Brought to you by Informa Tech
OMDIA

Publication date:
03 Jun 2022
Author:
Hollie Hennessy, Senior Analyst, IoT Cybersecurity

On the Radar: The Armis Visibility Platform spans IoT, IT, and OT assets

Summary

Catalyst

Armis offers an agentless asset intelligence platform. Initially designed for Internet of Things (IoT) devices but now also utilized for OT, healthcare, and traditional IT environments, the platform looks to provide an asset inventory, identify security issues, and pave the way for response actions with a range of integrations.

Omdia view

OT, medical, and IoT devices can significantly widen an organization's threat and risk landscape, especially if they are unmanaged.

In critical national infrastructure (CNI), IoT devices are often utilized at scale – such as in a hospital where there can be up to 15 devices per hospital bed, or in energy and industrial settings. In an environment with converging operational technology (OT) and IT networks, IoT devices add another layer that needs securing.

During 2021, there was a sharp rise in ransomware attacks, including notable attacks on CNI, such as the Colonial Pipeline attack in May of that year. A breach involving IT, OT, or IoT devices can allow a hacker to move laterally between devices and networks in order to deploy ransomware – or some devices can even have ransomware deployed on them, be rendered inoperable, or have their data's integrity compromised.

These recent breaches have renewed focus on securing CNI and the necessity of including OT and IoT devices in that scope.

The COVID-19 pandemic has fueled a change in an organization's threat landscape. Bring your own device (BYOD) is now more popular, with employees connecting a range of personal devices to an organizational network. This extends the broad range of devices that need securing in other verticals, including retail and higher education.

Why put Armis on your radar?

Armis's roots in IoT make it a significant player in the market. With over 2 billion devices tracked, and tens of millions of device behavioral profiles identified, it has a solid background of intelligence and data to secure a wide range of devices. However, compared to OT and IT in number of deployments, IoT has some "catching up" to do. Thus, Armis has taken its offering of asset intelligence to both OT and IT settings, as well as IoT, compared to some other vendors that tend to focus on IT in combination with OT and IoT.

Market context

Visibility is one of the key areas within OT and IoT cybersecurity technology. There can be hundreds, or even thousands, of devices that are not accounted for, regularly looked at, or monitored, which can cause significant risk. Visibility is often seen as one of the first steps toward securing these devices – with the idea that you cannot protect what you cannot see or do not know about.

In certain verticals, such as CNI, the impact of a potential breach or hack can be more detrimental to companies, their employees, and their customers. Such incidents can cost thousands, if not millions of dollars, in operational downtime, cause disruption for civilians, and even be life threatening.

Another layer of complication within critical infrastructure is that these networks traditionally rely on an internal-only network connection, such that they are known as "air gapped" networks, and are therefore deemed secure. However, technological advancement, the convergence of OT and IT networks, and the introduction of IoT technology has opened up these devices and assets to more potential breaches and risk, despite the benefits of increased efficiency and analysis.

In addition, many devices run on legacy protocols rather than standard ones like TCP/IP, are difficult (or impossible) to update, and need very careful consideration over when they can actually be patched, monitored, or modified so as not to disrupt critical operations.

An overarching view of the assets on the network, including numerous IoT devices, as well as potential risk, vulnerability, and anomalies, is necessary. The Armis platform looks to provide this view, combining detection, visibility, classification, and alerting.

Product/service overview

The Armis product is a standalone platform – a technology that feeds data into its backend knowledge base for normalization, correlation, and analysis. Data is gathered by collectors deployed by Armis, either physical or virtual, on a network span port or as a network tap, and compared to a library of over 2 billion devices. Its data is generally from packet headers, so encrypted traffic is not a barrier. Armis also integrates with existing IT and security solutions to gather advanced data about each asset to enrich the details of everything it finds. Armis can also deploy with no collectors, at the request of its customers, using only telemetry from existing tech solutions.

The data is then fed back to the customer's security operations teams for further analysis and action if deemed necessary. While the platform provides visibility of devices and detection of anomalous activity, as well as alerting to potential issues, some response capabilities are not included, leaving a gap for Armis to partner with other vendors and allow customers to utilize their existing security technology.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Armis's technology connects to other systems, whether for telemetry data or to enable enforcement and orchestration, such as a vulnerability management system. If something anomalous is flagged, it can trigger a scan on demand, for example.

Company information

Background

Armis is a cybersecurity solutions provider, now headquartered in Palo Alto, California. The company was founded in 2015 by CEO Yevgeny Dibrov and CTO Nadir Izrael, previously of the Unit 8200 intelligence arm of the Israel Defense Forces (IDF).

Armis currently has over 600 employees and expects to double its headcount in 2022. It has raised more than $600m to date, with its latest round at $300m announced in November 2021, led by One Equity Partners, with existing investors that include Brookfield Technology Partners, Insight Partners, CapitalG, and Georgian also taking part. It aims for floatation in 2024.

Current position

Although Armis began with its sole focus on IoT, over the past two to three years it has seen its customers and business expand into the areas of OT, healthcare, and IT; i.e., it is not just the OT/IT convergence that brings its own security risks, needs and necessities, but also securing the IT environment as a standalone.

Thus, its customers range from those looking to gain visibility and secure IoT, such as in Amazon or Walmart warehouses, to those that are looking to secure OT and purely IT networks. The charging mechanism for the Armis platform varies. Unlike some other models for IoT cybersecurity software, it rarely prices by device, although the company stresses that the pricing mechanism is flexible, depending on the client's type of operation. In general, the calculation takes into account company size, full-time equivalents (FTEs), etc.

Future plans

Armis is currently strongest in the US market but is looking to expand its customer base and presence in Europe – where it plans to sell through partners and channels rather than directly.

In addition, Armis is working on partnerships for Japan and Latin America. Armis does not offer managed services alongside its technology, and this paves the way for future partnerships. Current partners include CrowdStrike, IBM, Check Point, SentinelOne, Torq, Cisco and Optiv.

In terms of verticals, Armis is present in many – with a focus on medical and industrial/manufacturing, given its beginnings in IoT. It hasn't had a particularly strong presence in financial services, but the company identifies that sector as a growth area.

This multi-vertical proposition is somewhat different to Armis's major competitors – such as Nozomi Networks and Dragos, whose focus is on industrial IoT – and was also that of Claroty's until its Medigate acquisition in December 2021 allowed it to expand its presence in the medical space.

Regarding the technology itself, Armis's additional funding round looks to support acquisitions. The company is focusing on two areas of interest, AI technology and better graphing technology, both for its internal insights and for additional and elevated threat visibility for the customer.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Key facts

Table 1: Data sheet: Armis

Product/service name	Armis Asset Intelligence Platform	**Product classification**	SaaS
Version number	22.1	**Release date**	Quarterly
Industries covered	Manufacturing, healthcare, IT/enterprise, retail, public sector, energy & utilities	**Geographies covered**	Global
Relevant company sizes	5,000+	**Licensing options**	Per FTE or per site
URL	www.armis.com	**Routes to market**	Channel
Company headquarters	Palo Alto, CA	**Number of employees**	600+

Source: Omdia

Analyst comment

Armis is a relatively new company compared to its significant rapid growth and market valuation ($3.4bn as of its last funding round). The vendor positions itself within the realm of IoT, but its agentless, passive technology allows for quick, effective deployment spanning IoT, IT, and OT – with minimal downtime and disruption, which is vital when it comes to operational technology.

Unlike others in the space, it does not limit its focus to one vertical. That said, the lack of focus on one vertical does not hold the vendor back: Armis's asset knowledge, from extensive asset intelligence, is vast, impressive, and difficult to rival. Its ability to be deployed in traditional IT or OT environments, as well as in the convergence of the two, plus IoT, makes Armis an attractive option, even in areas where IoT devices are not utilized at scale.

However, in the IT space, there is a potential use case for identifying virtual assets in a hybrid environment. Although it can identify both virtual and cloud assets, as it operates largely in the IoT/OT space, it is nearly always on physical networks.

Armis's integration and partnerships with an extensive range of vendors is significant. This strengthens its go-to-market strategy and allows it to orchestrate response. Thus, the Armis Platform can be utilized in many scenarios above and beyond asset inventory and anomaly detection, from alerting and ticket creation, through to enforcing policy, triggering scans, and patching devices.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Market Landscape: Industrial IoT Cybersecurity Operation and Management Solutions (June 2020)

Fundamentals of Security Operations Solutions for Operational Technology and the Industrial Internet of Things (April 2022)

On the Radar: P-X Systems provides detection nodes for OT networks (April 2022)

On the Radar: Dragos offers security for ICS/OT networks (February 2022)

Author

Hollie Hennessy, Senior Analyst, IoT Cybersecurity

askananalyst@omdia.com

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com