WAVE REPORT

The Forrester Wave™: IoT Security Solutions, Q3 2025

The Nine Providers That Matter Most And How They Stack Up

Paddy Harrington and three contributors

IN THIS RESEARCH

Summary

In our evaluation of IoT security solutions providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps you select the right one for your needs.

IoT Security Solutions Are A Crucial Component Of Your Enterprise Security

Internet-of-things (IoT) devices are now part of every organization, no matter the industry, location, or size. Ranging from printers, motion sensors, and smart assistants to warehouse scanners, infusion pumps, and smart meters, these purpose-built devices are essential to daily operations. However, resource restrictions mean these connected devices often lack the same local security functions of standard endpoints — desktops, servers, mobile devices — and are more susceptible to being attacked and compromised. The Mirai botnet in 2016 exposed the vulnerability of certain IoT devices, and this led to vendors introducing solutions to identify the risks incumbent to these devices. The increasing rate of attacks and their evolving complexity highlight the need

for security leaders to implement proper IoT security solutions to reduce the threats coming through these ubiquitous devices.

IoT security solutions customers using this evaluation to inform a purchase decision should consider:

- **Asset discovery is crucial, but not the only critical capability.** You can't protect what you don't know is there, and for many businesses this means discovering and classifying hundreds of thousands to millions of devices across a global infrastructure. This task can take months to complete but is just one component of protecting your IoT environment. Staging your discovery project to uncover your critical assets first will allow you to move to evaluating communication paths and implementing proper segmentation, addressing vulnerabilities and risks within the uncovered devices before moving onto the next set of assets.

- **Vulnerability management and risk posture management are not the same.** Vulnerability management focuses on identifying, prioritizing, and remediating vulnerabilities in IoT devices, including firmware and network services, whereas risk posture management assesses the overall security of the IoT ecosystem, including device trustworthiness, network segmentation, and operational context. Prioritize vulnerability management within your IoT security solution, especially if you have an enterprise risk posture management platform. Both functions improve infrastructure security and reduce the threats that come through your IoT devices.

- **New IoT infrastructure policies must not introduce issues to operations.** From vulnerability mitigation to network segmentation, before a policy is deployed

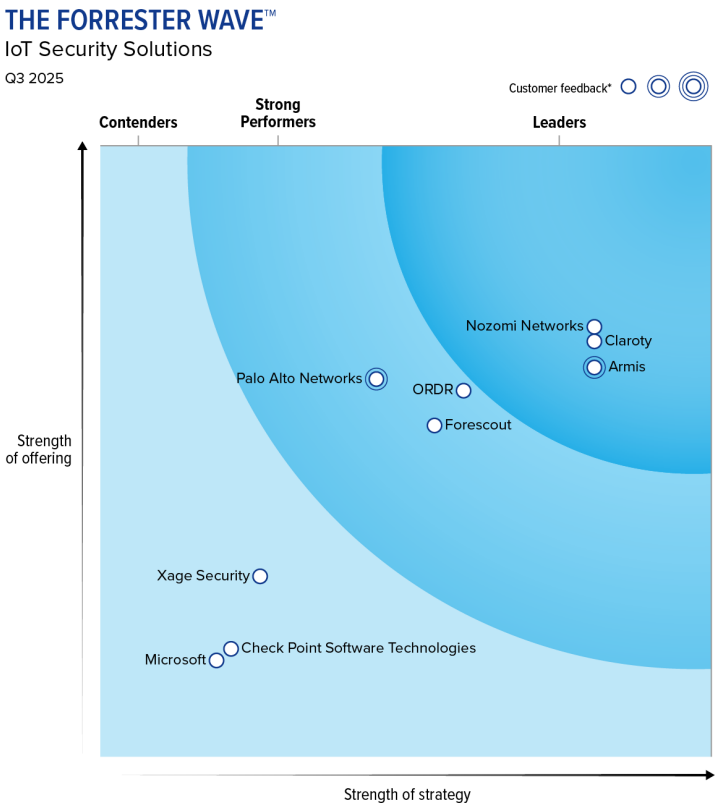
within your IoT environment, your analysts need to assess the impact of these changes, as they can have severe ramifications on your business processes. A printer being inaccessible can be annoying, but a bar code scanner in the warehouse unable to communicate with the order-processing application can delay shipping and miss customer SLAs. It's important that your IoT security platform reviews your proposed policy changes to reduce operational issues.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, and Contenders (see Figures 1 and 2). We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt the findings based on their priorities using Forrester's interactive provider comparison experience.

FIGURE 1

Forrester Wave™: IoT Security Solutions, Q3 2025



*A halo indicates above-average customer feedback. A double halo indicates that the vendor is a Customer Favorite.

FIGURE 2

Forrester Wave™: IoT Security Solutions Scorecard, Q3 2025

	Forrester's weighting	Armis	Check Point Software Technologies	Claroty	Forescout	Microsoft	Nozomi Networks	ORDR	Palo Alto Networks	Xage Security
Current offering		3.58	1.64	3.76	3.18	1.56	3.86	3.42	3.50	2.14
Device identification and classification	10%	5.00	1.00	5.00	3.00	1.00	5.00	3.00	3.00	1.00
Vulnerability assessment and resolution	10%	5.00	1.00	5.00	3.00	1.00	3.00	3.00	3.00	1.00
Risk posture management for IoT infrastructure	9%	3.00	1.00	5.00	3.00	3.00	5.00	3.00	3.00	1.00
Identity and access management	5%	1.00	3.00	1.00	5.00	1.00	3.00	3.00	3.00	5.00
Encryption support	5%	1.00	3.00	3.00	3.00	1.00	1.00	3.00	3.00	3.00
Network segmentation and microsegmentation	10%	3.00	1.00	5.00	3.00	1.00	3.00	5.00	5.00	3.00
Network threat monitoring	10%	5.00	3.00	3.00	3.00	1.00	5.00	3.00	5.00	3.00
Device threat monitoring	5%	3.00	1.00	3.00	3.00	1.00	5.00	3.00	3.00	3.00
Device configuration monitoring and management	5%	3.00	1.00	5.00	3.00	3.00	5.00	5.00	1.00	1.00
Security operations integration	5%	3.00	1.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Compliance mapping	5%	5.00	1.00	1.00	1.00	1.00	3.00	3.00	5.00	1.00
Orchestration and automation	5%	3.00	3.00	3.00	5.00	1.00	3.00	5.00	3.00	3.00
Reporting and analytics	3%	3.00	3.00	3.00	3.00	1.00	3.00	1.00	3.00	3.00
Threat intelligence	5%	3.00	1.00	3.00	3.00	3.00	5.00	3.00	5.00	1.00
Deployment options	4%	3.00	1.00	5.00	5.00	3.00	3.00	5.00	1.00	3.00
Artificial intelligence capabilities	4%	5.00	3.00	3.00	3.00	1.00	5.00	3.00	5.00	1.00
Strategy		4.30	1.80	4.30	3.20	1.70	4.30	3.40	2.80	2.00
Vision	20%	5.00	1.00	5.00	3.00	1.00	5.00	3.00	3.00	1.00
Innovation	15%	5.00	3.00	5.00	3.00	1.00	3.00	3.00	3.00	3.00
Roadmap	20%	5.00	1.00	5.00	3.00	1.00	5.00	3.00	3.00	1.00
Partner ecosystem	10%	3.00	3.00	5.00	3.00	3.00	3.00	3.00	3.00	1.00
Adoption	10%	5.00	1.00	3.00	3.00	1.00	3.00	5.00	3.00	3.00
Pricing flexibility and transparency	10%	3.00	1.00	3.00	5.00	3.00	5.00	5.00	1.00	3.00
Supporting services and offerings	15%	3.00	3.00	3.00	3.00	3.00	5.00	3.00	3.00	3.00

Scores are on a scale of 1 (below par relative to others evaluated) to 5 (superior relative to others evaluated).

Leaders

Nozomi Networks

Founded in 2013 with a focus on industrial control systems' visibility and security, Nozomi Networks' mission has been to protect the devices that keep businesses

running. Nozomi has since evolved its platform to address the increasing array of IoT devices and stay ahead of market changes and security threats.

- **Strategy.** Nozomi understands the growing attack surface of IoT networks, and its vision is to make its Vantage platform a leading solution for IoT security management. Its roadmap reflects this ambitious vision, supported by significant R&D investments. Transparent pricing helps its customers plan deployments effectively, ensuring they can integrate IoT security into their broader cybersecurity initiatives.

- **Capabilities.** Nozomi provides differentiated IoT asset discovery with support for complex building management system protocols as well as Wi-Fi, Bluetooth, LoRaWAN, and 5G. This not only assists its risk posture management functions but also allows wider threat monitoring functions at both the device and network level. Nozomi's advanced AI model choices further reduce uncertainty and increase the accuracy of detected threats. However, its encryption support only monitors the state and use of cryptography; it doesn't control the use of cryptography by IoT devices.

- **Customer feedback.** Reference customers praised Nozomi's strength in finding assets across the entire enterprise and noted its support throughout all the deployment phases. However, they found its vulnerability management was a step behind, and some customers had challenges with the user interface. Only one of Nozomi's reference customers responded to Forrester's outreach for this evaluation.

- **Forrester's take.** Nozomi's approach to protecting all digital assets is best suited to customers who are looking to make IoT security a priority in their organization and not just another division of endpoint

security.

View Nozomi Networks' detailed scorecard.

Claroty

Claroty entered the security space in 2014, offering on-premises, passive monitoring solutions for operational technology (OT) devices. It acquired Medigate in 2022 and expanded its xDome platform to protect extended IoT (xIoT) and OT devices. It has broadened its xIoT coverage across markets and now focuses on asset-targeted protection.

- **Strategy.** Claroty's pivot to asset-targeted protection reflects its vision of enhancing its platform to meet customers at various stages of their IoT security journey. It has built market-specific sales and technical teams to ensure smooth solution adoption, while gathering customer feedback to inform product improvements, introduce innovative features, and build a strong roadmap. Claroty extends this market focus to partnerships: It has a network of channel vendors that understand industry-specific challenges in complying with regulations and industry standards.
- **Capabilities.** Claroty delivers detailed insights into discovered assets, using passive monitoring, safe active queries, and integration with enterprise configuration management databases (CMDBs). This data enables analysts to assess vulnerabilities, gauge risk posture, and design effective network segmentation policies that can be tested prior to deployment. However, the platform can't integrate identity and access management (IAM) functions with enterprise certificate authorities to better control device identity, and compliance mapping requires purchasing an extra service.
- **Customer feedback.** Customers praised Claroty's

asset discovery and vulnerability analysis capabilities, noting the high quality of its insights. Some suggested the Claroty platform can be challenging for junior analysts, as it requires substantial IoT expertise for optimal use.

- **Forrester's take.** Claroty's market-focused teams mean it's a good fit for customers in different industries who want to secure their IoT assets and OT networks.

View Claroty's detailed scorecard.

Armis

Founded in California in 2015, Armis has steadily expanded its Centrix platform to discover and protect all types of devices. Its acquisitions of CTCI, Silk Security, and OTORIO enable the solution to address diverse customer needs for asset identification, threat detection, and air-gapped network protection.

- **Strategy.** Armis' vision centers on delivering enterprisewide exposure management that goes beyond IoT and OT devices. Its innovation investments and acquisitions support this goal. Its roadmap aligns with customer priorities while anticipating future needs to ensure the platform evolves alongside its clients. This forward-looking strategy fosters successful adoption and helps customers deploy the Centrix platform successfully.

- **Capabilities.** Armis offers a vast inventory of device details, enabling security analysts to assess the state of discovered assets without requiring immediate third-party integration. Key features include vulnerability assessment, remediation, and robust compliance mapping to validate adherence to industry standards. However, Armis requires certificate management integration to take encryption

management beyond monitoring. This prevents the solution from having native IAM control.

- **Customer feedback.** Customers praised Centrix for its overall effectiveness and Armis' commitment to supporting deployments; they valued the vendor's dedication to fostering successful customer relationships. However, some customers have had an issue with maintaining the asset database, which required periodic manual cleanup.

- **Forrester's take.** Armis provides a versatile solution for enterprises looking for asset inventory, vulnerability mitigation, risk management, and least privileged access across industries and device types.

View Armis' detailed scorecard.

Strong Performers

ORDR

Founded in 2015 by technologists from Aruba Networks and Cisco, ORDR entered the IoT security market with network technology and security expertise. Headquartered in California, ORDR originally specialized in healthcare but has expanded its IoT security solution to support customer deployments in other industries.

- **Strategy.** ORDR's vision for securing IoT assets drives its innovation via a roadmap aligned with industry needs. Its guided approach to customer adoption, from purchasing to optimization, ensures long-term deployment success; it's supported by transparent, tiered pricing tailored to market verticals. This model ensures customers only pay for what they need, making it adaptable to diverse business requirements.

- **Capabilities.** ORDR excels in network

segmentation, a critical function for IoT security. From assessment and analysis to policy creation and predeployment simulation, ORDR ensures thorough segmentation and enforces least privilege access rules. Its air-gapped network support is among the best in the market, protecting IoT devices across IT and OT environments. However, its dashboard is in evolution and has components that feel outdated compared with others in this evaluation, and this can present navigation/usability challenges.

- **Customer feedback.** Customers spoke highly of ORDR's relationship with them and felt ORDR's network traffic analysis is top-notch. They also noted that deployments can require too many sensors to find all the assets, while backend automation relies on a lot of scripts, which can be cumbersome to manage.

- **Forrester's take.** ORDR is a great fit for customers seeking comprehensive network segmentation management for their IoT devices.

View ORDR's detailed scorecard.

Forescout

Forescout has been in the cyber asset discovery and protection market since 2000. Based in California, it has grown naturally and via acquisitions — like that of Cysiv in 2022 — to deliver a security infrastructure platform that can secure all types of cyber assets.

- **Strategy.** Forescout's strategy aligns with its customers' IoT security requirements. Its global partner network helps customers migrate along their IoT security path, and it has an industry-accepted approach to customer adoption. Forescout's greatest strength is its pricing options, which are concise and tailored to meet the global demands of its clients.

- **Capabilities.** Forescout's platform addresses the core IoT security functions of asset discovery, vulnerability and risk posture management, and network segmentation. A standout is its complete governance of IAM functions for agentless devices throughout their lifecycle. And it's one of the few vendors in the market that can provide a complete on-premises deployment option, along with cloud and hybrid delivery, to support cloud-averse customers. However, Forescout's compliance mapping capabilities currently lag those of other vendors in this evaluation.

- **Customer feedback.** Customers valued the depths of Forescout's policy engine, from asset discovery to network segmentation to report automation; they felt the solution's modularity helps maintain operational uptime. They also noted that Forescout's modularity can make the solution more complex than others to manage and maintain. Only one of Forescout's reference customers responded to Forrester's outreach for this evaluation.

- **Forrester's take.** Forescout's long history of cyber asset discovery and protection makes it a strong fit for customers looking for an enterprisewide solution to secure their IoT infrastructure.

View Forescout's detailed scorecard.

Palo Alto Networks

Palo Alto Networks is a prominent network and endpoint security provider; it entered the IoT security space via its 2019 acquisition of Zingbox. Utilizing its Strata and Cortex platforms, Palo Alto brings cloud-based, centralized management functions to the IoT security market.

- **Strategy.** Palo Alto Networks aims to be a

comprehensive cybersecurity platform that addresses all enterprise cybersecurity needs, including IoT. Its roadmap and innovation align with this vision, supported by a strong partner ecosystem and effective adoption programs. However, pricing is a drawback: Customers currently have to pay for the broader platform approach that combines Strata and Cortex, while competitors offer equivalent functionality in a single solution.

- **Capabilities.** Palo Alto Networks excels in network threat monitoring as well as network segmentation and microsegmentation, and its native compliance mapping ensures customer environments align with the necessary regulatory and standards governance models. Vulnerability assessment and resolution and risk posture management are on par, but device configuration monitoring and management are only available through other modules in its larger platform. Its cloud-first offering may create some challenges in supporting IoT environments within internet-disconnected networks.

- **Customer feedback.** Customers affirmed Palo Alto Networks' strength in network threat monitoring and deeply appreciated the relationship it has developed with them. Common concerns were that asset identification can be finicky and frequent UI changes as the platform evolves can increase administration and training costs.

- **Forrester's take.** Palo Alto Networks is a good choice for customers that use Palo Alto Networks for other cybersecurity disciplines and are looking to incorporate IoT security.

View Palo Alto Networks' detailed scorecard.

Contenders

Xage Security

Xage Security started in 2016 with a distributed ledger security platform for industrial IoT (IIoT). It has expanded its solution to cover more devices and provide secure remote access, least privilege access, and secure data exchange.

- **Strategy.** Xage's vision is that discovery is not a prerequisite to protection — but we'd argue that if you don't know the depths what you're trying to protect, you can leave gaps in your security. Its innovation has been positive, but its roadmap merely aims to bring its offering up to par with others in this evaluation. Its customer adoption and support programs are solid, and its pricing and licensing flexibility are on par.
- **Capabilities.** Xage's key differentiator is its IAM functions for IoT devices, offering good control of encryption as well as strong network segmentation and threat defense. The only drawback is the need to deploy its Xage Extended Protection (XEP) appliances to support that segmentation functionality; others in this evaluation can support policy deployment across a wide range of vendors. Xage has some native device identification and classification functions, but it relies heavily on integrations to support these, leading to low-quality information for vulnerability assessments and risk posture management.
- **Customer feedback.** Customers valued the overall architecture of the Xage solution and noted how easy it is to work with the vendor. While the broader network segmentation functions were just what they needed, they felt microsegmentation could be a challenge to deploy.
- **Forrester's take.** Xage Security is a good fit for enterprises that have already deployed asset

discovery tools but lack a solution to handle IoT infrastructure protection.

View Xage Security's detailed scorecard.

Check Point Software Technologies

Established in 1993, Check Point Software Technologies has a long history of network security solutions. In 2020, it introduced its IoT Protect solution to expand its device coverage to IoT infrastructures.

- **Strategy.** Check Point's vision for IoT Protect is as an expansion of its cybersecurity platform. This has its benefits for existing Check Point customers but may create obstacles to adoption for those that have adopted security solutions from other vendors. Its IoT security innovation is good, and it provides a solid partner community and quality support services.
- **Capabilities.** Its network threat monitoring is on par, as are its IAM capabilities and encryption support functions. Device identification and classification do not provide the same asset details, automated classification, or the breadth of device coverage of others in this evaluation without the integration of external solutions; this leads to deficits in how it natively handles vulnerability assessments and risk posture management.
- **Customer feedback.** Customers appreciated the relationship they have with Check Point and the solution's integration into Check Point's broader cybersecurity platform. Only one of Check Point's reference customers responded to Forrester's outreach for this evaluation.
- **Forrester's take.** Check Point's IoT Protect suits existing Check Point customers that need to protect their IoT assets.

View Check Point Software Technologies' detailed scorecard.

Microsoft

Microsoft acquired CyberX in 2020 to expand its cybersecurity offerings to IoT and OT devices. Microsoft sees that these devices are not just challenges for specific verticals but also part of enterprise infrastructures across a wide array of markets.

- **Strategy.** While called Defender for IoT, Microsoft's solution focuses primarily and heavily on supporting OT and industrial IoT devices. Microsoft offers services for other IoT devices that are common among all enterprises but not to the depth of other vendors in this evaluation. Its partner ecosystem and adoption focus in the IoT space is on par with its rivals, while its pricing model is a cost-effective add-on to a Microsoft 365 E5 license, which can benefit many customers.
- **Capabilities.** Because the solution leans more toward supporting OT and industrial IoT devices, its enterprise IoT device support for key capabilities like asset discovery, vulnerability assessment and resolution, or network segmentation lag others in this evaluation. Microsoft also relies on other vendors to provide network threat monitoring. The Microsoft platform has good overall risk posture management and device configuration monitoring.
- **Customer feedback.** Customers appreciated that the offering integrates easily into their existing Microsoft 365 cybersecurity infrastructure and doesn't require a significant learning curve for effective use. Microsoft did not provide reference customers for this evaluation.

- **Forrester's take.** Microsoft's Defender for IoT is a good option for existing Microsoft E5 customers who are looking for an easy platform with which to begin their IoT security journey.

View Microsoft's detailed scorecard.

Vendor Offerings

Forrester evaluated the offerings listed below (see Figure 3).

FIGURE 3

Evaluated Vendors And Product Information

Vendor	Product evaluated
Armis	Armis Centrix™ for OT/IoT Security v25.2
Check Point Software Technologies	IoT Protect (R82), IoT Embedded
Claroty	The Claroty Platform
Forescout	Forescout 4D Platform
Microsoft	Microsoft Defender for IoT
Nozomi Networks	The Nozomi Networks Platform
ORDR	ORDR AI Protect
Palo Alto Networks	Strata Network Security Platform and Cortex Platform
Xage Security	Xage Fabric Platform 4.2.0

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Evaluation Overview

We evaluated vendors against three categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies, including elements such as vision and innovation.
- **Customer feedback.** A halo on a vendor's marker

indicates above-average customer feedback relative to the other evaluated vendors. A double halo indicates outstanding customer feedback: We consider the vendor to be a Customer Favorite. As part of this evaluation, we speak with up to three customers of each vendor. We also consider customer input from our previous research.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

- **Broad, enterprise-level support.** The vendor natively provides core functions for this space, such as asset identification and discovery, threat and anomaly detection, and asset vulnerability and risk management; it has a demonstrated track record for supporting large enterprises. The vendor's IoT security solution isn't designed for specific market segments and provides relevant product functionality for a wide range of industries.
- **A solution available for purchase as a standalone product.** The product has its own SKU and pricing. It is not solely available as a free feature within a larger portfolio.
- **Substantial revenue in the market.** The vendor has at least $25 million in annual revenue from its IoT security product in the past four quarters.
- **Mindshare among Forrester's enterprise clients.** Forrester clients frequently mention the product as one they are considering prior to a purchase. We have heard about the product from our clients in the form of inquiries, advisories, consulting engagements, and other interactions over the past year. Other vendors mention this vendor as a competitor.

Other Notable Vendors

The Forrester Wave evaluation is an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market and additional vendors that Forrester considers to be notable for enterprise clients in our corresponding report: The IoT Security Solutions Landscape, Q2 2025.

Supplemental Material

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos and briefings, and interviews with customers (vendors may provide up to three reference customers; we also consider feedback from other customers we've spoken with). We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by July 1, 2025, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with our vendor review policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. We score vendors that met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation in accordance with our vendor participation policy and publish their positioning along with those of the participating vendors.

Microsoft declined to participate in the full Forrester Wave evaluation process. For vendors that are not full participants, Forrester uses primary and secondary research in its analysis. For example, we might use public information, data gathered via briefings, and independently sourced customer interviews to score the vendor. We may ask the vendor for an abbreviated briefing and/or to provide reference customers. We may also rely on estimates to score vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the integrity policy posted on our website.