SECURITY FOR THE REMOTE WORKFORCE

For many organizations, wide scale adoption of work from home (WFH) practices has become commonplace with a larger percentage of their overall workforce working remotely. This has created visibility and asset management challenges for these businesses as they often lack the ability to fully support a remote workforce, in a secure way. Security teams that do not have full visibility to assets in the home will have significant difficulty determining the scope of a compromise, containing it, and remediating from exploits. With remote work here to stay, security professionals need ways to maintain the same level of asset discovery, risk assessment and security policy enforcement that they have when employees are working in the office.

VISIBILITY IS ESSENTIAL FOR WORK FROM HOME CYBERSECURITY

Most organizations today struggle to see their entire IT asset inventory—from managed to unmanaged to IoT devices, even when their workers are working from corporate offices. This visibility challenge is even more difficult when the users and their devices, both managed and unmanaged, are remotely connected to a variety of different services behind the firewall and in the cloud. This problem is particularly acute as organizations shift to more cloud-based services and traffic is no longer traversing the corporate network, but rather is going from the home to the cloud. As an example, many security tools were designed to manage a specific device and/or agent, and do not consolidate information across other tools. The resulting 'blindspot' that most security teams have largely stems from these gaps left by traditional security tools combined with the inability to easily get a reliable and consolidated view of all assets.

Discover devices used by workers remotely and at home even when not logged into the corporate network.

Track when a user logs into a cloud application, their location, if a device is missing a critical security agent or update or using applications with vulnerabilities.

Identify issues and discrepancies, correlate that information, provide alerts and execute policy enforcement to bring an additional layer of security for WFH or remote users

DISCOVER ALL YOUR ASSETS AT HOME

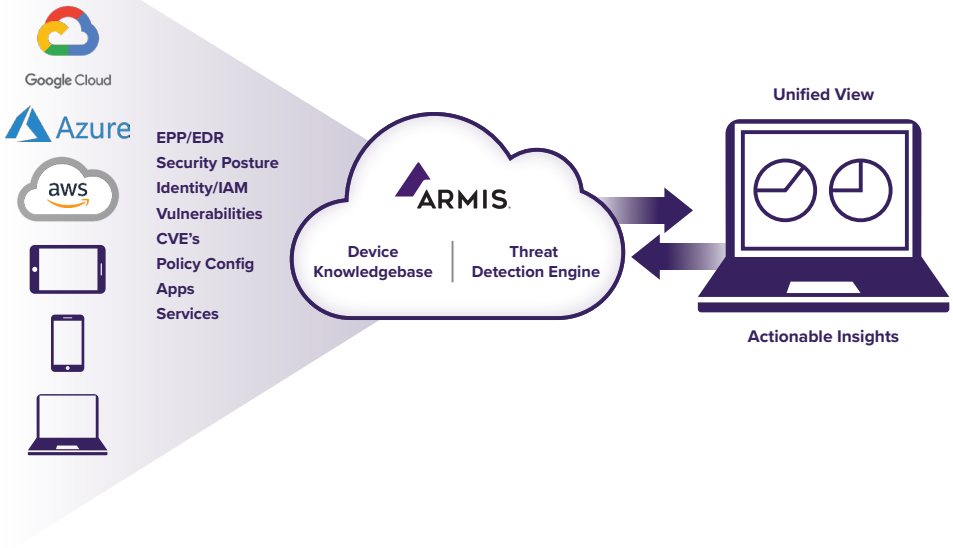
Regardless of all the tools IT and security professionals have, they are still facing two critical challenges. First, tools are siloed with no single source of truth or that provide an accurate picture of everything. And that “everything” now encompasses a massively expanded work from home scenario.

Armis provides a singular and comprehensive view of assets in your environment, including remote or off-prem devices.

Here is a partial list of the information we can identify in a real-time and continuous nature:

- Device type
- Version
- Reputation
- Software
- Known vulnerabilities
- Patches
- User identity
- Location
- Risks

UNIFIED ASSET DISCOVERY, RISK ASSESSMENT AND POLICY ENFORCEMENT FROM HOME TO CLOUD TO OFFICE



ACTIONABLE INSIGHTS

Armis provides you with visibility to home users, their location, their managed devices and the applications & services they are using. By aggregating and correlating all this telemetry data into a single view, Armis gives you insights that can help you identify specific devices, their state, and any security gaps or exposures you may have. From these insights, you can then take action to put in motion steps to remediate.

For example, while those devices are in the office, you are likely to run scheduled vulnerability scans to determine any security weaknesses of those machines. It is far less likely, however, that you would point your vulnerability scanners to a device that is in the home meaning that device has missed a scheduled scan leaving it and you exposed.

With Armis, you can easily identify those devices:

- Passively match to known CVE’s to uncover a browser or application version with a known vulnerability
- Determine if they have the proper security configuration such as disk encryption enabled
- Orchestrate updates or patches to application software or endpoint agent

Armis can identify where assets are, whether they are missing critical security agents or updates, if their configurations are compliant with security. policies, which applications they are using and if they are vulnerable and need to be patched. All this data is displayed in a single unified view complete with comprehensive search, reporting and policy management capabilities.

IDENTIFY RISKS AND GAPS FOR OFF-NETWORK ASSETS

Beyond discovering the assets, Armis can identify risks and vulnerabilities for managed devices off-prem or in the home, as well as those interacting with your applications & services. Armis gathers information from your existing IT & security management systems to understand what a device is, how it is being used, what services it is communicating with 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 ENFORCEMENT WHEN HOME USERS ARE OUT OF COMPLIANCE

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 other IT or security management solutions. This includes actions like feeding device risk data to your SIEM or CMDB, validating device configuration, or kicking off a process to remotely install or patch software.

YOUR QUESTIONS ANSWERED

The Armis platform also features the Armis Standard Query (ASQ) tool. Using ASQ, you can search for devices, vulnerabilities, services, users, policies, configurations and more — the combinations are virtually endless.

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.

ARMIS
1.888.452.4011
armis.com

20201005-2