REPORT

The Forrester New Wave™: Microsegmentation, Q1 2022

The Nine Providers That Matter Most And How They Stack Up

March 10, 2022

David Holmes

with Stephanie Balaouras, Angela Lozada, Peggy Dostie

Summary

In Forrester's evaluation of the emerging market for network microsegmentation, we identified the nine most significant providers in the category — Akamai Technologies, Aruba, Avocado Systems, Cisco, ColorTokens, Illumio, Sangfor Technologies, Unisys, and VMware — 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 and risk professionals can use this report to select the right partner for their microsegmentation needs.

Topics

Microsegmentation Is Esse... | Microsegmentation Evaluati... | Vendor QuickCards

Microsegmentation Is Essential For Zero Trust Private Networks

More than a decade after Forrester first defined the Zero Trust (ZT) Model for information security, most of the operational domains of Zero Trust have matured quickly. The exception is the private network: It remains the most difficult domain in which to apply Zero Trust principles. The private network needs microsegmentation the most; it is still far too flat and is the happy home of insecure printers and unsuspecting users easily lured into ransomware situations by cybercriminals. Therefore, this evaluation focuses on solutions for private networks and excludes public cloud and container environments.

Vendors that specialize in microsegmentation solutions have done the best in this evaluation. The vendors who field a host-based agent and use it to both transit flow telemetry and to enforce policy provide the best solutions, and security and risk pros should look at these vendors first. To limit the blast radius of APTs, Log4Js, and the ransomware-du-jour, buyers should look for solutions with flow and asset discovery, visualization, a wide range of supported operating systems, and, in some cases, segmentation at the process level. Implicit trust on the network must end, and microsegmentation is the key.

Microsegmentation Evaluation Overview

The Forrester New Wave™ differs from our traditional Forrester Wave™. In the Forrester 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 nine vendors in this assessment: Akamai Technologies, Aruba, Avocado Systems, Cisco, ColorTokens, Illumio, Sangfor Technologies, Unisys, and VMware (see Figure 2 and see Figure 3). Each of these vendors has:

- **A proprietary microsegmentation solution to enforce ZT on an enterprise network.** We included only vendors with solutions that can segment at the level of the individual host on a private network. We excluded vendors whose solutions primarily focused on public cloud and/or container systems.
- **Annual microsegmentation revenues of at least $3 million**. We included vendors with at least $3 million annual revenues in the 12 months ending on the cutoff date.
- **At least 40 customers using their microsegmentation solution.** We included vendors with 40 or more enterprise customers using their microsegmentation solution.
- **An unaided mindshare within the industry and Forrester clients.** The vendors we evaluated are frequently mentioned in Forrester client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies. These vendors are also mentioned by other vendors during Forrester briefings as viable and formidable competitors.

Figure 1

Assessment Criteria: Microsegmentation, Q1 2022

Assessment criteria	Platform evaluation details
Flow and asset discovery	How does the vendor's solution discover applications, flows, and assets on the network? What is the solution's breadth of application and device coverage? From what information sources does the solution pull to understand and group the assets?
Policy management	How granular is the suggested policy, and how likely is it to be acceptable without major review or changes? How well does the solution apply the proposed policy changes? How does the vendor's solution manage microsegmentation policy over time? How does the solution adapt to changes in the network?
Policy enforcement	How well does the solution's policy actually translate into network security capability? How well does the solution get deployed at sufficient scale while also enforcing very granular, down-to-the-host network policy? How does the solution manage false positives?
Interface and reporting	How intuitive are the solution's user interfaces? What options exist to configure policy and manage alerts? What reports are available for compliance and security teams?
Host agents	How well does the solution support microsegmentation at the host level? What operating systems are supported? How is the solution's upgrade experience? What security abilities do the host agents provide?
Agentless aspect	How does the solution enforce microsegmentation policy around devices where an agent cannot be installed? If network infrastructure is used to enhance the segmentation for these devices, how well does the integration work?
Integrations	How well does the solution integrate with other elements of the technology stack, such as the network infrastructure, reporting platforms, vulnerability management, and orchestration platforms? What significant use cases are enabled by these integrations?
Product vision	How well does the product vision align with the current and future needs of customers? Is the vision focused on securing the customer's existing and future environments? How well is the company identifying and responding to competitive threats?
Roadmap	How well defined is the company's execution plan, and how does its roadmap align with its vision? How strong is the company's ability to define specific time frames, milestones, and benchmarks in its strategy and then execute on them?
Product and services support	How does the vendor assure the product will be deployed, the policy created, and the environment secured? How does the vendor measure customer satisfaction, and what steps does it take to continually improve service and support?

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

Figure 2

Forrester New Wave™: Microsegmentation, Q1 2022

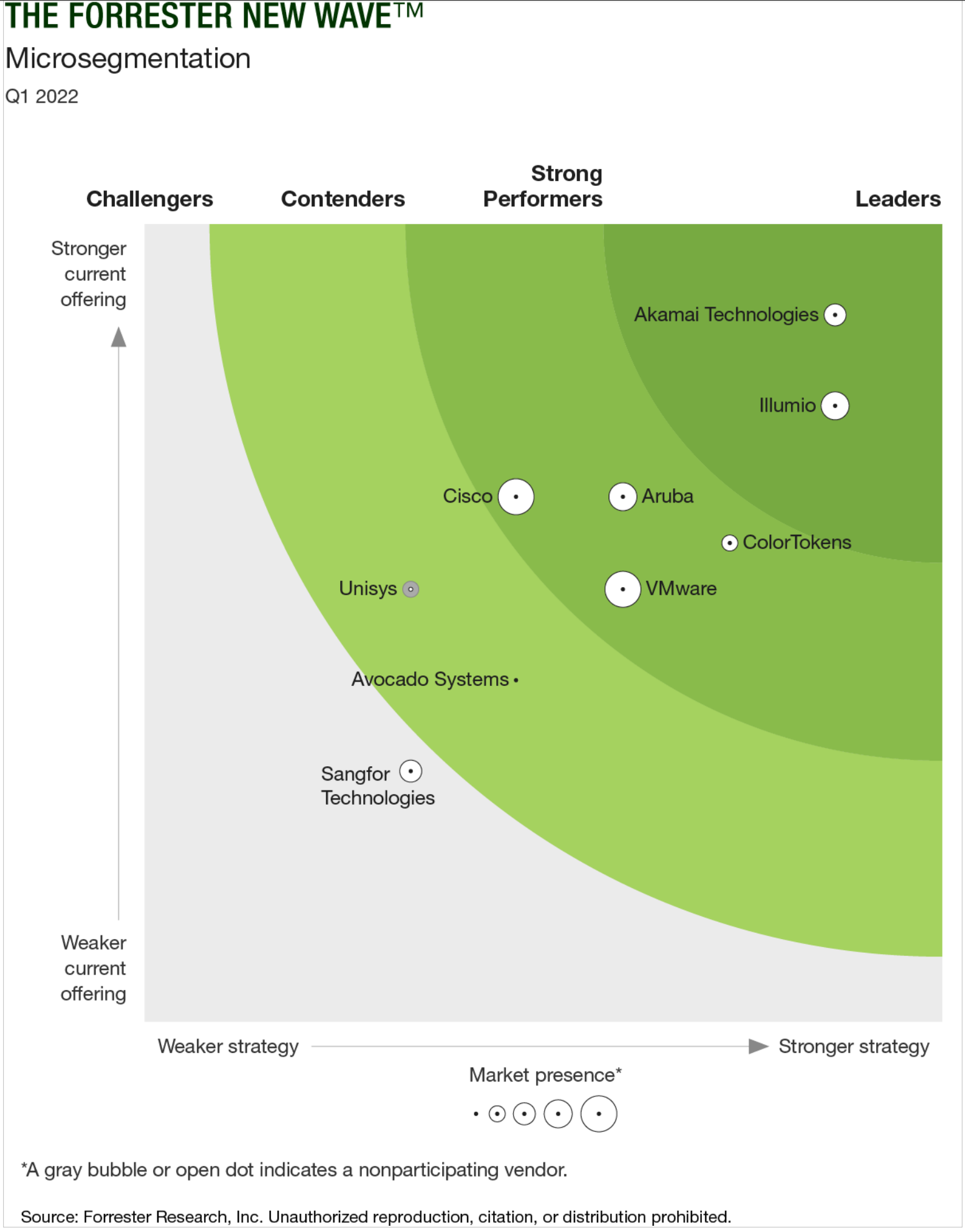


Figure 3

Forrester New Wave™: Microsegmentation Scorecard, Q1 2022

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

Vendor QuickCards

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

Akamai Technologies: Forrester's Take

Our evaluation found that Akamai, which acquired this product with the purchase of Guardicore (see Figure 4):

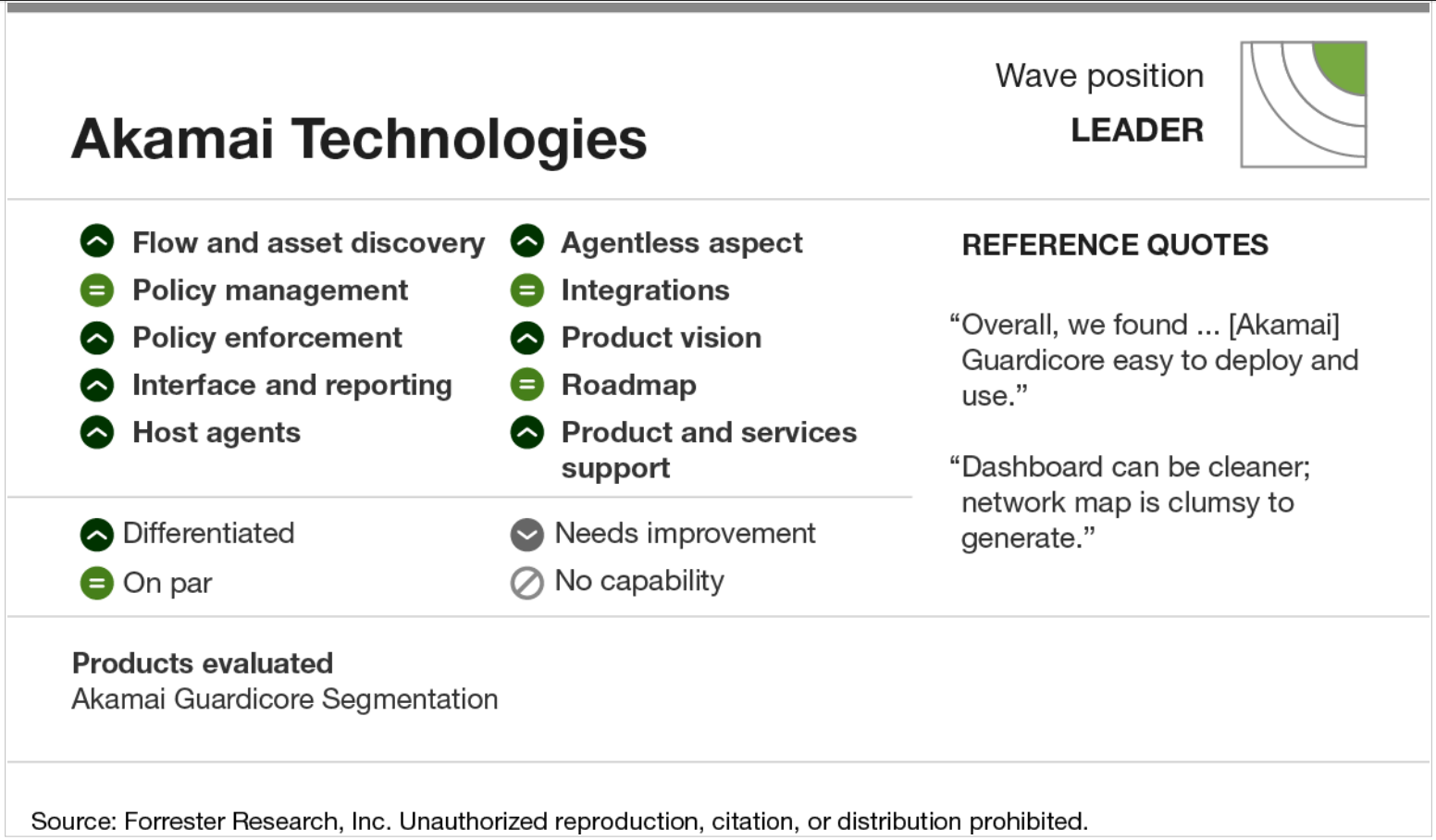
- **Offers a flexible security tool that goes beyond just microsegmentation.** Guardicore's infinite tagging system and proprietary firewall solve the segmentation problem and can also support incident response.
- **Lacks some custom integrations.** Guardicore integrates with vulnerability management and asset inventory but not the ITSM and ITIL tools that would expand its reach into IT.
- **Is an excellent overall microsegmentation solution for IT.** Enterprises looking to deploy a host-based, granular network should look at Guardicore.

Akamai Technologies Customer Reference Summary

Akamai customers praise the product's user interface as intuitive and easy to use. They also say it's quick to deploy (only one to two months). However, they recommend giving the tool sufficient time to baseline legitimate traffic.

Figure 4

Akamai Technologies QuickCard



Illumio: Forrester's Take

Our evaluation found that Illumio (see Figure 5):

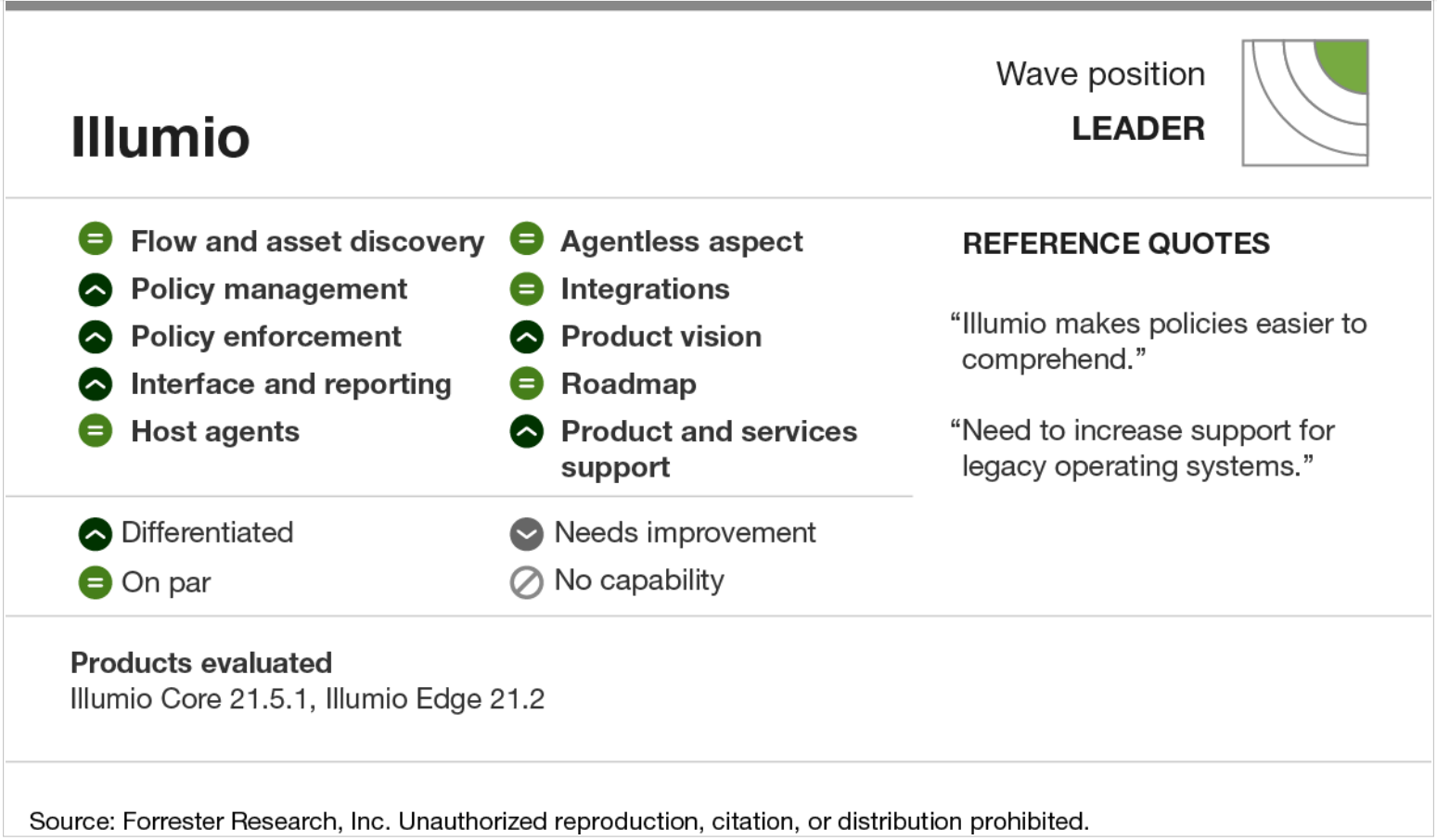
- **Focuses on operationalizing Zero Trust policies in the network.** No other vendor obsesses about enforcing explicit network policy like Illumio. Illumio's policy management, policy enforcement, and interface set the standard for microsegmentation.
- **Must optimize performance for very large deployments.** Many of Illumio's customers have the largest microsegmentation deployments, and policy synchronization at this scale needs further performance improvement.
- **Is the choice for organizations wanting predictable microsegmentation at scale.** Illumio's application labeling model enforces the disciplined approach to Zero Trust security that many large organizations sorely need.

Illumio Customer Reference Summary

Illumio customers praise the vendor's labeling approach, policy enforcement, ability to troubleshoot connectivity issues, and robust RBAC policies. They cite performance issues in the largest, most complicated deployments.

Figure 5

Illumio QuickCard



ColorTokens: Forrester’s Take

Our evaluation found that ColorTokens (see Figure 6):

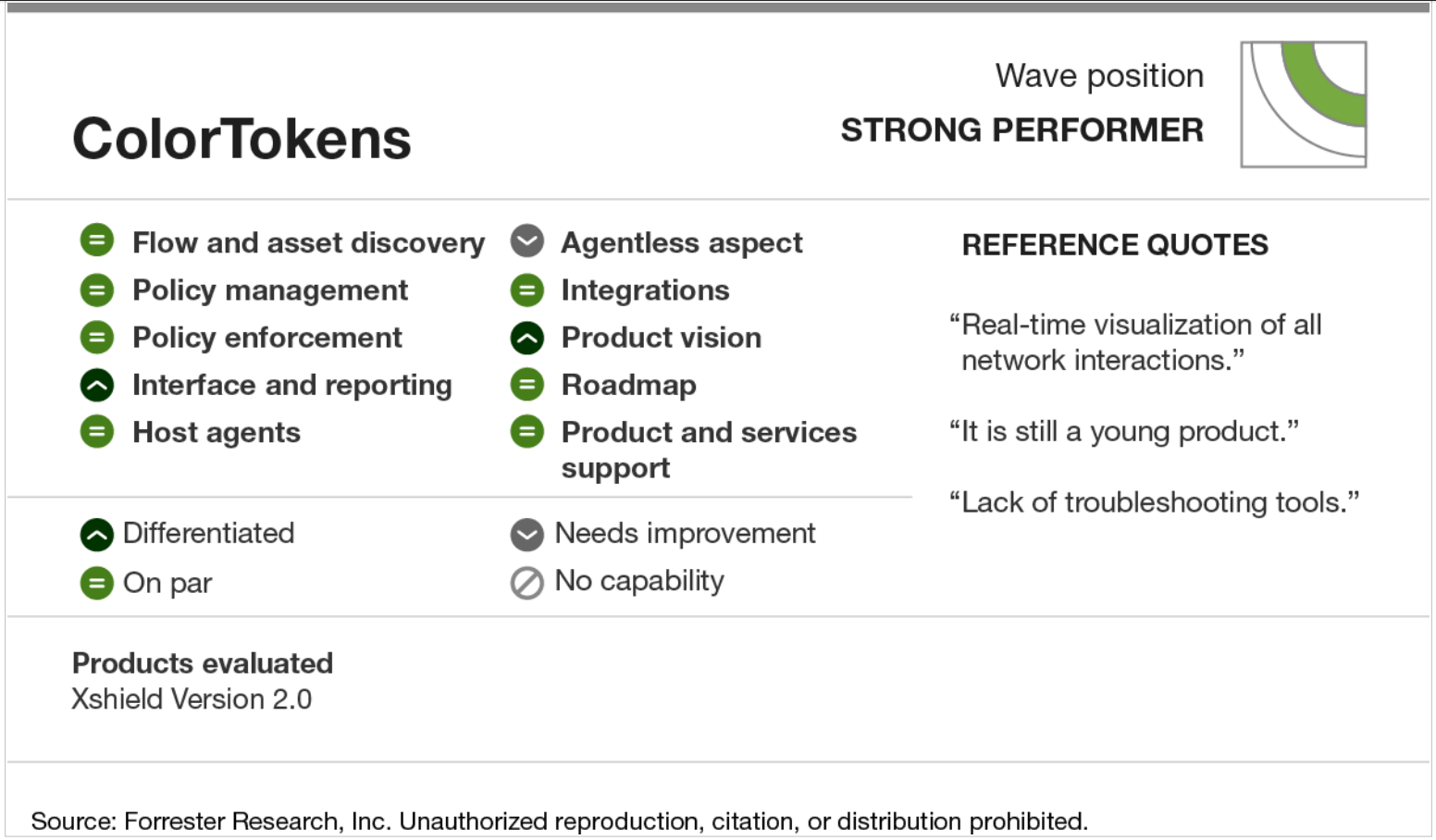
- **Is a strong entrant to the market.** ColorTokens has excellent flow visualization, application templates, policy simulation, and other capabilities largely on par with its competition.
- **Still has some growing up to do.** The vendor has room for improvement during rollouts and in the ability to microsegment in an agentless environment.
- **Provides healthy competition to the established leaders.** Organizations looking for host-based microsegmentation managed as a service from an ambitious newcomer should put ColorTokens on their short list.

ColorTokens Customer Reference Summary

ColorTokens reference customers were generous in their praise of the vendor’s capabilities. They liked the solution’s visualization, policy management, and RBAC. They noted room for maturity around troubleshooting, needing more Linux support, and five grouping layers of visualization instead of just three.

Figure 6

ColorTokens QuickCard



Aruba: Forrester's Take

Our evaluation found that Aruba (see Figure 7):

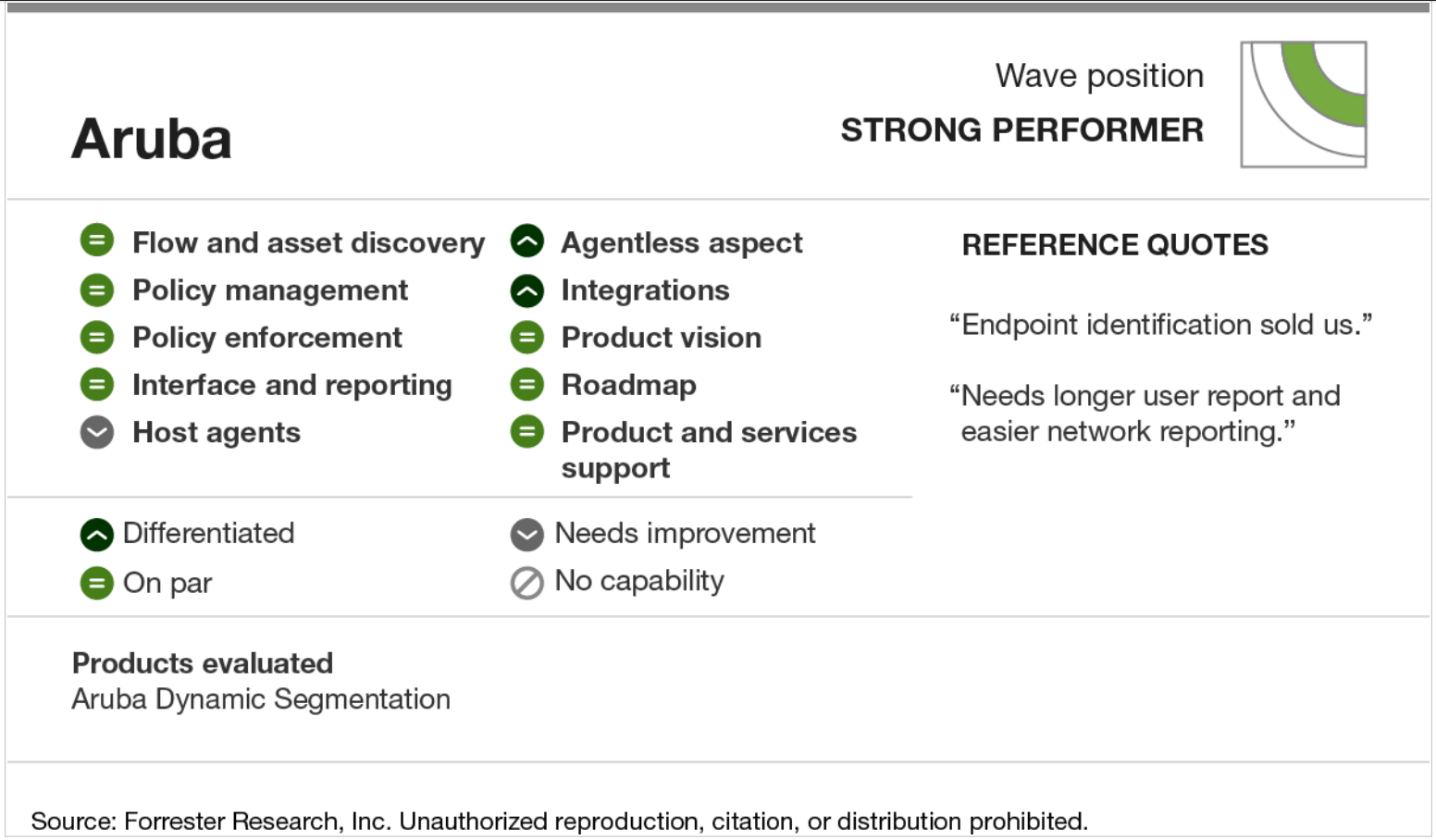
- **Delivers a unique, powerful network security solution ...** Aruba can provide both encryption and host-level microsegmentation in a network without using host agents. Its asset identification capabilities are impressive.
- **... predicated on Aruba networking gear.** Aruba Dynamic Segmentation must improve its flow detection and application mapping in order to compete with the Leaders in this report.
- **Is absolutely the right fit for Aruba customers.** Aruba's powerful, seemingly magical, dynamic segmentation achieves its peak potential when Aruba is firmly embedded in the wired and wireless infrastructure.

Aruba Customer Reference Summary

The Aruba customer reference praises the vendor's dependability and ease of use and cites endpoint identification as a strength. They dislike the user and network reporting.

Figure 7

Aruba QuickCard



VMware: Forrester’s Take

Our evaluation found that VMware’s NSX (see Figure 8):

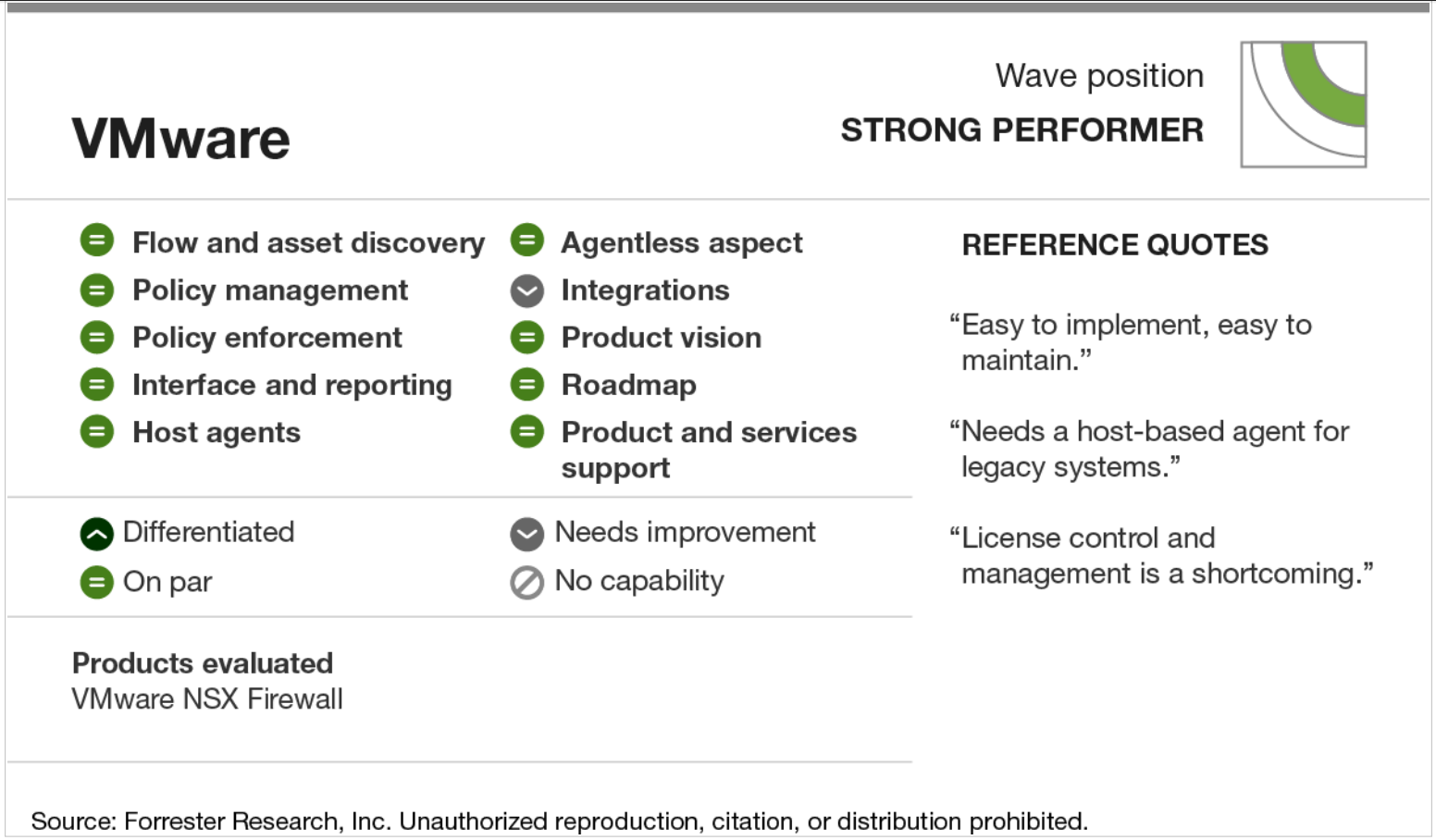
- **Inspects east-west traffic with both signatures and behavioral analysis.** NSX is microsegmentation built into the VMware hypervisor where it can be coupled with the vendor’s inline security inspection. NSX’s flow discovery and policy management absolutely shine in the virtualized private data center.
- **Could improve outside the hypervisor.** While NSX’s natural strength is the hypervisor, VMware can still improve microsegmentation in the physical world with better integration to switches, routers, load balancers, and ITIL/TSM.
- **Is the strongest choice for VMware environments.** Private clouds heavily invested in the VMware ecosystem will find no better choice than NSX.

VMware Customer Reference Summary

VMware customers praise the solution’s ease and speed of deployment. They appreciate how it is built into the environment, requiring no new equipment or software. However, they cite integrations with legacy systems as needing improvement.

Figure 8

VMware QuickCard



Cisco: Forrester's Take

Our evaluation found that Cisco (see Figure 9):

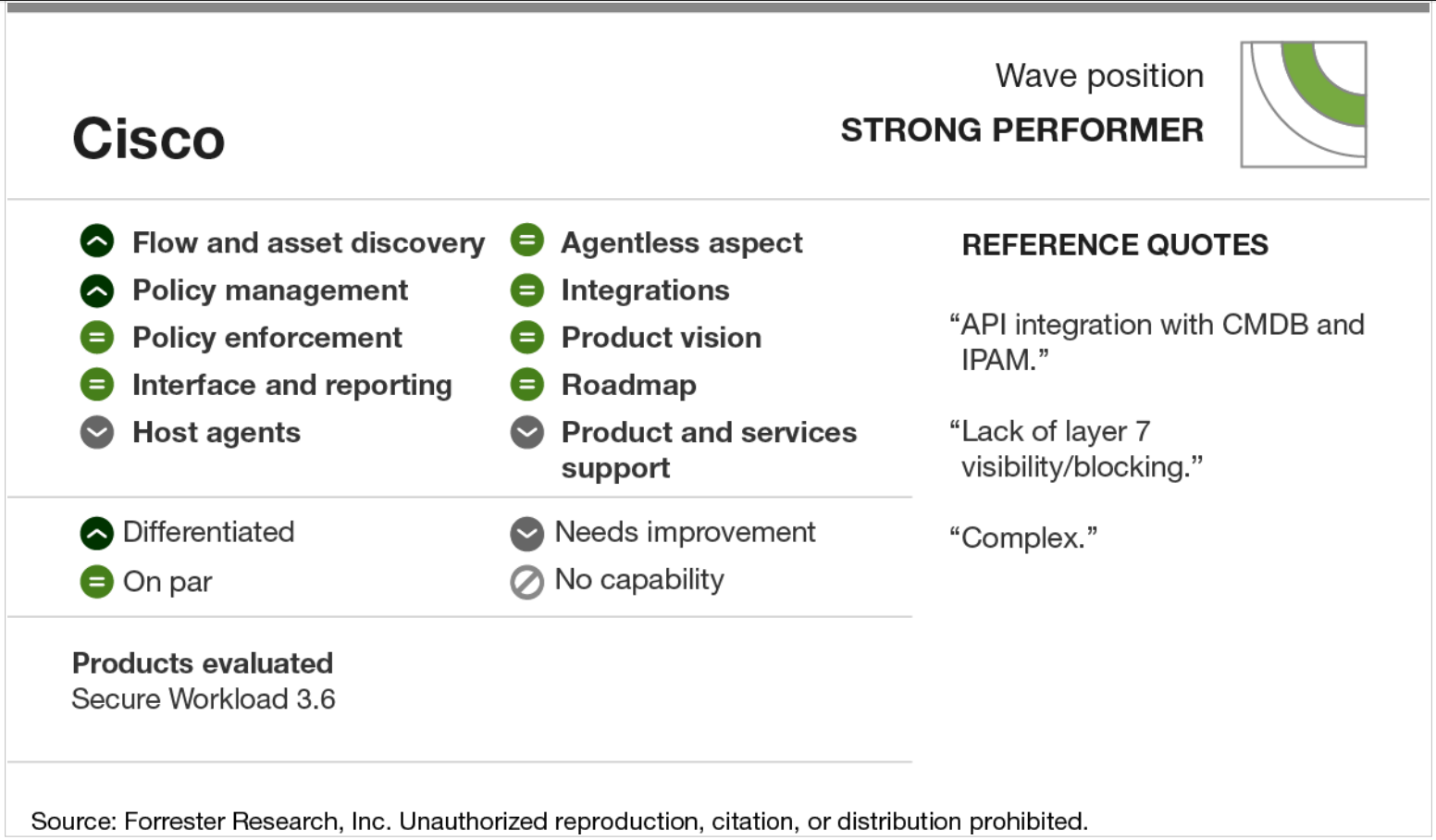
- **Excels at flow discovery and policy management.** Cisco's Secure Workload discovers flows and assets from network sources well and can test policy changes against long-term historical analysis better than any other competitor.
- **Needs to work with customers on deployment.** Cisco needs to work better with customers to ensure microsegmentation is correctly deployed and enforced. The vendor's reliance on partners to ensure microsegmentation actually gets to enforcement could be improved with more customer success management.
- **Is the right fit for Cisco shops.** Organizations invested in Cisco networking equipment will benefit from Secure Workload's ability to pull flow information from the infrastructure.

Cisco Customer Reference Summary

Some Cisco Secure Workload customers praise the solution's flexibility with regard to integrations with other systems CMDB like IPAM. Others find the solution's complexity frustrating.

Figure 9

Cisco QuickCard



Avocado Systems: Forrester's Take

Our evaluation found that Avocado (see Figure 10):

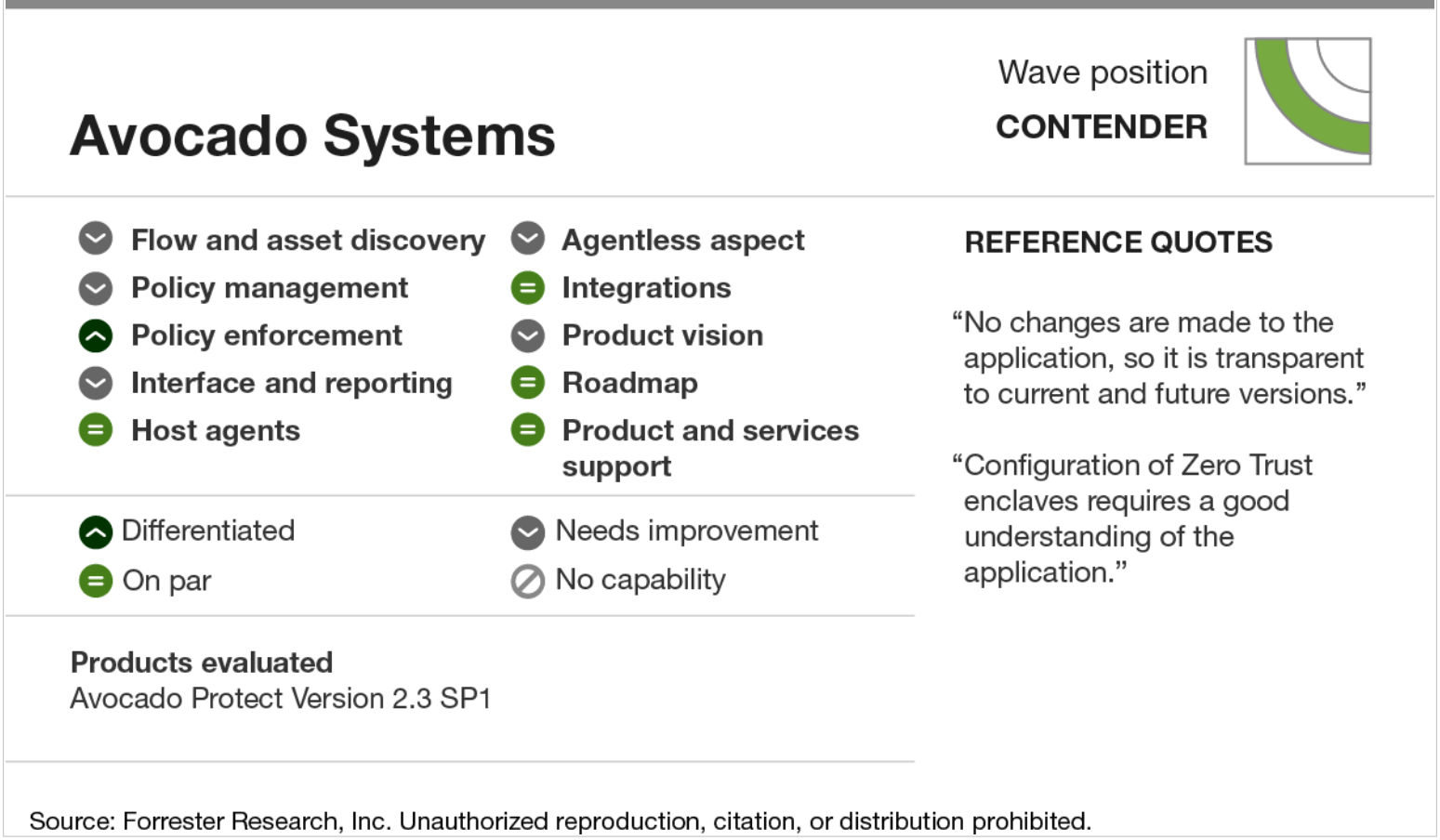
- **Excels at process-level security.** Avocado ringfences at the process level, providing an extra level of Zero Trust granularity. Avocado is one of the only vendors that stops attackers using shell exploits and other payloads from moving laterally across explicitly allowed layer 4 paths.
- **Needs more visualization and policy suggestion.** Avocado's Protect lacks a flow visualization to help the customer understand how their application components talk to each other.
- **Is ideal for organizations that need deep protection on critical applications.** Organizations looking for depth rather than breadth in their application coverage should seriously consider Avocado Systems.

Avocado Systems Customer Reference Summary

Avocado customers appreciate the interprocess view of applications not available in other tools and the ability to provide protection without changing the applications themselves. They called out the lack of visualization and want more Linux OS coverage.

Figure 10

Avocado Systems QuickCard



Unisys: Forrester's Take

Our evaluation found that Unisys (see Figure 11):

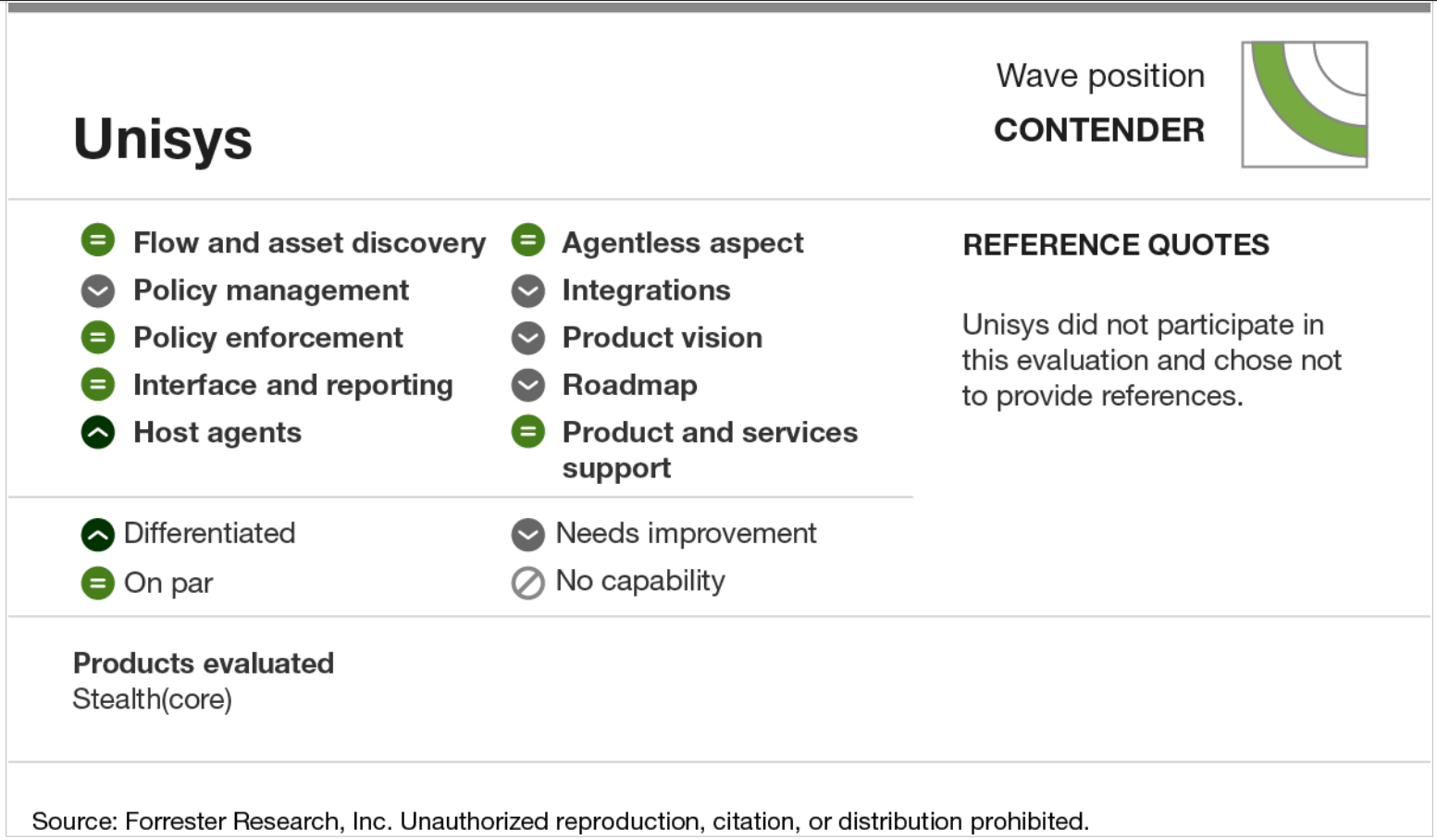
- **Combines microsegmentation with cloaking.** Hosts using Unisys Stealth are invisible outside their enclaves and gain encrypted tunnels. Unisys boasts of large, active deployments numbering in the tens of thousands of hosts.
- **Lacks integrations for the enterprise market.** While Unisys includes SIEM integrations, it lacks the EDR and ITSM integrations that private sector orgs will come to expect.
- **Resonates with defense agencies.** High-security environments, like defense-related agencies and subcontractors, will find Unisys Stealth an attractive solution for microsegmentation, cloaking, and security inspection.

Unisys Customer Reference Summary

Unisys did not participate in this evaluation and did not provide references.

Figure 11

Unisys QuickCard



Sangfor Technologies: Forrester's Take

Our evaluation found that Sangfor (see Figure 12):

- **Integrates well with the vendor's firewall and internet gateway.** Sangfor's enterprise firewall and internet access gateway corral unauthorized endpoints to enforce segmentation and host quarantine.
- **Needs significant work in policy management.** Sangfor lacks robust flow discovery, a critical capability for microsegmentation, and a clean shift from transparent mode to policy enforcement.
- **Is the right tool for Sangfor customers.** Asia Pacific buyers invested in the Sangfor ecosystem will benefit the most from the vendor's endpoint solution.

Sangfor Technologies Customer Reference Summary

Sangfor did not provide customer references for this report.

Figure 12

Sangfor QuickCard

Sangfor Technologies

Wave position
CHALLENGER

Flow and asset discovery	Agentless aspect
Policy management	Integrations
Policy enforcement	Product vision
Interface and reporting	Roadmap
Host agents	Product and services support

REFERENCE QUOTES

Sangfor did not provide customer references for this report.

Differentiated	Needs improvement
On par	No capability

Products evaluated
Sangfor Endpoint Secure 3.5.5 EN

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.