ALIGNMENT TO CIS CRITICAL SECURITY CONTROLS

Alignment to CIS Critical Security Controls

The Center for Internet Security (CIS) publishes a set of security guidelines called the "Critical Security Controls." These security controls have developed a reputation for being effective and practical.

As the number of connected "things" on networks increases, enterprises need to ensure that their security controls provide visibility to those devices. Many security products fail to do this, giving rise to a phenomenon known as "shadow IT". Gartner has stated that "by 2020, one-third of successful attacks experienced by enterprises will be on data located in shadow IT resources, including shadow Internet of Things (IoT)."[1]

Enterprises that deploy the Armis platform have complete visibility, so they do not have a shadow IT problem. The Armis mission is to ensure that all devices in your enterprise environment – both on and off your network – are visible and secure.

The information below explains how the Armis platform aligns to the twenty Critical Security Controls.

Control 1: Inventory and Control of Hardware Assets

Through passive listening techniques, the Armis platform discovers all devices on your enterprise network as well as devices that are in proximity to your network and that can be seen thru RF analysis. This discovery covers both primarily connected devices (those that have an IP address) and peripherally connected devices (those that connect to an attached device using protocols like Bluetooth, NRF, Zigbee, etc.). The end result is a complete inventory of devices – right down to make, model, MAC address, IP address, and operating system.

Control 2: Inventory and Control of Software Assets

Without using agents, the Armis platform discovers software that is running on all devices in your enterprise. The fact that the platform does not use agents allows it to discover software running not just on managed computers but also BYOD devices and the increasingly large number of connected "things" that are on enterprise networks—video cameras, thermostats, Amazon Echo devices, medical devices, industrial devices, etc.

Control 3: Continuous Vulnerability Management

The Armis platform constantly monitors all devices on the enterprise network and identifies the vulnerabilities that are present in each device based on the software version which the platform detects through passive monitoring techniques. The Armis platform does this without any need for an agent on the endpoint; this allows the platform to detect software vulnerabilities on just about everything—managed computers, BYOD devices, and the increasingly large number of connected "things" that are on enterprise networks.

Second, the platform continuously monitors the behavior of all devices on and near your network as a way to detect possible compromise. Amis compares every device's real-time activity to the established and "known-good" activity baseline for the specific device which is stored in our device Knowledgebase. When abnormal behavior in your network is detected, the platform updates the risk score and generates a security alert.

The risk score that the Armis platform produces for each device in your environment is based on multiple factors including the software vulnerabilities that we detect, known attack patterns that we are aware of (which are, in part, generated by our continuous threat intelligence feed), and the behavior that we observe of each device on your network.

Control 4: Controlled Use of Administrative Privileges

The Armis platform does not currently provide this control.

Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

The Armis platform does not currently provide this control.

Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

The Armis platform does not currently provide this control.

Control 7: Email and Web Browser Protections

The Armis platform does not currently provide this control.

Control 8: Malware Defenses

IoT devices are not usually protected by traditional anti-malware defenses. The best way to detect malware activity on IoT devices is through behavioral analysis.

IoT devices are essentially small, purpose-built computers running a network stack, operating system, and a very specific application designed to perform only the function that the device was designed for. From a network traffic perspective, IoT devices perform a limited number of very specific tasks – their behavior is usually very predictable.

The Armis platform monitors every device in your environment on a continuous basis and compares the behavior to the "normal" baseline that exists in the Armis Device Knowledgebase. The Device Knowledgebase contains over 8 million individual device profiles which includes such things as how often each device typically communicates to another device, over what protocol, how much data is transmitted, etc. This information includes historical observations from all of our customers' environments plus claims from device manufacturers.

Because of the crowd-sourced nature of the Armis Device Knowledgebase, the platform can detect threats from "patient zero" devices much faster, and with fewer false positives, than traditional security products that simply look for deviations from historical patterns or signature-based pattern matches. The moment that a new device is added to a network where

the platform has been deployed, we can immediately tell if the device is behaving abnormally based on deviations from the baseline behavior that we have witnessed previously; there is no learning period needed.

Control 9: Limitation and Control of Network Ports, Protocols, and Services

The Armis platform passively monitors device communications and associates active ports, services, and protocols to the hardware assets in the asset inventory. The Armis policy engine can be configured to alert or remediate (e.g. quarantine) whenever the platform observes a device utilizing unauthorized ports, protocols or services.

Control 10: Data Recovery Capability

The Armis platform does not currently provide this control.

Control 11: Secure Configurations for Network Devices like Firewalls, Routers, and Switches

The Armis platform can detect unencrypted WiFi traffic which indicates a misconfiguration in your wireless access points.

Control 12: Boundary Defense

The Armis platform continuously monitors all connections in your environment and will alert you if a device has connected across a boundary. This includes connections that occur within your network as well as off-network connections, such as a corporate computer that has mistakenly connected to a rogue access point (sometimes called a “pineapple”). The platform detects unintended network bridges and open (unsecured) hotspots that are often included in modern printers.

The Armis platform’s boundary defense is effective on wired, WiFi, and IoT wireless protocols such as Bluetooth, NRF, Zigbee, etc. Traditional network firewalls have no visibility to these points of data leakage, which is why the platform is uniquely valuable for this Critical Security Control.

Control 13: Data Protection

The Armis platform does not currently provide this control.

Control 14: Controlled Access Based on the Need to Know

The Armis platform does not currently provide this control.

Control 15: Wireless Access Control

The Armis platform provides several capabilities in this area:

1. The platform can provide a complete inventory of all authorized and unauthorized (rogue) wireless access points in your enterprise airspace.
2. The platform can monitor all wireless connections in your airspace and detect unintended network bridges and open (unsecured) hotspots that are frequently found in modern printers.
3. The platform can detect if any unencrypted WiFi traffic exists within your environment.
4. The platform monitors not just WiFI (802.11) but also ten other wireless protocols such as Bluetooth, NRF, Zigbee, Z-Wave, etc.

Control 16: Account Monitoring and Control

The Armis platform does not currently provide this control.

Control 17: Implement a Security Awareness and Training Program

The Armis platform does not currently provide this control.

Control 18: Application Software Security

The Armis platform does not currently provide this control.

Control 19: Incident Response and Management

The Armis platform does not currently provide this control.

Control 20: Penetration Tests and Red Team Exercises

The Armis platform does not currently provide this control.

1Gartner “How to Respond to the 2018 Threat Landscape”, 28 November 2017, analyst Greg Young.

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.com

20190527.1