The Forrester New Wave™: Connected Medical Device Security, Q2 2020

The Eight Providers That Matter Most And How They Stack Up

by Chris Sherman

June 11, 2020 | Updated: June 11, 2020

Why Read This Report

In Forrester's evaluation of the emerging market for medical device security solutions, we identified the eight most significant providers in the category — Armis, CyberMDX, Cynerio, Forescout, Gurucul, Medigate, Ordr, and Palo Alto Networks — and evaluated them. This report details our findings about how well each vendor scored against 10 criteria and where they stand in relation to each other. Security professionals and clinical engineers can use this review to select the right partner for their medical device security needs.

Key Takeaways

Cynerio, CyberMDX, Medigate, And Armis Lead The Pack

Forrester's research uncovered a market in which Cynerio, CyberMDX, Medigate, Armis are Leaders; Palo Alto Networks and Ordr are Strong Performers; and Gurucul and Forescout are Contenders.

Understanding Clinical Use And Device Identification Are Key Differentiators

The best solutions differentiated themselves by addressing the diverse and unique needs of a clinical environment. Accurate device identification across the broadest range of devices helps reduce the burden on security staff looking for complete visibility into their clinical engineering networks.

The Forrester New Wave™: Connected Medical Device Security, Q2 2020

The Eight Providers That Matter Most And How They Stack Up

by Chris Sherman
with Merritt Maxim, Elsa Pikulik, Matthew Flug, and Peggy Dostie
June 11, 2020 | Updated: June 11, 2020

Table Of Contents

Related Research Documents

Best Practices: Medical Device Security

Lessons Learned From The Latest HIPAA Security And Privacy Incidents

New Tech: Medical Device Security, Q1 2020

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Healthcare Requires Specialized Security Tools For Medical Devices

Medical device security is a growing concern for healthcare providers globally as attackers focus on exploiting these especially vulnerable targets. Several cases have been identified over the past few years where attackers directly compromised a medical device as part of overall campaigns against hospitals.[1] Recently, Interpol, the US Department of Homeland Security, and the United Kingdom's National Cybersecurity Centre have all issued warnings to hospitals around the increased risk of cyberattack and ransomware.[2] Unfortunately, the risk is only growing as more connected medical devices are deployed into a clinical environment.[3]

Connected medical devices can make up 74% of the devices on a hospital's network, yet these devices are typically invisible in the eyes of traditional endpoint and network security solutions.[4] The reasons are twofold: First, connected medical devices that have gone through regulatory approval are generally sensitive to unaccounted-for voltage and performance fluctuations and simply cannot support a security agent installation. Second, they are often managed and secured by a different team in the hospital such as clinical engineering, biomedical engineering, and/or medical technology management compared with the rest of the data network where traditional IT management and security resides. The network security tools used by those in charge of the data network and assets (laptops, desktops, mobile devices, servers) generally can't recognize medical device traffic and subsequently offer little protection beyond VLANs and firewalls at ingress/egress points. Specialized medical device security products bridge this divide by providing visibility and control through passive connections to networking infrastructure.

Medical Device Security Evaluation Overview

The Forrester New Wave™ differs from our traditional Forrester Wave™. In the New Wave evaluation, we assess only emerging technologies, and we base our analysis on a 10-criterion survey and a 2-hour briefing with each evaluated vendor. We group the 10 criteria into current offering and strategy (see Figure 1). We also review market presence.

We included eight vendors in this assessment: Armis, CyberMDX, Cynerio, Forescout, Gurucul, Medigate, Order, and Palo Alto Networks (see Figure 2 and see Figure 3). Each of these vendors has:

1. **A solution to secure connected medical devices within a clinical engineering network.** Vendors must supply a network-based security product aimed at preventing, detecting, and/or remediating security threats to a hospital's medical device ecosystem.
2. **An established presence within the healthcare provider market.** Included vendors must have an established presence in the healthcare provider market with at least 40 healthcare provider customers using the vendor's technology to protect clinical devices. At least two enterprise-level (1,000 or more employee) healthcare provider reference customers must be made available to Forrester for participation in this study.

3. **Financial viability.** Vendors must demonstrate financial viability by having a minimum of $40 million funding to date or $10 million in annual revenue for the product in question.
4. **Forrester client interest.** Forrester clients must have demonstrated interest in the vendor's product over the past 12 months.

FIGURE 1 Assessment Criteria

Criteria	Platform evaluation details
Architecture	Where do sensors/appliances need to be placed in the network for typical operation? How many sensors and/or appliances does the typical large hospital (e.g., 500 beds and 2,000 devices) require? What information does the vendor's product require to be transmitted off-premises? How is this data secured (both in transit and at rest)? Does the vendor have a SaaS-based management console? Is there an initial baselining/training period required in the customer's environment, and if so, how long does the vendor recommend?
Analytics and reporting	Does the vendor produce dynamic reports that effectively communicate risks associated with a medical device environment? For example, can environmental context (device brand/type, medical use, department, sensor data type, device usage, etc.) be used to prioritize security alerts? Can these be used to inform risk thresholds for specific devices, allowing admin to align risk segments with the medical, compliance, and/or business value of the devices? Can action be taken directly from a report (e.g., does the vendor offer "clickable" reports)? How is clinical usage and/or workflow tracked for each device? Are baselines for "normal" activity identified for any form of device behavior? Does the product analyze medical data communicated over the network between devices? How is malicious activity identified, and if static, what indicators, active/passive heuristics, deception, and/or ML are used?
Attack response	What are all the remediation and/or response actions available to customers when a security attack/risk is identified (e.g., configuration changes, device quarantine, behavioral block, device removal from network, etc.)? What forms of device/behavioral whitelisting/blacklisting are leveraged in the product, and what are the specifics around how new attack tools and techniques are identified then subsequently protected against?
Threat research	How does the vendor discover new medical device threats and vulnerabilities? Are medical devices the sole focus of threat research, or are other hardware/software assets included (e.g., software as a medical device, workstations, mobile devices, etc.)? How many vulnerability disclosures were made to manufacturers in the past 24 months? How many global unique medical devices are identified within the threat research/device database? How is incomplete/incorrect medical device data in the database dealt with in the product? Are customers allowed to suggest edits to the device database, and if so, can this be done from within the admin console?

FIGURE 1 Assessment Criteria (Cont.)

Criteria	Platform evaluation details
Device visibility	How granular is the classification taxonomy of the devices in the environment (i.e., device function, type, OS/firmware, vendor, and model)? How does the vendor ensure that classification taxonomies remain up to date in light of new devices, vendors, models, etc.? Does the product provide visibility into the network and/or device-level communications protocols? These include medical-specific protocols such as Health Level 7 (HL7), Digital Imaging and Communications in Medicine (DICOM), Integrating the Healthcare Enterprise (IHE), and nonmedical-specific protocols such as Bluetooth, Wi-Fi, and RS-232. Which ones are relevant? Does the vendor provide visibility into data flow/connections with other assets, clinical care teams/users, nonmedical IoT devices, cloud/network connections, and medical device manufacturer/third-party service provider remote logins/updates?
Vulnerability management	Does the product track medical device vulnerabilities (i.e., CVEs and medical device security advisories)? How are these reported on, and what actions can be taken from the admin console?
Integrations	What are all of the native, out-of-the-box integrations with third-party security and IT operations tools. Which are bidirectional, and what are the specific benefits to customers? Which (if any) of these integrations are required for the capabilities the vendor outlined in response to the visibility and remediation sections above?
Vision	How well does the vendor's product vision align to address the major customer requirements for medical device security? How is the vendor positioning its product in relation to other vendors? What differentiating capabilities is the solution or vendor offering?
Roadmap	What are the vendor's short-term (less than 12 months) and long-term (more than 12 months) product roadmap, organized by planned release date? How differentiated is the roadmap from competition? Are the planned features expected to contribute meaningfully to customer and product success?
Market approach	Is the company executing a successful go-to-market approach? Does the vendor have a well-thought-out partner strategy?

FIGURE 2 Forrester New Wave™: Connected Medical Device Security, Q2 2020

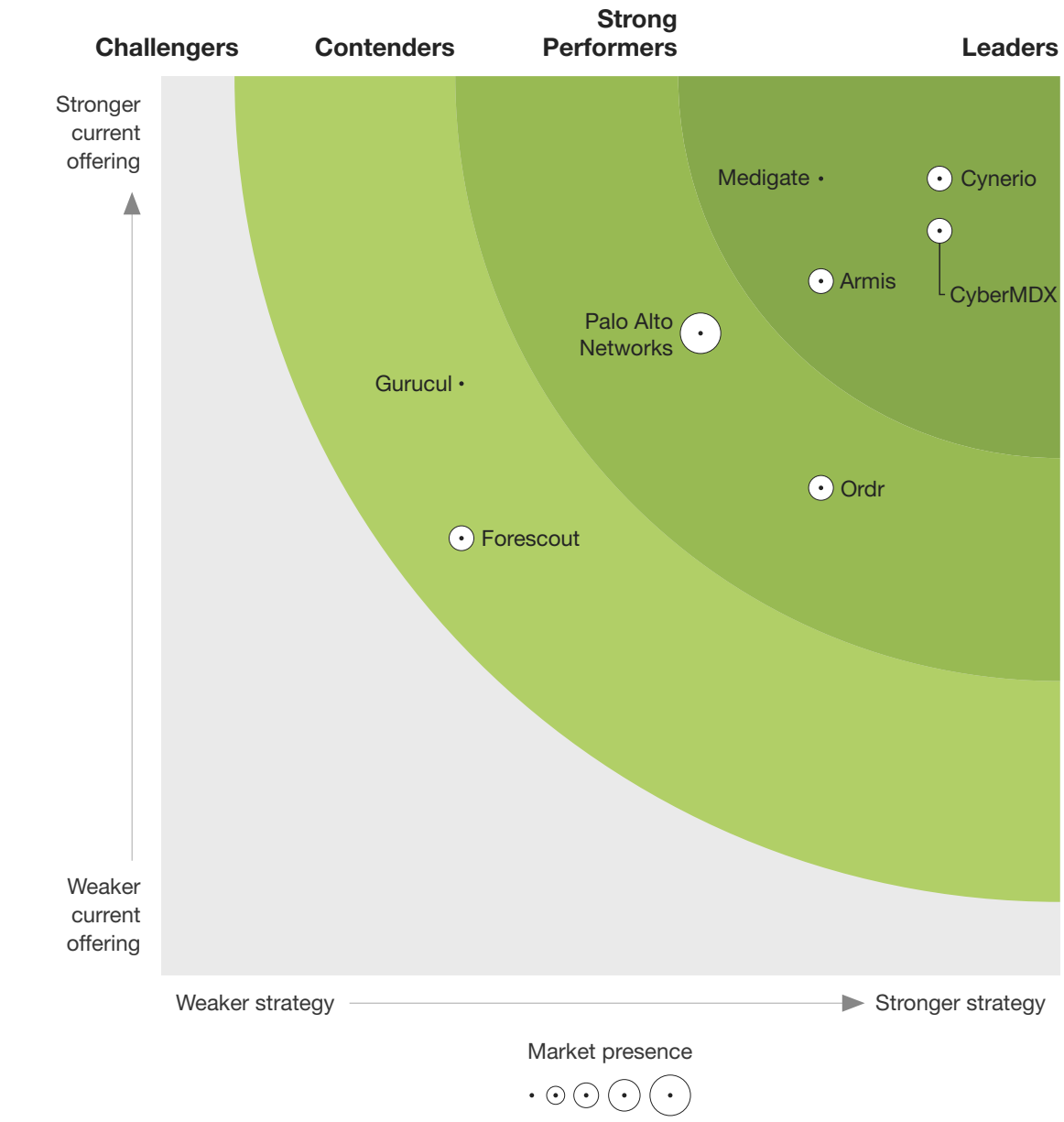
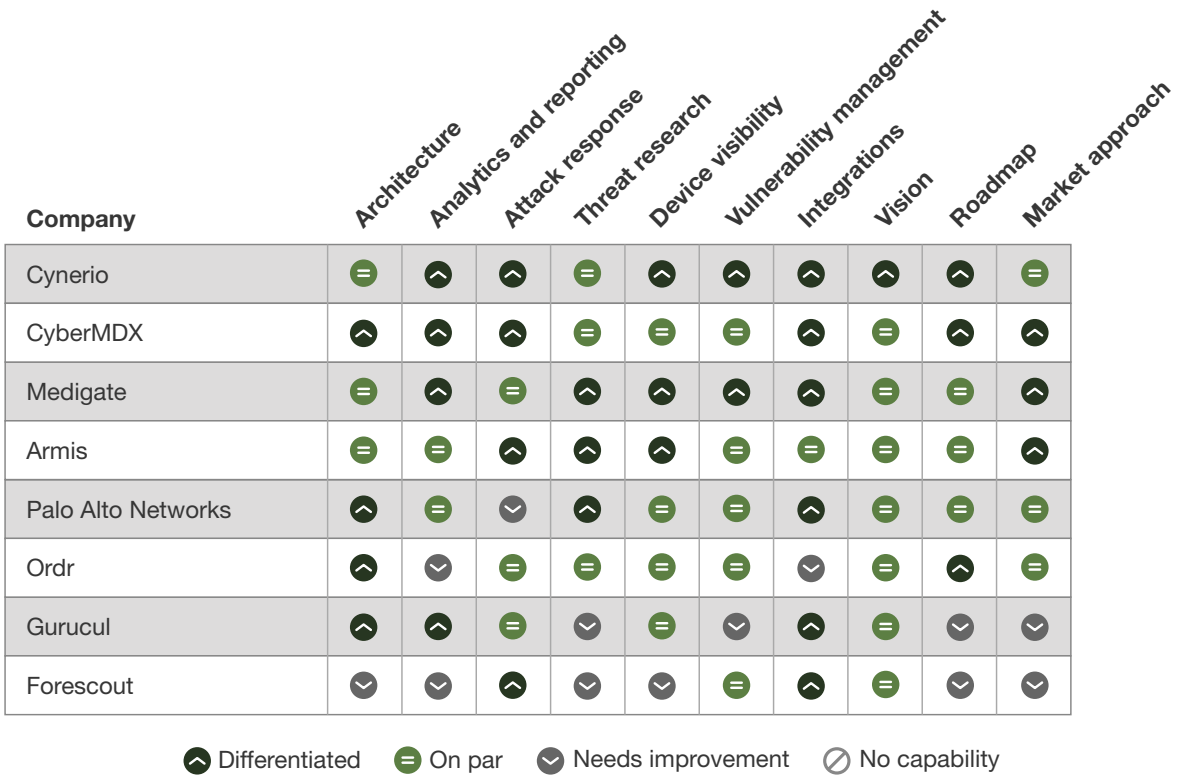


FIGURE 3 Vendor QuickCard Overview



Vendor QuickCards

Forrester evaluated eight vendors and ranked them against 10 criteria. Here's our take on each.

Cynerio: Forrester's Take

Our evaluation found that Cynerio (see Figure 4):

- **Leads with comprehensive threat analytics and clinical insight.** Cynerio offers strong insight into medical device activity and correlations between device telemetry, clinical workflow, and external threat feeds. Unique offerings include MITRE ATT&CK mapping, deception technologies, and MDS2 intake.[5] Its UI is also one of the easiest to navigate.
- **Needs to expand its device identification database.** Cynerio's device identification breadth was average in our evaluation and may not be sufficient for customers who manage a range of new and old devices across medical and enterprise IoT environments.
- **Is best for companies that value technical flexibility.** Cynerio is still small enough that it can respond quickly to changing customer requirements and quickly integrate with many clinical and IT systems.

Cynerio Customer Reference Summary

Cynerio's reference customers were extremely satisfied with the level of device visibility, analytics, and remediation options available across their supported medical devices. Device autosegmentation was frequently cited as a useful feature of the product.

FIGURE 4 Cynerio QuickCard

Cynerio

Wave position
LEADER

= **Architecture**	^ **Vulnerability management**
^ **Analytics and reporting**	^ **Integrations**
^ **Attack response**	^ **Vision**
= **Threat research**	^ **Roadmap**
^ **Device visibility**	= **Market approach**

^ Differentiated
= On par
v Needs improvement
⊘ No capability

Products evaluated
Valor v1.1

REFERENCE QUOTES

"Things that used to take weeks for our team to find and analyze, using Cynerio, it only takes minutes to a day, comparatively no time at all."

"The scope of the product is limited to medical devices and IoT; we would like to see broader capabilities supporting IT devices as well."

CyberMDX: Forrester's Take

Our evaluation found that CyberMDX (see Figure 5):

- **Leads with risk-based segmentation and robust analytics.** CyberMDX provides device analytics including security telemetry, device malfunction data, and utilization metrics. Analysis covers external systems including cloud assets and telehealth systems, with a future vision toward expanding into software-as-a-medical device (SaaMD).
- **Needs to improve investigation complexity and new device identification.** Some of the investigation workflows and tasks can be hard to navigate without more training. Customers also cited timing delays when identifying new devices joining the clinical environment.
- **Is best for organizations trying to move to a Zero Trust security strategy.** The product is able to identify risk levels proactively based on factors such as device behavior, device utilization, clinical use, and device dependencies. Segmentation and containment rules are automatically suggested based on identified risk.

CyberMDX Customer Reference Summary

CyberMDX customers felt the product allowed their security investigation times to be reduced. Further, the product's breadth allows nonsecurity staff to gain value from the product.

FIGURE 5 CyberMDX QuickCard

CyberMDX

Wave position
LEADER

Architecture	Vulnerability management
Analytics and reporting	Integrations
Attack response	Vision
Threat research	Roadmap
Device visibility	Market approach

Differentiated
On par
Needs improvement
No capability

Products evaluated
CyberMDX v4.5

REFERENCE QUOTES

"The product has opened up the ability to take action and have a conversation about our priority levels for threats."

"There can be a few weeks' delay between when a device is connected and when it is reported on."

Medigate: Forrester's Take

Our evaluation found that Medigate (see Figure 6):

- **Offers leading device identification capabilities with behavioral baselining.** Every device identified by Medigate has a behavioral pattern that characterizes "normal" device function. Correlations between deviations from these baselines and network security alerts helps reduce false positives. This is combined with excellent device identification accuracy.
- **Must expand total number of integrations.** Medigate has many strong, bidirectional integrations, such as with Forescout and those that enable "virtual patching," but the number of total supported integrations is still limited compared with other vendors in this study.
- **Best fits companies with complex clinical environments.** Medigate has a very hands-on approach with customers that enables a lot of product customizations. This is especially useful in overly complicated environments with unique needs.

Medigate Customer Reference Summary

Medigate's customers informed Forrester they are very happy with the product's ability to detect and quickly respond to new cyberattacks in their environment. The quality in technical support was consistently cited as a differentiator.

FIGURE 6 Medigate QuickCard

Medigate

Wave position
LEADER

= **Architecture**	^ **Vulnerability management**
^ **Analytics and reporting**	^ **Integrations**
= **Attack response**	= **Vision**
^ **Threat research**	= **Roadmap**
^ **Device visibility**	^ **Market approach**

^ Differentiated
= On par
v Needs improvement
⊘ No capability

REFERENCE QUOTES

"When choosing a vendor, we valued Medigate's expertise in medical device security."

"Keeping up with the pace of new features is challenging."

Products evaluated
Medigate Device Security Platform

Armis: Forrester's Take

Our evaluation found that Armis (see Figure 7):

- **Offers a comprehensive medical and enterprise IoT security solution.** Armis combines threat prevention and detection for the broadest ranges of devices. Armis has extensive device identification capabilities and threat research/analysis for complete device protection.
- **Lacks the same level of clinical insight as others in the study.** While Armis offers insight into medical device protocols like HL7, HLE, and DICOM, insight into clinical context and dependencies takes more effort to extract from the solution compared to others in this study.
- **Is best for companies seeking a security solution for clinical engineering and IT.** Armis is building a platform that will protect all medical and IT network endpoints. This is useful for healthcare providers who want a security solution that can bridge the divide between IT and clinical engineering security teams.

Armis Customer Reference Summary

Armis' customer references appreciated the level of insight they got into user access and device behavior. References noted issues with false positives, but acknowledged this is improving.

FIGURE 7 Armis QuickCard

Armis

Wave position
LEADER

Architecture	**Vulnerability management**
Analytics and reporting	**Integrations**
Attack response	**Vision**
Threat research	**Roadmap**
Device visibility	**Market approach**

Differentiated
On par
Needs improvement
No capability

Products evaluated
Armis Enterprise Suite v3.0

REFERENCE QUOTES

"We had an inventory of medical devices for many years, but Armis' differentiator was their ability to update, validate, and give us visibility into our inventory."

"The Armis deployment took longer than we would have liked."

Palo Alto Networks: Forrester's Take

Our evaluation found that Palo Alto Networks (see Figure 8):

- **Delivers strong threat intelligence and broad device support.** Palo Alto Network's Zingbox technology protects all medical and enterprise IoT devices within a healthcare environment. Palo Alto Networks' well-regarded Unit 42 threat research team, together with Zingbox medical device threat researchers, gives ground truth to security alerts.
- **Needs to iron out post-acquisition staffing and false-positive challenges.** After acquiring Zingbox in late 2019, customers reported challenges with getting engineering support. Also, their extensive forensics capability has a high number of false positives.
- **Is best for existing Palo Alto Networks customers.** Palo Alto Networks has extensive plans to integrate the Zingbox technology into its overall network security platform.[6] Once the integration is completed, Palo Alto Networks will be the first vendor to offer a complete, integrated portfolio of network, endpoint, enterprise IoT, and medical device security.

Palo Alto Networks Customer Reference Summary

Palo Alto Networks reference customers enjoyed the ease and speed in which the product is deployed. Each commented on the lack of support resources and high false positives.

FIGURE 8 Palo Alto Networks QuickCard

Palo Alto Networks

Wave position
STRONG PERFORMER

Architecture	**Vulnerability management**
Analytics and reporting	**Integrations**
Attack response	**Vision**
Threat research	**Roadmap**
Device visibility	**Market approach**

Differentiated
On par
Needs improvement
No capability

Products evaluated
Zingbox IoT Guardian

REFERENCE QUOTES

"Rollout was very easy. It was completely installed in two weeks."

"Wanted to integrate with a different system, but Zingbox does not have engineers available after their acquisition."

Ordr: Forrester's Take

Our evaluation found that Ordr (see Figure 9):

- **Combines strong vulnerability reporting with easy deployment.** Ordr's vulnerability reporting is extensive and covers many medical and nonmedical systems. Correlations and prioritizations are automatically made between device identification, external sources such as MDS2, ICS-Cert, CVE, and vulnerability scanners in the customer's environment.
- **Needs to simplify its user interface for threat analysis.** Threat analysis and reporting workflows are not intuitive for several common workflows.
- **Is well suited for healthcare providers that want architectural flexibility.** While still offering traditional on-prem deployments for those who require it, Ordr's SaaS architecture reduces deployment complexity compared with the others in this study. This will work well for organizations that allow device telemetry to leave their local environment.

Ordr Customer Reference Summary

Ordr reference customers were very happy with the ease of deployment and training offered for the product. However, references cited issues with device misidentification and third-party product integration.

FIGURE 9 Ordr QuickCard

Ordr

Wave position
STRONG PERFORMER

Architecture	**Vulnerability management**
Analytics and reporting	**Integrations**
Attack response	**Vision**
Threat research	**Roadmap**
Device visibility	**Market approach**

Differentiated	Needs improvement
On par	No capability

Products evaluated
Ordr Systems Control Engine (SCE) v7.2 r5

REFERENCE QUOTES

"Ordr did a good job identifying network traffic off the bat. Now they are helping us fill gaps and optimizing the profiling capabilities."

"The Ordr UI makes it difficult to find the information we are looking for."

Gurucul: Forrester's Take

Our evaluation found that Gurucul (see Figure 10):

- **Focuses on device behavioral analysis.** Gurucul monitors medical and enterprise IoT devices and creates "models" for every identified asset. This gives security admin the ability to analyze threat activity (e.g., device compromise, malfunction, improper data flow).
- **Still needs to improve its clinical workflow alignment.** Gurucul doesn't analyze and report on clinical use to the same depth as others in this study. Admin must manually determine clinical priority associated with security alerts and identifying remediations.
- **Is best for companies focused on limiting insider risks.** Organizations looking to combine user behavioral analysis (UBA) with medical device security will find Gurucul possesses the products and vision to bring this capability to market, giving healthcare organizations the ability to identify insider risks involving both traditional IT assets and medical/enterprise IoT devices.

Gurucul Customer Reference Summary

Gurucul's reference was very happy with the level of visibility into device function and risk analysis. Forrester's client feedback was that insight into clinical use and device dependencies was lacking.

FIGURE 10 Gurucul QuickCard

Gurucul

Wave position
CONTENDER

Architecture	Vulnerability management
Analytics and reporting	Integrations
Attack response	Vision
Threat research	Roadmap
Device visibility	Market approach

Differentiated
On par
Needs improvement
No capability

REFERENCE QUOTES

"The features that we like best are entity behavior, discovery, and analytics."

"Gurucul's models require a lot of tweaking, which we found challenging."

Products evaluated
Unified Security and Risk Analytics (USRA) v8.1

Forescout Forrester's Take

Our evaluation found that Forescout (see Figure 11):

› **Passively inspects enterprise IoT, OT, and medical devices with strong remediation.** Forescout provides coverage of the entire device estate, using several bidirectional third-party product integrations to extend identification and analysis capabilities. Its modular approach allows more comprehensive medical insight and control through add-ons.

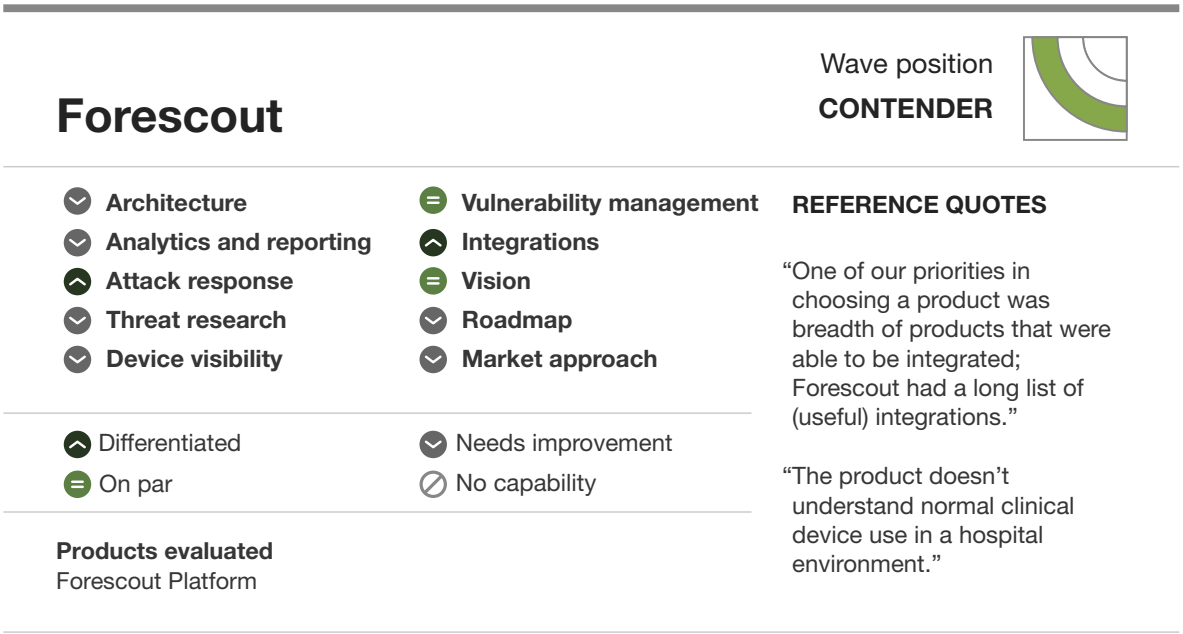
› **Needs to catch up on medical device-specific discovery and analysis.** Forescout provides forensics data on many devices that can't be identified without the purchase of Medigate, offered as a bundle with several native product integrations. However, reporting and analysis workflows are still separate in some cases between the two products.

› **Is best for existing Medigate customers seeking added breadth.** If you're an existing Medigate customer and want to extend your analysis into the IT, OT, and enterprise IoT networks, Forescout has a suite of products aimed at the broader hospital ecosystem.

Forescout Customer Reference Summary

Forescout's references were satisfied with the breadth of assets covered and third-party integrations, but all wanted more visibility and depth for medical devices.

FIGURE 11 Forescout QuickCard



Supplemental Material

The Forrester New Wave Methodology

We conducted primary research to develop a list of vendors that met our criteria for the evaluation and definition of this emerging market. We evaluated vendors against 10 criteria, seven of which we based on product functionality and three of which we based on strategy. We also reviewed market presence. We invited the top emerging vendors in this space to participate in an RFP-style demonstration and interviewed customer references. We then ranked the vendors along each of the criteria. We used a summation of the strategy scores to determine placement on the x-axis, a summation of the current offering scores to determine placement on the y-axis, and the market presence score to determine marker size. We designated the top-scoring vendors as Leaders.

Integrity Policy

We conduct all our research, including Forrester New Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

[1] See the Forrester report "Best Practices: Medical Device Security."

[2] Source: "Cyber warning issued for key healthcare organisations in UK and USA," National Cyber Security Centre, May 5, 2020 (https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations).

Source: "COVID-19 Exploited by Malicious Cyber Actors," Cybersecurity & Infrastructure Security Agency, April 8, 2020 (https://www.us-cert.gov/ncas/alerts/aa20-099a).

Source: "Cybercriminals targeting critical healthcare institutions with ransomware," Interpol, April 4, 2020 (https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware).

[3] Source: "Medtech and the Internet of Medical Things," Deloitte Centre for Health Solutions, July 2018 (https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf).

[4] Source: Elizabeth O'Dowd, "Healthcare Wireless Network Coverage, Capacity Top Challenge," HIT Infrastructure, February 1, 2017 (https://hitinfrastructure.com/news/healthcare-wireless-network-coverage-capacity-top-challenge).

[5] MDS2 is the Manufacturer Disclosure Statement For Medical Device Security.

[6] Palo Alto Networks has informed Forrester that an upcoming launch scheduled for late June 2020 will completely integrate Zingbox IoT security technology into the broader Palo Alto Networks product, services and support ecosystem

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.