PALO ALTO NETWORKS AND ARMIS

IoT Security For Every Enterprise

KEY POINTS

- Automatically stop IoT threats at the firewall.
- Dynamically enforce firewall policy based on device behavior and device risk score.
- Isolate compromised devices and prevent data leakage on both the wired and wireless networks.
- Broaden the security footprint past the perimeter all the way to the access layer.

New devices, behaviors, and threats are changing enterprise networks from the inside out, and security teams are looking for ways to ensure that policy, enforcement, and protection are consistently applied for all devices and connections. The integration of Armis with the Palo Alto Networks® next-generation firewall delivers on this vision by tying the internal security context of IoT devices to the bedrock of enterprise security policy at the firewall.

Today, security teams are facing a wave of IoT and unmanaged devices that are beyond the reach of endpoint security. Each device usually contains multiple wired and wireless connectivity options, and new threats have quickly emerged to take advantage of this new attack surface. New attack vectors such as BroadPwn, BlueBorne, and KRACK opened the door to direct device-to-device attacks, with IoT attacks growing by more than 280% in the first half of 2017 alone[1].

Armis secures this new attack surface and coordinates with the next-generation firewall to provide automated, policy-driven enforcement at the firewall. Armis identifies all devices in the local environment both on the wire and on dozens of wireless protocols, tracks device behaviors, automatically identifies threats and misbehaving devices, and protects the wireless network. Next, when Armis detects a threat or compromised device, the solution automatically communicates this to the next-generation firewall which can create a dynamic policy to block traffic at the firewall.

ARMIS - CONTROL FOR IOT, UNMANAGED DEVICES, AND SHADOW NETWORKS

While enterprises have traditionally been able to secure their managed devices with endpoint security agents, this model no longer works for a growing number of enterprises. Increasingly, organizations must secure a new breed of devices that cannot support a security agent, yet have full operating systems and network stacks with a variety of connectivity options.

Printers, Smart TVs, Bluetooth peripherals, IP phones, Smart HVACs, personal assistants such as the Amazon Echo, and employee personal devices all fit into this category, and are just a few examples of a larger trend. Increasingly, devices are networked by default and ready to connect via WiFi or Bluetooth as first options. This can lead to the device being directly exposed to over-the-air attacks, or accidentally connecting to unsanctioned devices and networks, creating a so-called "shadow network". The plethora of connectivity options can lead devices to being connected both wired and wirelessly at the same time, creating unseen bridges between trust zones.

Armis brings real-time visibility and control to this new breed of devices. Without the need for sensors or an agent, Armis can monitor the local environment to identify all devices and automatically classify them by type. This includes devices using WiFi, Bluetooth, and dozens of other protocols. The Armis solution automatically understands appropriate device behavior based on its type and history. The Armis solution continuously monitors all devices and all interactions for both known and unknown threats and signs of compromise. When a threat is detected, the solution can block the affected device on the wireless side and notify the Palo Alto Networks firewall on the wired side.

Armis Agentless IoT Security Platform		
 Discover	 Analyze	 Protect
◦ Managed and unmanaged ◦ Wired and wireless ◦ On and off the network	◦ Risk and threat quantification ◦ Behavioral analysis ◦ Anomaly detection	◦ Enable safe devices to connect ◦ Remove suspicious devices ◦ Manually or per policy

PALO ALTO NETWORKS NEXT-GENERATION FIREWALL

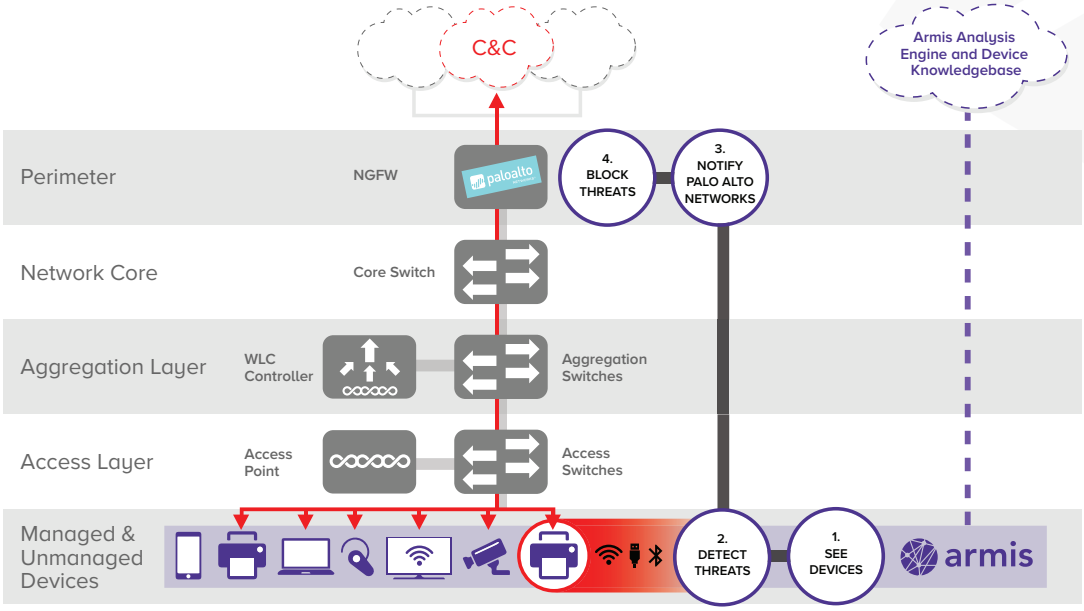
The next-generation firewall classifies all traffic, including encrypted traffic, based on application, application function, user and content. This enables comprehensive, precise security policies, ensuring that only authorized users run sanctioned applications, greatly reducing the surface area of cyber attacks across the organization.

Unlike legacy firewalls that are based on a "layered security" architecture, Palo Alto Networks next-generation firewalls use a unified security design that classifies all traffic into full context before applying one set of flexible security rules in a single pass. This makes policies far easier to understand and enforce, while also greatly improving the overall speed, and removing additional points of failure.

HOW THE INTEGRATION WORKS

To illustrate the integration, we will consider a common IoT infection as an example. In this case, we will look at a compromised printer, although the same scenario would apply to any number of other device types. Like many IoT devices, printers often have a combination of wired, WiFi, and Bluetooth connectivity options. Let's assume the device has been compromised by BlueBorne. This initial infection would not be seen by traditional security as it was a direct device-to-device connection over the Bluetooth protocol.

Once compromised, the device may attempt to scan the local internal environment, connect to new devices, and ultimately to reach out to a remote command-and-control server on the Internet. Let's see how the combined Armis and Palo Alto Networks solution would respond:



1. **Device Visibility**
   First, Armis provides visibility over all devices and all their connections. With the ability to monitor WiFi, Bluetooth, and dozens of other protocols, Armis is able to see the printer and classify it as such automatically. Armis would also be able to see the initial infection over Bluetooth, as well as WiFi.

2. **Detect Threat**
   Armis also continuously monitors the behavior of all devices and detects abnormal and malicious behavior. Behavior baselines are established based on Armis's global database of device behaviors, comparison to other similar devices in the local environment, as well as the specific device's history. When the compromised printer begins attempting to connect to other hosts on the network, Armis immediately recognizes that it is compromised and takes action based on policy. This could include blocking any wireless connections from the host in addition to informing the firewall (see step below).

3. **Notify the Firewall**
   Next, we need to ensure that we can block the command-and-control traffic and prevent any data exfiltration. To do this, the Armis automatically notifies the next-generation firewall and adds the IP address of the compromised device to the dynamic block group.

4. **Block Threat**
   The Palo Alto Networks firewall blocks all traffic from the compromised device.

This approach allows organizations to add control over all their devices on both the wired and wireless side, and tie this new intelligence to the central network security policy that lives in the firewall.

THE NEW ENDPOINT

Enterprise security teams increasingly face a new breed of endpoint in their networks. With full network stacks and operating systems, these devices are typically as capable as a tradition endpoint, yet often cannot support a security agent and are difficult to update. These devices also contain a variety of connectivity options that are designed to connect and work right out of the box. This means that these devices are often the most active and flexible at the access layer beyond the reach of traditional perimeter controls. Here are a few common categories and examples of this new and challenging type of endpoint.

- **IoT Devices.** HVAC systems, security systems, lighting systems, security cameras, refrigerators, vending machines, smart TVs, etc.
- **Personal Devices.** Smart devices, smart speakers, streaming media, or digital assistants (Amazon Echo, Apple watch, etc).
- **Industry-Specific Devices.** Industrial Control Systems, medical devices (patient monitoring systems, mobile imaging systems, infusion pumps, communication badges, etc), retail etc).
- **Office Devices and Peripherals**. Printers, VoIP phones, TV screens and monitors, Bluetooth keyboards, headsets, etc.

With Palo Alto Networks and Armis working together, businesses can broaden their security footprint past the perimeter all the way to the access layer to address these new devices.

DEVICE KNOWLEDGEBASE

In a world where you can't put a security agent on a device, and billions of new devices are coming online, you need a new way to identify what each is doing at any given time. Armis' unique approach is to bring a deeper and more profound understanding of how a device should and should not behave. Armis has the largest Device Knowledgebase available today. It is a "crowdsourced" knowledgebase that continuously learns and evolves based on every device in and around deployment environments and Armis' labs.

The Device Knowledgebase provides unique visibility into devices, letting us see and learn how they behave. Armis supplements this with external threat feeds, vulnerability databases, among others. We can mix and match devices, their make up and capabilities to extrapolate risk factors. We leverage machine learning and the Armis Risk Analysis Engine to apply at scale, comparing observed device characteristics and behavior against a baseline of normal behavior. This gives Armis critical insights that determine if a device should be disconnected from the organization, if, for example, it is exhibiting signs of being part of a botnet.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets.

www.paloaltonetworks.com

ABOUT ARMIS

Armis eliminates the IoT security blind spot, protecting enterprises from the threat of unmanaged or rogue devices and networks. Fortune 1000 customers trust Armis' agentless IoT security platform to discover unmanaged devices, analyze their behavior, and protect your critical information and systems. Armis is a privately held company and headquartered in Palo Alto, California, with an office in Tel Aviv.

www.armis.com

Sources

[1] Aug 2017 TechRepublic/F5 "Report: IoT attacks exploded by 280% in the first half of 2017"

armis

1.888.452.4011
armis.com