CYBERSECURITY ASSET MANAGEMENT

SEE AND SECURE EVERY THING™

ARMIS

How many ____laptops____ do you have?

users
virtual machines
mobile devices
servers
cloud instances
IoT devices
security cameras
badge readers

CAN YOU ACCURATELY SAY HOW MANY ASSETS YOU HAVE? AND ARE THEY SECURE?

Today's enterprises still struggle to see their complete IT asset inventory—from managed to unmanaged to IoT devices, from virtual machines to clouds, and more. For devices in your environment and in your airspace—on premise and remote—can you accurately identify all you have? Most companies can't, and this leaves them exposed to compliance, vulnerability, and security issues.

The Armis® agentless device security platform provides a flexible, seamless, and comprehensive cybersecurity asset management solution. We provide full visibility into all assets by combining data from other systems with Armis to create one source of truth for all your assets (hardware, software, and services), and provide the risk posture of devices to keep your business and users secure.

- Discover all of your assets
- Identify gaps, vulnerabilities & risks
- Automate & enforce security policies

A FEW OF OUR INTEGRATIONS

ABSOLUTE, aws, BITSIGHT, BlackBerry CYLANCE, BLUECAT, brinqa, Check Point, CHEF, Cherwell, cisco, CROWDSTRIKE, cybereason, DUO, exabeam, FIREEYE, FLEXERA, Gigamon, Google Cloud, Guardicore, IBM, Infoblox, jamf, KEYSIGHT TECHNOLOGIES, cisco Meraki, Microsoft, netbox, okta, paloalto NETWORKS, puppet, QUALYS, RAPID7, REDSEAL, SentinelOne, snow SOFTWARE, solarwinds, servicenow, splunk>, sumo logic, TANIUM, tenable, vmware, vmware Carbon Black, zscaler

DISCOVER EVERY ASSET — EVERY THING

Armis provides a singular and comprehensive view of all the devices in your environment, including remote or off-prem devices. Here is a partial list of the information we can identify in real-time and continuous nature:

- Device type
- Version
- Reputation
- Users
- Software
- Cloud instances
- Known vulnerabilities
- Patches
- Risks

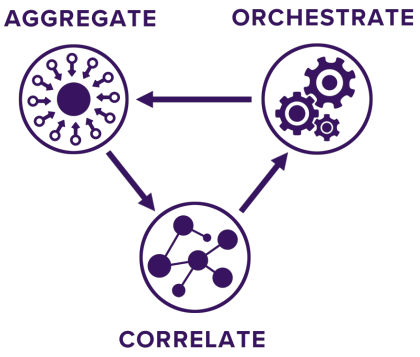
Moreover, Armis can identify when and where assets are, whether they are missing critical security agents or updates, which applications they are using and if they are vulnerable, and can identify remote workers and off-prem devices.

IDENTIFY RISKS & SECURE DEVICES

Beyond discovering the assets, Armis can identify risks and vulnerabilities for devices in the office, at remote locations, as well as those interacting with your cloud environments. Armis understands what a device is and how it is being used and correlates that information against our platform's inherent understanding of device characteristics and behaviors. Armis then compares a device's individual risk profile with your organization's risk posture to provide automated security and policy enforcement.

AUTOMATE & ENFORCE SECURITY POLICIES

If Armis identifies a vulnerability, risk, or security gap, it can automate security and policy enforcement. We can orchestrate the necessary actions in conjunction with your IT or security management solutions, or at the network level. This includes actions like feeding device risk data to your SIEM or CMDB, triggering a vulnerability scan, if appropriate, kicking off a process to install software, or blocking or quarantining a device.



- Create a CMDB entry
- Trigger a vulnerability scan
- Deploy software
- Update device information
- Create an incident in a ticketing system
- Feed device data to SIEM
- Block or quarantine a device

FAST AND SIMPLE TO DEPLOY

The Armis platform is fast and easy to deploy across your environment because it doesn't require any agents and it integrates directly with your existing IT and security management tools. The platform can be up and running in just minutes, and starts providing asset inventory information and insights right away.

IDENTIFY VULNERABLE APPLICATIONS

Beyond identifying assets, Armis can identify vulnerable apps running on devices. Our integrations with your IT and security management solutions, along with our deep device identification and classification, allow you to see the applications running on devices, and if there are vulnerabilities, such as:

- Is the device missing an agent?
- Is the device running an unpatched version of Chrome?
- Is the device running an exploitable version of VxWorks or other RTOS?

SIMPLE QUERIES IMPORTANT INSIGHTS

Armis provides a simple yet powerful Query Tool, letting you identify specific devices, their state, and any security gaps or exposures you may have. It's an easy "If this, then that" visual query builder that lets you create reports and get insights quickly. For example, you can create a query to identify which devices are running a version of an application or operating system that contains known vulnerabilities. Armis lets you track:

- Managed devices
- Unmanaged and IoT devices
- Mobile devices
- Virtual Machines
- Cloud Instances
- Specialized devices (medical, healthcare, manufacturing, OT, etc.)
- Users

ABOUT ARMIS

Armis is the leading agentless, enterprise-class device security platform, designed to protect organizations from cyberthreats created by the onslaught of unmanaged and IoT devices. Fortune 1000 companies trust our real-time and continuous protection to see and control all managed, unmanaged, un-agentable and IoT devices – from traditional devices like laptops and smartphones to new smart devices like smart TVs, webcams, printers, HVAC systems, industrial control systems and PLCs, medical devices and more. Armis provides passive and unparalleled asset inventory, risk management, and detection & response. Armis has the world's largest Device Knowledgebase, tracking over 280 million devices, tracking device behavior, connections, and history.

ARMIS

1.888.452.4011
armis.com

20200812-2