REPORT REPRINT

Armis Scales with Agentless Approach to Unmanaged and IoT Device Security

PATRICK DALY

23 AUG 2018

With new funding under its belt and a little over a year in the market, Armis has exhibited solid growth across multiple metrics and made several advances in developing its go-to-market strategy.

451 Research®

Armis has been in the market for just over a year with an IoT security platform designed to provide visibility, threat detection and policy enforcement for unmanaged and IoT devices and the company continues to grow as it begins to scale its operations. A series B round in April added to the significant level of funding that has enabled Armis to quickly ramp up product development, sales and marketing efforts. The result has been the Armis Device Knowledgebase containing over six million unique behavioral profiles and new partnerships and integrations with complementary products and continually increasing employee and customer counts.

THE 451 TAKE

Armis' growth over the last year has been impressive, although not necessarily unexpected. Many enterprises struggle to keep up with the proliferation of unmanaged and IoT devices entering their environments and lack up-to-date device inventories, visibility into device operations and the necessary controls to mitigate risk when a device is compromised. All these challenges increase the value of a platform like Armis' to the enterprise. The company's Device Knowledgebase is perhaps its strongest asset, with the unique behavioral characteristics of each device the company has discovered to date constituting roughly six million device identities that can be leveraged to detect threats based on behavioral abnormalities. At the same time, the company has established a solid go-to-market strategy with a combination of direct-to-enterprise sales and technology partnerships, most notably a joint offering with Palo Alto Networks' NGFW. While Armis is one of only a handful of vendors directly targeting visibility and control of unmanaged and IoT devices in the enterprise right now, the competition may begin to heat up soon as the number of unmanaged and IoT devices in the enterprise continues to increase and vendors take note of the growing opportunity.

CONTEXT

Armis, which was founded in 2015 and officially exited from stealth mode in June 2017, has grown significantly in the last year across several measurable criteria. An additional $30m in series B funding raised in April from Sequoia Capital, Bain Capital Ventures, Red Dot Capital Partners and Tenaya Capital brought total investment in the company to $47m. Employee counts more than doubled, from about 30 at its launch to 70 today, while customer count grew from 15 to several dozen over the same period. Armis is primarily focused on selling to large enterprises and counts several Fortune 100 companies among its customers.

In addition to its product portfolio, the company regularly conducts research on the vulnerabilities and threats affecting IoT and other unmanaged devices. Armis identified a Bluetooth-based vulnerability called BlueBorne that it claims affects over 5.3 billion devices, and can be used for a range of attacks including remote code execution on the targeted device. Armis recently published a report expanding upon research done into the DNS Rebinding vulnerability by leveraging its Device Knowledgebase to estimate the number and type of vulnerable devices.

PRODUCTS

Armis is an agentless offering that deploys as a virtual appliance that plugs into a switch on the customer's network to passively discover and profile all devices in the environment, managed and unmanaged, and identify potential threats affecting or stemming from those devices. By default, the product does not trust devices connected to the corporate network as it continuously monitors traffic for anomalous activity. Behavioral analysis engines alert to anomalies and the customer has the option to manually follow up or enable Armis to automatically enforce policies that would remove the affected device from the network. For the most part, Armis says that customers prefer to go the manual route due to the possibility of inadvertently disrupting the business if a given device is cut off from the network. A typical response is for Armis to open a ticket in the customer's SIEM or orchestration platform to initiate the incident response platform.

To effectively analyze all device behavior, Armis has built a Device Knowledgebase at the back end that currently consists of over six million unique device profiles. Profiles are built using information around device type, observed behavior, connections to other devices and resources on the network, reputation, firmware version, data stored at rest on the device and the device's history of compromise. New profiles are added to the Knowledgebase as they are discovered, creating a sort of network effect in which the product's ability to quickly and reliably identify abnormal behavior increases with each new deployment. Armis has also built a threat analysis engine that applies a risk score to alerts, leveraging the Knowledgebase's understanding of how each device interacts with network resources to determine the potential for an attack to escalate in conjunction with historical data on the severity of previous instances where the same type of device exhibited the same behavior.

Armis integrates with various other aspects of a company's security workflow. Integrations with Phantom, Splunk and ServiceNow enable alerts to be automatically fed into these platforms for incident response. Other integrations with Palo Alto Networks, Cisco's Identity Services Engine and Aruba ClearPass facilitate Armis' active enforcement capabilities by allowing policies defined in Armis' dashboard to be automatically enforced at the network switch. Armis is a NextWave Technology Partner with Palo Alto Networks, providing an integrated offering where alerts from Armis are used to automatically change rules in Palo Alto's NGFW to block threats, extending Palo Alto's own enforcement capabilities beyond managed devices to unmanaged ones.

STRATEGY

The Palo Alto Networks partnership illustrates one potential avenue for Armis' go-to-market efforts; namely, by working with networking equipment and firewall vendors to become truly device aware and extend their monitoring and enforcement capabilities beyond managed devices connected to the corporate network. This value proposition was a large part of the motivation behind Cisco's acquisition of Duo in early August.

As Armis scales its sales and marketing efforts, another opportunity is to sell into SMBs and smaller enterprises. Right now, Armis is focused primarily on marketing its product to large enterprises, which makes sense given that these organizations are more likely to have sufficient budget for the security resources necessary to conduct incident response on alerts generated by the platform. However, MSSP partnerships that would deliver Armis' offering to the MSSP's customers as a fully managed service could open the door for SMBs to benefit from the visibility into the activities of unmanaged and IoT devices and enforcement capabilities that Armis is able to offer.

COMPETITION

There are a few pure-play IoT security vendors with offerings aimed at providing visibility and management for IoT and unmanaged devices. ZingBox and SecuriThings are two such companies, although they differ in the degree of active capabilities offered and deployment models. ZingBox's offering is most similar to Armis' in terms of messaging; it passively monitors traffic from connected devices and builds device profiles combined on observed behavior and other characteristics of the device, similar to Armis' Device Knowledgebase. However, unlike Armis, ZingBox focuses mostly on providing this intelligence for medical devices.

SecuriThings differs from both ZingBox and Armis in that it installs an agent on IoT devices that have the processing power required to do so. The agent then collects device telemetry and is used for automatic policy enforcement. This approach is unlikely to work in all cases because there are still some low-resource embedded devices that it will be difficult to fit an agent on, but in those cases SecuriThings takes a passive approach.

Outside of these pure plays, Armis competes for budget mostly with the NAC space (although the technological approaches differ and Armis could complement a NAC implementation) and those vendors now espouse a 'zero-trust' approach. NAC offerings provision access, but then typically assume that a device is trusted once it gains access to the network. NAC offerings are more concerned with ensuring that the right devices connect to the network than they are with ensuring that those devices are exhibiting normal behavior while connected, which Armis does.

Armis also detects threats in real time. In response, several vendors have begun marketing zero-trust access, which would more accurately be called conditional access management, which allows a device to access certain network resources while never assuming it is trusted on the network. For example, Centrify and Duo monitor user behavior and account misuse to ensure that user accounts are not attacked. Armis claims that its specialized Device Knowledgebase gives it an advantage over these vendors that are more focused on user behavior and account misuse without the need for an agent on the device.

SWOT ANALYSIS

STRENGTHS

With the Device Knowledgebase automatically growing with every new device that Armis discovers, the company has created a positive feedback loop whereby the effectiveness of its offering and its value to customers grows with each new customer deployment.

WEAKNESSES

Without an agent, Armis needs to rely on network data to gain an understanding of normal device behavior and detect threats rather than having access to the device itself, although this is by design due to the resource constraints of many IoT devices precluding the deployment of a traditional agent.

OPPORTUNITIES

While Armis is mostly focused on the Fortune 1000 right now, establishing a few partnerships with prominent MSSPs could help provide a path to market with SMBs that are beginning to grapple with IoT security concerns as well.

THREATS

As the opportunity in unmanaged and IoT device security becomes more tangible, the number of competitors entering the space is likely to accelerate. As market competition increases, it may become more difficult for Armis to differentiate.