Now Tech: Network Analysis And Visibility (NAV), Q4 2021

Forrester's Overview Of 32 NAV Providers

October 18, 2021

By Steve Turner with Joseph Blankenship, Alexis Bouffard, Peggy Dostie

Summary

Security and risk (S&R) professionals can use network analysis and visibility (NAV) to detect threats with high fidelity using network traffic, identify opportunities for security posture improvement, and bring in additional telemetry for orchestrating a response, if needed. But to realize these benefits, you'll first have to select from a diverse set of vendors that vary by size, functionality, geography, and vertical market focus. S&R pros should use this report to understand the value they can expect from a NAV provider and to select one based on size and functionality.

Gain Visibility And Detect Threats Using Network Analysis and Visibility

Networks are the critical, required path from endpoint to application. Organizations and their employees have traditionally put inherent trust in the networks they utilize to connect back to company resources. Adversaries abuse that trust to laterally move within organizations undetected, exfiltrate high-value data, and execute destructive attacks like ransomware. The adoption of Zero Trust architecture is, however, diminishing the inherent trust in networks and requiring visibility and analytics of internal network traffic. Besides monitoring outbound network traffic, security practitioners need complete visibility into not only traffic traveling north-south, but also east-west. NAV solutions are a must-have threat detection mechanism to shine a beam of light into dark, forgotten enterprise crevasses. Forrester defines NAV as:

> A category of security solutions that deploy passively in networks to analyze network traffic in order to detect threats using behavioral and signature-based approaches, discover and establish relationships between assets, provide flow analysis, extract relevant metadata, allow for full or targeted packet capture, integrate with other control points to remediate detected threats, and enable network forensics.

NAV solutions help organizations to:

- **Detect threats with high fidelity utilizing network traffic across hybrid infrastructure.** NAV solutions detect when a service, endpoint, or other on-premises or cloud-based computing infrastructure stops behaving normally. NAV solutions also provide visibility into devices where agents can’t be installed such as cloud microservices, internet-of-things (IoT) devices, and OT technology.

- **Identify opportunities for security posture improvement.** NAV solutions can see the encrypted and unencrypted communication between devices, detecting legacy protocols in use such as SMBv1, broken endpoint agents communicating to the ether, and misconfigured services causing operational chaos by flooding the network with unwanted traffic.

- **Bring in additional telemetry and orchestrate a response if needed.** NAV solutions bring in endpoint, cloud, and identity telemetry to correlate with the initial network detection to add additional incident context, thereby lowering false positives. They can also integrate with those sources or a SOAR to remediate a detected threat.

Select Vendors Based On Size And Functionality

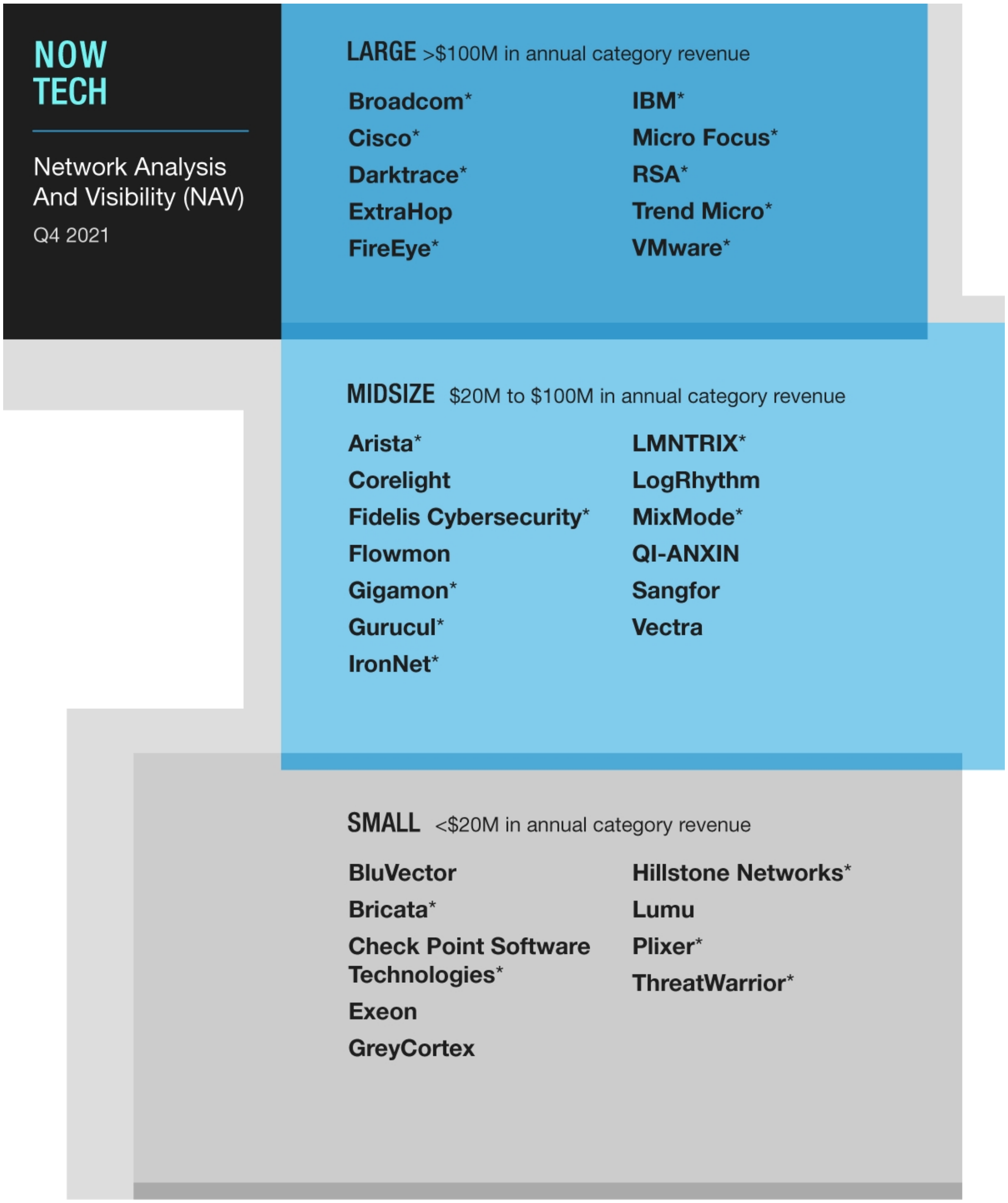
We've based our analysis of the NAV market on two factors: market presence and functionality.

Network Analysis And Visibility Market Presence Segments

We segmented the vendors in this market into three categories, based on NAV revenue: large established players (more than $100 million in NAV revenue), midsize players ($20 million to $100 million in revenue), and smaller players (less than $20 million in revenue) (see Figure 1).

Figure 1

Now Tech Market Presence Segments: Network Analysis And Visibility (NAV), Q4 2021



NOW TECH

Network Analysis And Visibility (NAV)

Q4 2021

LARGE >$100M in annual category revenue

Broadcom*	IBM*
Cisco*	Micro Focus*
Darktrace*	RSA*
ExtraHop	Trend Micro*
FireEye*	VMware*

MIDSIZE $20M to $100M in annual category revenue

Arista*	LMNTRIX*
Corelight	LogRhythm
Fidelis Cybersecurity*	MixMode*
Flowmon	QI-ANXIN
Gigamon*	Sangfor
Gurucul*	Vectra
IronNet*	

SMALL <$20M in annual category revenue

BluVector	Hillstone Networks*
Bricata*	Lumu
Check Point Software Technologies*	Plixer*
Exeon	ThreatWarrior*
GreyCortex	

*Forrester estimate

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

Network Analysis And Visibility (NAV) Functionality Segments

To explore functionality at a deeper level, we broke the network analysis and visibility market into four segments, each with varying capabilities (see Figure 2 and see Figure 3):

- **Point solution.** These products are deployed as standalone solutions and don't rely on integrations with other tools to deliver NAV functionality. These solutions deploy using passive sensors that collect network telemetry for analysis. They require a security analytics platform or SIEM to enrich detections with other telemetry from other data sources. These products may include API or native integrations with SOAR, EDR, XDR, network security solutions, or ticketing systems to respond to detections.

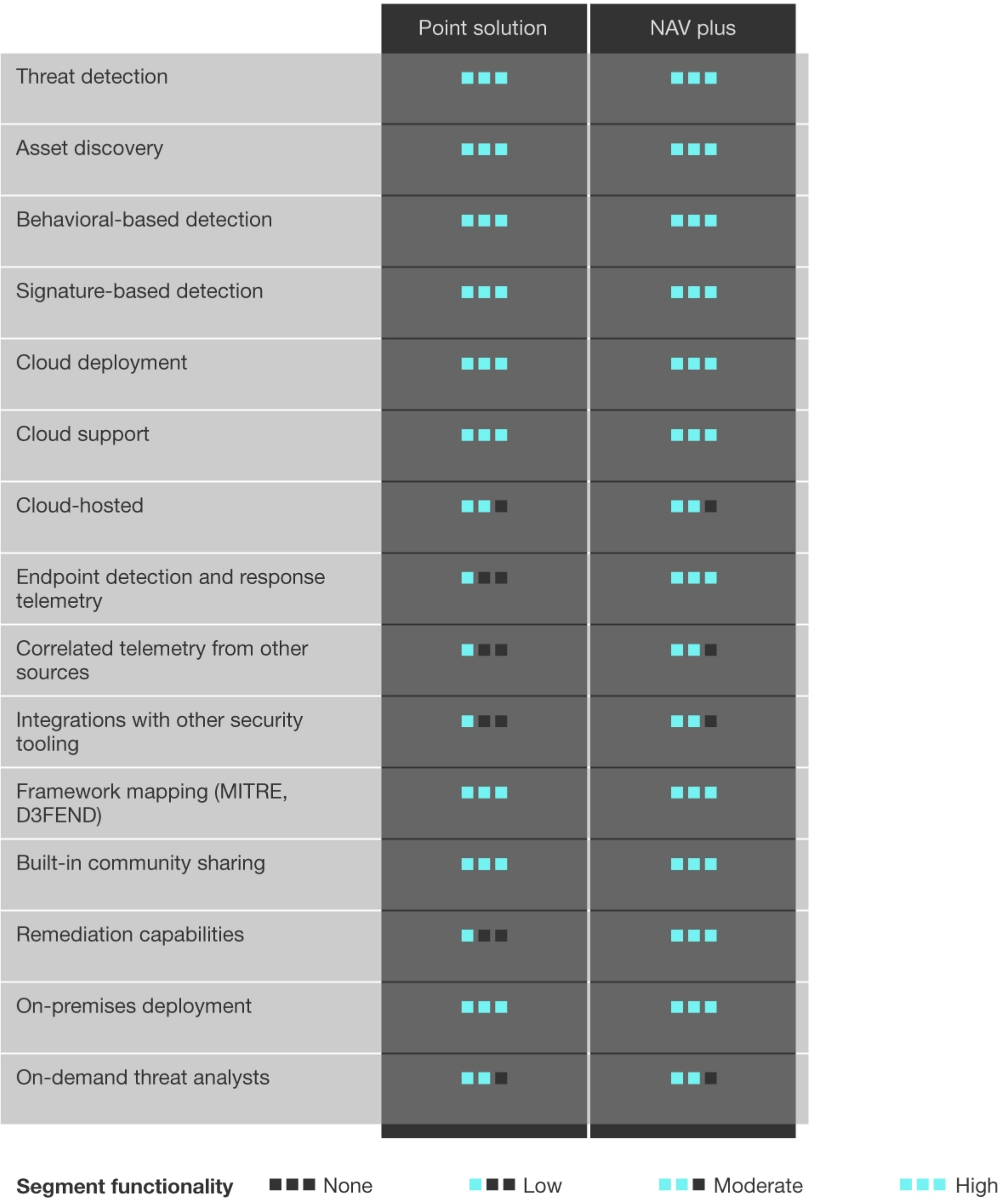
- **NAV plus.** These products natively enrich detections with telemetry from other sources such as endpoints and identity. NAV plus solutions perform analysis natively without reliance on external tools like security analytics platforms and correlate detections from different sources into incidents. These products include API and native integrations with SOAR, EDR, network security solutions (like firewalls), and ticketing systems for response. These solutions may also orchestrate responses for organizations that don't have a SOAR. Like point solutions, these products use passive sensors for data collection.

- **Security analytics platform.** These products are part of security analytics (SA) platforms. While the sensors are deployed similarly to point solutions and NAV plus solutions, the telemetry is pulled into the SA platform for analysis. These solutions aren't rooted in a specific technology for detections. They typically pull in multiple data sources such as endpoint logs, network logs, and security logs to correlate and enrich detections. SA platforms allow for custom creation of detections and correlations by end users. These solutions are typically paired with a SOAR or orchestration technology built into the SA platform for orchestrated response.

- **NAV as a feature.** These solutions integrate the collection of network telemetry and NAV functionality with an overarching platform where the analysis and correlation of detections occurs. These products require minimal to no custom logic from end users related to setting up data ingestion and detection. They typically use the network telemetry to correlate to other sources of data to form an incident. An example of this is an extended detection and response (XDR) platform where detections are rooted in EDR data using other sources like network telemetry to enrich detections and incidents.

Figure 2

Now Tech Functionality Segments: Network Analysis And Visibility, Q4 2021, Part 1



	Point solution	NAV plus
Threat detection	🟦🟦🟦	🟦🟦🟦
Asset discovery	🟦🟦🟦	🟦🟦🟦
Behavioral-based detection	🟦🟦🟦	🟦🟦🟦
Signature-based detection	🟦🟦🟦	🟦🟦🟦
Cloud deployment	🟦🟦🟦	🟦🟦🟦
Cloud support	🟦🟦🟦	🟦🟦🟦
Cloud-hosted	🟦🟦⬛	🟦🟦⬛
Endpoint detection and response telemetry	🟦⬛⬛	🟦🟦🟦
Correlated telemetry from other sources	🟦⬛⬛	🟦🟦⬛
Integrations with other security tooling	🟦⬛⬛	🟦🟦⬛
Framework mapping (MITRE, D3FEND)	🟦🟦🟦	🟦🟦🟦
Built-in community sharing	🟦🟦🟦	🟦🟦🟦
Remediation capabilities	🟦⬛⬛	🟦🟦🟦
On-premises deployment	🟦🟦🟦	🟦🟦🟦
On-demand threat analysts	🟦🟦⬛	🟦🟦⬛

Segment functionality ⬛⬛⬛ None 🟦⬛⬛ Low 🟦🟦⬛ Moderate 🟦🟦🟦 High

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

Figure 3

Now Tech Functionality Segments: Network Analysis And Visibility, Q4 2021, Part 2

	Security analytics	NAV as a feature
Threat detection	🟦🟦🟦	🟦🟦🟦
Asset discovery	🟦🟦⬛	🟦🟦⬛
Behavioral-based detection	🟦🟦⬛	🟦🟦🟦
Signature-based detection	🟦🟦⬛	🟦🟦🟦
Cloud deployment	🟦🟦🟦	🟦🟦🟦
Cloud support	🟦🟦🟦	🟦🟦🟦
Cloud-hosted	🟦🟦🟦	🟦🟦🟦
Endpoint detection and response telemetry	🟦🟦⬛	🟦🟦⬛
Correlated telemetry from other sources	🟦🟦🟦	🟦🟦🟦
Integrations with other security tooling	🟦🟦⬛	🟦🟦🟦
Framework mapping (MITRE, D3FEND)	🟦🟦🟦	🟦🟦⬛
Built-in community sharing	🟦🟦⬛	🟦⬛⬛
Remediation capabilities	🟦🟦⬛	🟦⬛⬛
On-premises deployment	🟦🟦⬛	🟦🟦⬛
On-demand threat analysts	🟦🟦⬛	🟦⬛⬛

Segment functionality ⬛⬛⬛ None 🟦⬛⬛ Low 🟦🟦⬛ Moderate 🟦🟦🟦 High

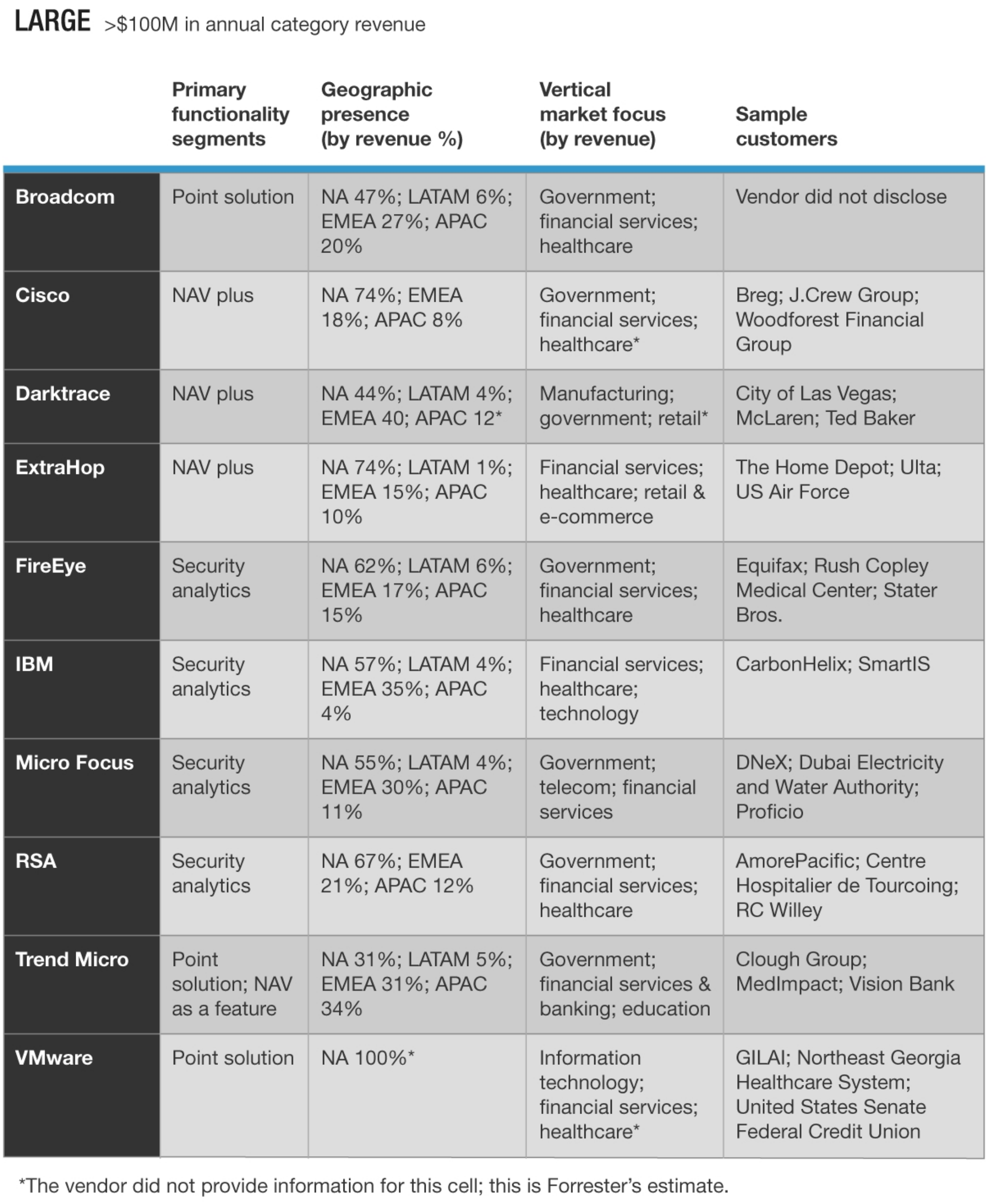
Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Align Individual Vendor Solutions To Your Organization’s Needs

The following tables provide an overview of vendors, with details on functionality category, geography, and vertical market focus (see Figure 4, see Figure 5, and see Figure 6).

Figure 4

Now Tech Large Vendors: Network Analysis And Visibility, Q4 2021



LARGE >$100M in annual category revenue

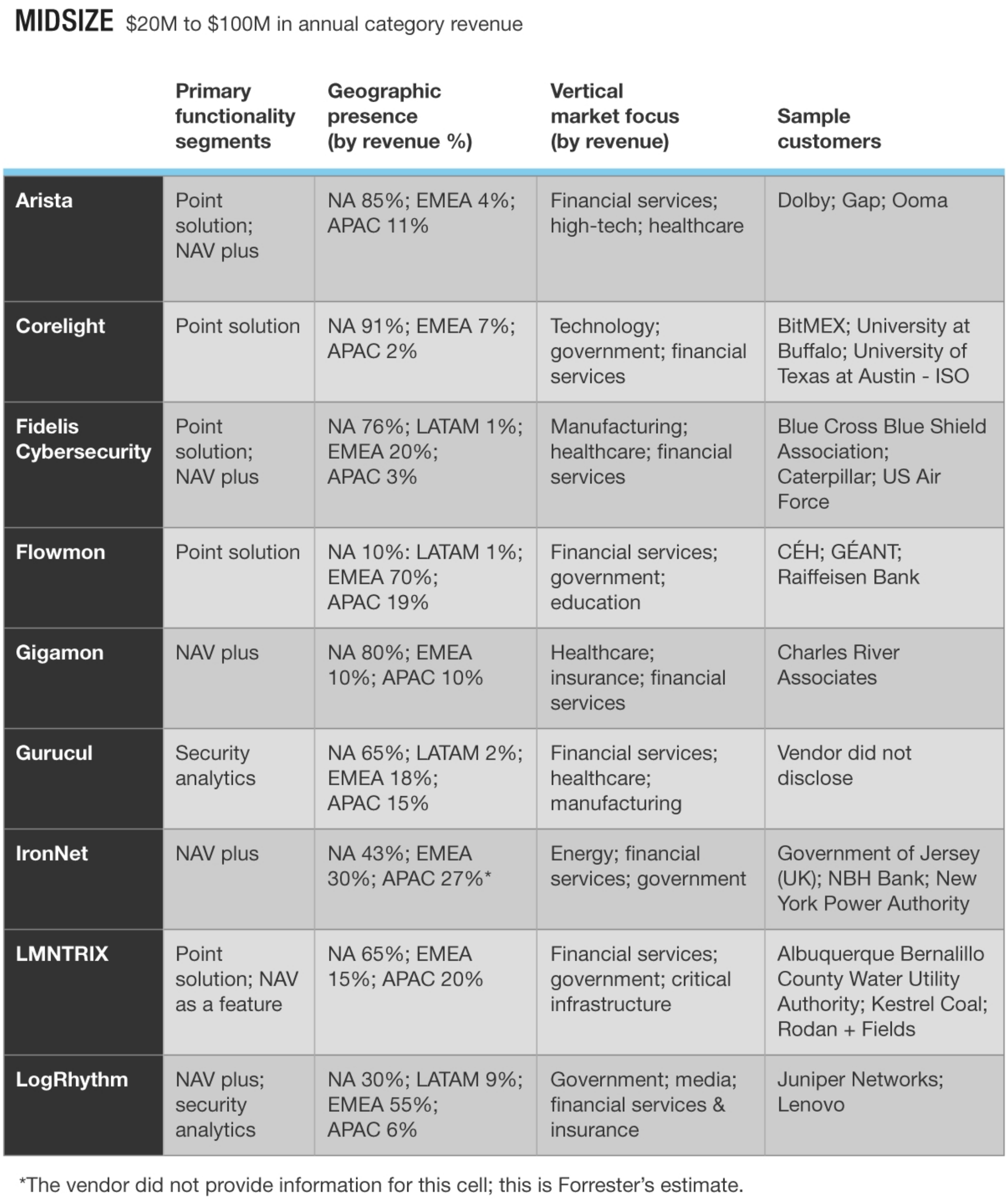
	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (by revenue)	Sample customers
Broadcom	Point solution	NA 47%; LATAM 6%; EMEA 27%; APAC 20%	Government; financial services; healthcare	Vendor did not disclose
Cisco	NAV plus	NA 74%; EMEA 18%; APAC 8%	Government; financial services; healthcare*	Breg; J.Crew Group; Woodforest Financial Group
Darktrace	NAV plus	NA 44%; LATAM 4%; EMEA 40; APAC 12*	Manufacturing; government; retail*	City of Las Vegas; McLaren; Ted Baker
ExtraHop	NAV plus	NA 74%; LATAM 1%; EMEA 15%; APAC 10%	Financial services; healthcare; retail & e-commerce	The Home Depot; Ulta; US Air Force
FireEye	Security analytics	NA 62%; LATAM 6%; EMEA 17%; APAC 15%	Government; financial services; healthcare	Equifax; Rush Copley Medical Center; Stater Bros.
IBM	Security analytics	NA 57%; LATAM 4%; EMEA 35%; APAC 4%	Financial services; healthcare; technology	CarbonHelix; SmartIS
Micro Focus	Security analytics	NA 55%; LATAM 4%; EMEA 30%; APAC 11%	Government; telecom; financial services	DNeX; Dubai Electricity and Water Authority; Proficio
RSA	Security analytics	NA 67%; EMEA 21%; APAC 12%	Government; financial services; healthcare	AmorePacific; Centre Hospitalier de Tourcoing; RC Willey
Trend Micro	Point solution; NAV as a feature	NA 31%; LATAM 5%; EMEA 31%; APAC 34%	Government; financial services & banking; education	Clough Group; MedImpact; Vision Bank
VMware	Point solution	NA 100%*	Information technology; financial services; healthcare*	GILAI; Northeast Georgia Healthcare System; United States Senate Federal Credit Union

*The vendor did not provide information for this cell; this is Forrester's estimate.

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

Figure 5

Now Tech Midsize Vendors: Network Analysis And Visibility, Q4 2021

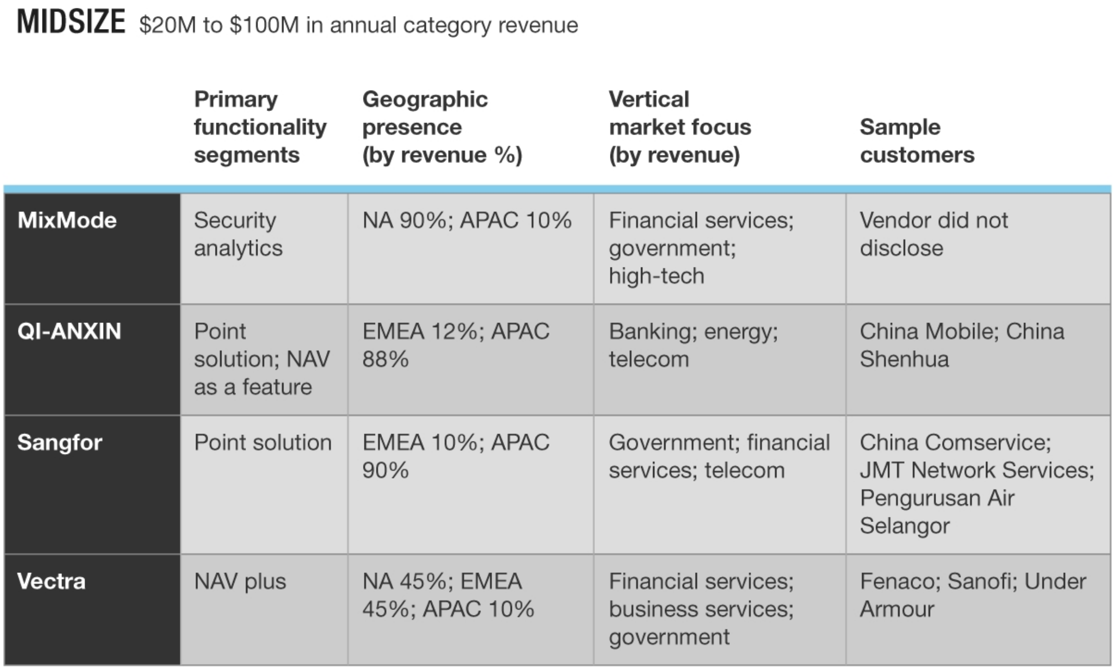


MIDSIZE $20M to $100M in annual category revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (by revenue)	Sample customers
Arista	Point solution; NAV plus	NA 85%; EMEA 4%; APAC 11%	Financial services; high-tech; healthcare	Dolby; Gap; Ooma
Corelight	Point solution	NA 91%; EMEA 7%; APAC 2%	Technology; government; financial services	BitMEX; University at Buffalo; University of Texas at Austin - ISO
Fidelis Cybersecurity	Point solution; NAV plus	NA 76%; LATAM 1%; EMEA 20%; APAC 3%	Manufacturing; healthcare; financial services	Blue Cross Blue Shield Association; Caterpillar; US Air Force
Flowmon	Point solution	NA 10%: LATAM 1%; EMEA 70%; APAC 19%	Financial services; government; education	CÉH; GÉANT; Raiffeisen Bank
Gigamon	NAV plus	NA 80%; EMEA 10%; APAC 10%	Healthcare; insurance; financial services	Charles River Associates
Gurucul	Security analytics	NA 65%; LATAM 2%; EMEA 18%; APAC 15%	Financial services; healthcare; manufacturing	Vendor did not disclose
IronNet	NAV plus	NA 43%; EMEA 30%; APAC 27%*	Energy; financial services; government	Government of Jersey (UK); NBH Bank; New York Power Authority
LMNTRIX	Point solution; NAV as a feature	NA 65%; EMEA 15%; APAC 20%	Financial services; government; critical infrastructure	Albuquerque Bernalillo County Water Utility Authority; Kestrel Coal; Rodan + Fields
LogRhythm	NAV plus; security analytics	NA 30%; LATAM 9%; EMEA 55%; APAC 6%	Government; media; financial services & insurance	Juniper Networks; Lenovo

*The vendor did not provide information for this cell; this is Forrester's estimate.

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



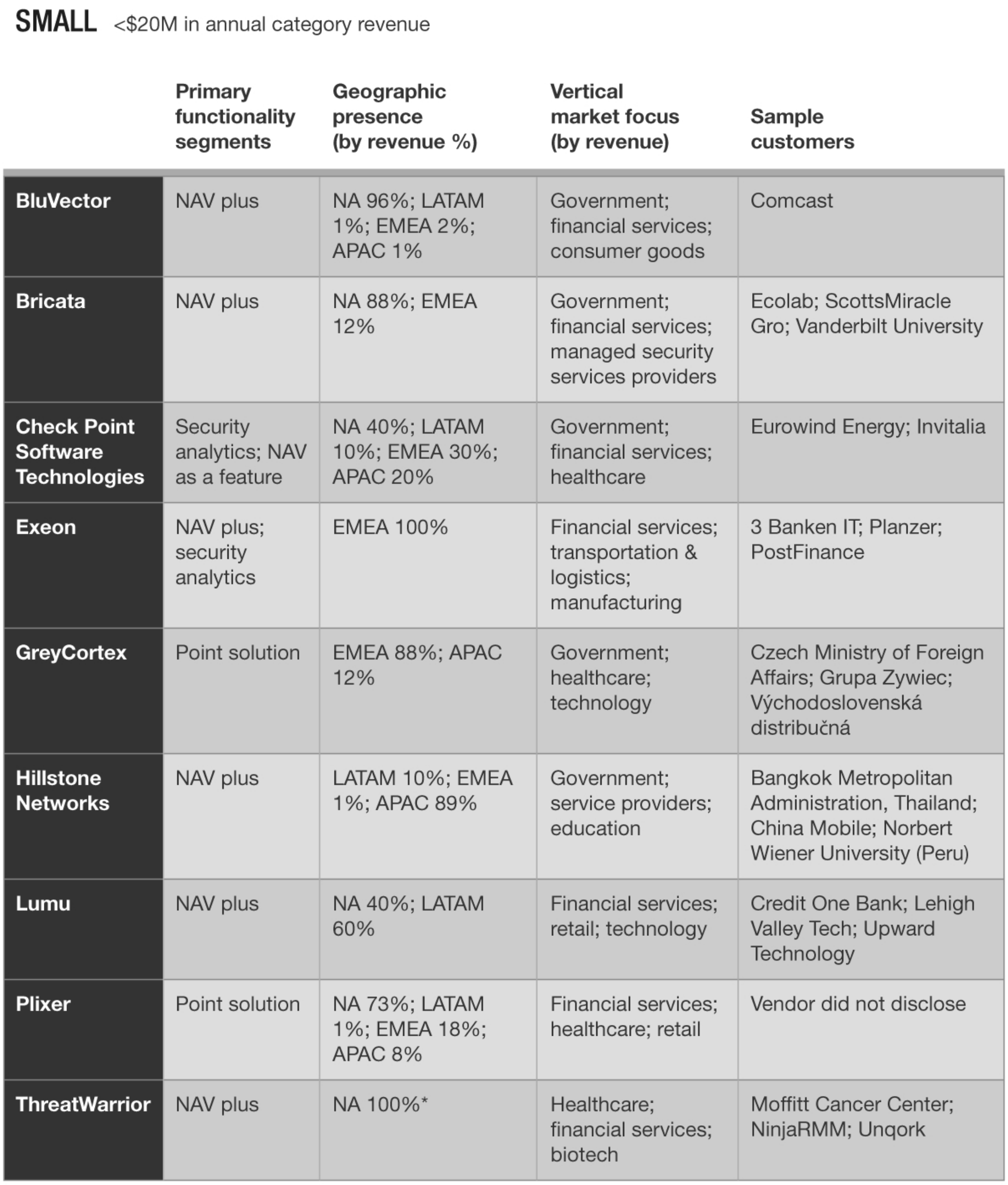
MIDSIZE $20M to $100M in annual category revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (by revenue)	Sample customers
MixMode	Security analytics	NA 90%; APAC 10%	Financial services; government; high-tech	Vendor did not disclose
QI-ANXIN	Point solution; NAV as a feature	EMEA 12%; APAC 88%	Banking; energy; telecom	China Mobile; China Shenhua
Sangfor	Point solution	EMEA 10%; APAC 90%	Government; financial services; telecom	China Comservice; JMT Network Services; Pengurusan Air Selangor
Vectra	NAV plus	NA 45%; EMEA 45%; APAC 10%	Financial services; business services; government	Fenaco; Sanofi; Under Armour

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

Figure 6

Now Tech Small Vendors: Network Analysis And Visibility, Q4 2021



SMALL <$20M in annual category revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (by revenue)	Sample customers
BluVector	NAV plus	NA 96%; LATAM 1%; EMEA 2%; APAC 1%	Government; financial services; consumer goods	Comcast
Bricata	NAV plus	NA 88%; EMEA 12%	Government; financial services; managed security services providers	Ecolab; ScottsMiracle Gro; Vanderbilt University
Check Point Software Technologies	Security analytics; NAV as a feature	NA 40%; LATAM 10%; EMEA 30%; APAC 20%	Government; financial services; healthcare	Eurowind Energy; Invitalia
Exeon	NAV plus; security analytics	EMEA 100%	Financial services; transportation & logistics; manufacturing	3 Banken IT; Planzer; PostFinance
GreyCortex	Point solution	EMEA 88%; APAC 12%	Government; healthcare; technology	Czech Ministry of Foreign Affairs; Grupa Zywiec; Východoslovenská distribučná
Hillstone Networks	NAV plus	LATAM 10%; EMEA 1%; APAC 89%	Government; service providers; education	Bangkok Metropolitan Administration, Thailand; China Mobile; Norbert Wiener University (Peru)
Lumu	NAV plus	NA 40%; LATAM 60%	Financial services; retail; technology	Credit One Bank; Lehigh Valley Tech; Upward Technology
Plixer	Point solution	NA 73%; LATAM 1%; EMEA 18%; APAC 8%	Financial services; healthcare; retail	Vendor did not disclose
ThreatWarrior	NAV plus	NA 100%*	Healthcare; financial services; biotech	Moffitt Cancer Center; NinjaRMM; Unqork

*The vendor did not provide information for this cell; this is Forrester's estimate.

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

Use NAV As A Visibility Cornerstone On Your Path To Zero Trust

Organizations struggle to make sense of or justify the voluminous networking logs they've ingested into their security analytics platform or SIEM. These orgs suffer from expense in depth due to all the additional data ingestion costs that happen with no rhyme or reason other than "someone said we needed to collect these logs." NAV solutions take the guesswork out of figuring out where to start for network threat detection. They also illuminate configuration issues and broken security and infrastructure tooling. Security practitioners should seek out NAV solutions that:

- **Integrate with their existing security ecosystem.** Point products still have a place within organizations as they often excel at the capabilities they provide. Practitioners should choose NAV products that make it easy to integrate into their security tech stacks both utilizing built-in, native integrations and robust APIs for organizations that would prefer to build their own integrations. As organizations begin to experiment with XDR solutions or consider security analytics solutions, they need to document requirements for the expected level of integration, whether that's as a point solution or as a feature.

- **Provide automated analysis using both signature- and behavioral-based detections.** Behavioral detections have become key to detecting evolving attack types, especially when it comes to ransomware and data exfiltration. Practitioners should expect their NAV solution to deliver both behavioral- and signature-based detections that are continuously updated by the vendor but allow for organizations to add their own custom threat intelligence and indicators of compromise (IOCs). Organizations should also expect NAV solutions to quickly baseline their environments and generate few false positives with minimal configuration tweaking. Require NAV products to map to common frameworks such as MITRE ATT&CK and D3FEND.

- **Address visibility gaps and replace manual network analysis processes or tools.** NAV products provide out-of-the-box threat detection and analysis with minimal overhead. Consider replacing intrusion detection systems (IDS), massive network log ingestion, and other systems or processes that require significant time, effort, and cost to manage. Choose solutions that allow for forensic investigation and some level of threat hunting across network data (and other data if the solution provides) while providing tactical PCAPS where necessary for deeper analysis. NAV products should deliver more than threat detection by offering insights into network traffic such as asset discovery and application mappings and dependencies.

- **Bolster the Zero Trust principal of comprehensive security monitoring.** As organizations barrel down the path toward Zero Trust, implementing technologies that give more visibility and insight into what's happening within their infrastructure is critical. Security practitioners should choose NAV solutions that easily integrate with on-premises and cloud (SaaS, PaaS, IaaS) infrastructure to provide wide-ranging visibility. Security pros should consider products that enable and integrate with Zero Trust edge (ZTE), ZTNA, and segmentation solutions.

Supplemental Material

Market Presence Methodology

We defined market presence in Figure 1 based on total NAV revenue for one year.

To complete our review, Forrester requested information from vendors. If vendors didn't share this information with us, we made estimates based on available secondary information. We've marked companies with an asterisk if we estimated revenues or information related to geography or industries. Forrester fact-checked this report with vendors before publishing.

Companies We Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Arista

BluVector

Bricata

Broadcom

Check Point Software Technologies

Cisco

Corelight

Darktrace

Exeon

ExtraHop

Fidelis Cybersecurity

FireEye

Flowmon

Gigamon

GreyCortex

Gurucul

Hillstone Networks

IBM

IronNet

LMNTRIX

LogRhythm

Lumu

Micro Focus

MixMode

Plixer

QI-ANXIN

RSA

Sangfor

ThreatWarrior

Trend Micro

Vectra

VMware

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

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