used Cisco DNA Center for network management.

“We all went to our own separate places,” the security analyst explains. “If something rolled over from one area to another, we would have to pull up our dashboards and manually compare them. It was time-consuming and wildly inefficient.”

At one point, the team considered implementing log management software to help with log consolidation but determined that the cost was too prohibitive considering the size of the department. They also tried a security information and event management (SIEM) tool but found that it had some limitations. During the proof of value (PoV), the team saw that Armis in combination with network test access points (TAPs) made for a powerful duo. As the security analyst noted, they all agreed that “Armis checked all the boxes we were looking for.”

Armis speeds up day-to-day tasks and simplifies security management

The team has integrated Armis with CrowdStrike, Microsoft SCCM, network TAPs, Dynamic Host Configuration Protocol (DHCP) network server, Simple Network Management Protocol (SNMP) network mapper, and Cisco Meraki for wide access network (WAN) and wireless network.

Challenges

- Correlating disparate sources of data
- Inefficient process to manually compare data sets
- Incomplete or inaccurate information on software update and patch status
- No single view for team to view data
- Prioritizing vulnerabilities

All the data from these sources is pulled into Armis for easy reference, so instead of consulting three different management consoles, the team only needs to go to one place—the Armis dashboard. This has greatly reduced the time team members spend looking things up. “Data that used to take 30 minutes to correlate and look up is available in minutes now,” asserted the security analyst.

Armis is the organization’s primary location of record for all its assets, serving as its configuration management database (CMBD). It provides reports on devices that need to be upgraded, such as those with Windows operating systems that are behind several versions of patches, exposing them to higher risk. Armis has also substantially reduced the time the team spends on day-to-day tasks by consolidating data and prioritizing what is most important, whether it is fixing a CrowdStrike installation, pushing an SCCM update that was frozen or stuck, or rebooting a machine to install updates.

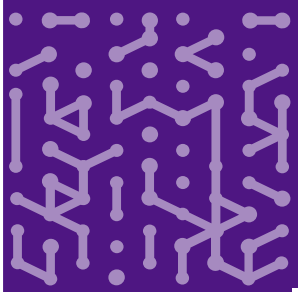
The security analyst goes to the dashboard in Armis to uncover the most important high-risk items and then works his way backwards from there. “Armis helps us detect discrepancies in patch status across all our systems and speeds up remediation of misconfigurations or other issues that need to be addressed in a timely manner,” he remarked.

Armis helps prioritize vulnerability management

For vulnerability management, the security analyst shared that his favorite feature of Armis is the Exploit Prediction Scoring System (EPSS), which leverages data to estimate the likelihood that a software vulnerability may be exploited. The team has a dashboard set up in Armis called “Prioritize Vulnerabilities” that

Armis Results

- Significant time savings on previously manual day-to-day tasks
- A single dashboard to view data from different systems
- Prioritization of vulnerabilities and threats
- Pinpointing security gaps, such as misconfigurations or unpatched systems, before they become a problem
- Identifying legacy systems that could pose a risk and need to be phased out



looks at devices that have a score higher than 90. When the team receives alerts from Armis based on these scores, they prioritize the servers first, then the desktops, and anything unusual with a BYOD device or devices on the public network.

Armis has also helped the team discover legacy equipment that is out of date. The security analyst shared the story of some scanners that had been in use at the department for a while, and the team never really knew exactly what operating systems they were running on. Armis discovered that they were running on Windows XP. “That was definitely news to us, and it gave us a reason to speed up the replacement of those devices,” pointed out the security analyst.

Another use case noted by the security analyst is how Armis has helped the team tighten up security gaps that had previously been going unnoticed. On about a weekly basis, Armis was finding instances where updates had not been pushed, software had not been installed, or software needed to be reinstalled. It wasn’t that there were misconfigurations, but, as the security analyst explained, “Software doesn’t always do what it’s supposed to do when it’s supposed to do it. There are lapses, and Armis helps us find those before they become a problem.”

The security analyst affirmed that Armis has provided the department with a clear ROI, measured in terms of time saved, additional insight into devices, and detection of lateral movement that they would not have seen otherwise. “Additionally, our partnership with Armis has been fantastic. Armis has been really innovative, even in the short time that we’ve been a customer. It’s one of the few vendors that continually makes strides to add services and improve its product on a quarterly basis,” he said.

“Armis helps us detect discrepancies in patch status across all our systems and speeds up remediation of misconfigurations or other issues that need to be addressed in a timely manner.”

Security Analyst
State Government

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial