FROST & SULLIVAN

CISCO

2018 Global Network Access Control Market Leadership Award

2018
BEST PRACTICES
AWARDS

Contents

Background and Company Performance

Industry Challenges

Network visibility of endpoints is critical. Every device on a network is a potential attack or reconnaissance point that must be discovered and secured. Organizations are faced with the increasing level of malware and cyber attacks. The enterprise network no longer sits within four secure walls. It extends to wherever employees and data travel. Mobility, digitization, and the Internet of Things (IoT) are changing the way we live and work. The result is that networks are expanding, resulting in increasing complexity of managing resources and disparate security solutions.

Network access control (NAC) is a foundational network security defense. NAC is about connecting trusted users with trusted network services. The majority of NAC deployments use the 802.1X protocol, an IEEE 802.1X open-standard protocol for port-based secure access. More advanced NAC solutions have gone well beyond stand AAA (authentication, authority and accounting) to enable rich user and device visibility for more streamlined, flexible, and secure services. Secure access also requires policy and access control for scalable segmentation in today's highly distributed networks.

IoT and mobility trends present potential threat vectors that organizations need to manage. According to Frost & Sullivan, there will be 45.4 billion connected devices by 2023. Most of these will be IoT devices. The high growth of IoT presents risk to enterprise networks since most organizations don't have full visibility and comprehensive secure access applied to all users and devices. It is not only the volume of devices but also the diversity of OS’s and devices that poses a challenge. Most IoT devices lack the resources for embedding an agent, thus agentless technology is required. As the volume of device diversity increases, the ability of an organization to see and control devices declines. This makes NAC's capabilities more relevant than ever.

Organizations need to develop visibility across the enterprise: campus, data center, private cloud, public cloud and Operational Technology (OT) networks. Other protocols in addition to 802.1X need to be supported. Organizations face challenges as IT and OT converge. For example, OT networks were isolated silos, but are now morphing into the Industrial Internet of Things (IIoT). OT networks are no longer physically separated from IT networks. Threats are moving between cyber and physical dimensions. Most OT devices are difficult to patch.

Organizations are migrating workloads to the cloud, both public and private. Support is needed for AWS, Azure and other cloud computing platforms. Network administrators must deal with multiple device locations and access points. It is a heterogeneous environment with multiple vendors and management is typically decentralized.

While NAC is a powerful security tool, it is a very complex technology that can be difficult to implement. Unlike the earlier generation of NAC, which was intrusive and restrictive,

NAC vendors must focus on easing deployment and management, and providing IT complete visibility into every endpoint on their networks.

The complexities of NAC deployment and management can be a factor of a) the customer's tendency to use multiple security solutions that are not integrated and orchestrated and b) the severe shortage of skilled professional security experts to manage them. More than 25% of organizations use anywhere between 11-20 security vendors and 16% of organizations have been found to use anywhere between 20-50. Leveraging a multitude of security vendors that are not integrated and orchestrated can produce a significant volume of security alerts that can be overwhelming for any limited security staff to manage.

Organizations are in need of a security system that automates, integrates and orchestrates with other security solutions such as Next Generation Fire Wall (NGFW), Security Information and Event Management (SIEM), and threat intelligence networks in order to increase NAC efficacy and justify its investment.

NAC is a fast growing market. In 2017, revenues grew 23.7% to $942.3 million. Frost & Sullivan projects a compound annual growth rate from 2017 to 2022 of 16.9%. While the high growth rate and size of the NAC market has attracted more than 12 vendors in the last few years, establishing a leadership position in such a competitive market is challenging both incumbent and new vendors in NAC.

Market Leadership of Cisco

The NAC market is dominated by Enterprise and Large Enterprise customers, organizations with 2,500 or more employees. This is Cisco's primary customer base. Cisco Identity Services Engine (ISE) is the leading vendor in the NAC market. It holds 34.3% market share (see graph) and has held that top spot for several years. Cisco ISE has over 29,000 customers, representing virtually every industry and a majority of the Fortune 500. Cisco is the dominant NAC player in Enterprise and Large Enterprise segments. It also dominates every vertical market and geographic region.

Cisco is able to effectively serve these large organizations by integrating ISE within its broad security portfolio and leadership position in networking equipment and services. Cisco is the largest enterprise and security vendor by revenue and is well established with large organizations.

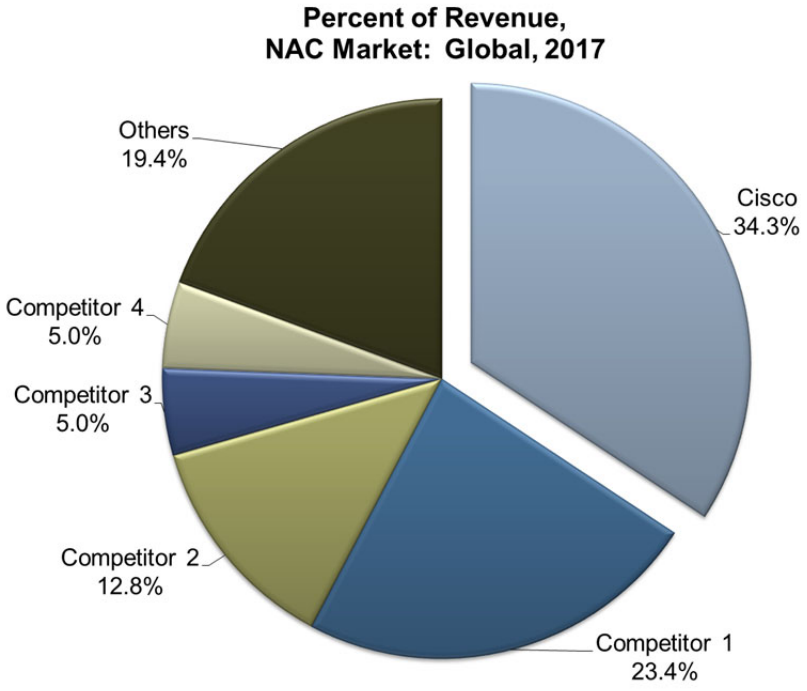
Cisco ISE is an integrated, open, and scalable solution that provides visibility, technology integration, automation, and granular policy control from a user and their device, and devices without users right to a resource or application. It's comprised of applications, services, and network controller features.

ISE works closely with other Cisco technologies such as Talos (threat intelligence organization), StealthWatch and Advanced Malware Protection (AMP). Cisco has focused

on growing its third-party ecosystem and partnerships. ISE 2.4 extends Cisco's focus on providing device profiling and visibility into the emerging industrial IoT market, especially in Manufacturing and Healthcare. Additionally, ISE has been incorporated into the Cisco Software-Defined Access solution, which is an architecture highly reliant on scalable policy services for what the industries terms "intent-based networking".

In the company's 2017 annual report, Cisco states, "We believe that security is the top IT priority for many of our customers. Our security strategy is focused on delivering a unified threat-centric security architecture combining network, cloud and endpoint-based solutions. Through this approach, we intend to provide security across the entire attack continuum before, during, and after a cyberattack to help our customers shorten the time between threat detection and response." Cisco's NAC solution is an integral part of its overall integrated security strategy.

Cisco's total security segment grew 9.3% in fiscal 2017, compared to total corporate revenue drop of 4.2%. Frost & Sullivan estimates that Cisco NAC had revenues of $323 million in calendar 2017, growing 13.9% over 2016. Thus, NAC is a growth driver for Cisco's fast growing security segment.



Growth Strategy Excellence

Cisco has a broad customer base in the NAC market covering virtually every industry. Cisco ISE is comprehensive, scalable and can be geared to the needs of a specific industry.

With clear,role-based segmentation Cisco has been consistently solving challenges for customers in the Financial Services industry. Cisco ISE also expands into IoT use cases with an increased interest from the OT industry. The company has success with customers in the Manufacturing and Healthcare industries with its Industrial Network Director and Medical NAC product offerings. Cisco partners with clinics, hospitals and medical equipment manufacturers to develop a holistic solution that not only identifies medical devices such as a blood pressure monitor, but also helps define policies on the level of access provided to the device on the network. Cisco has a proven solution for PCI compliance to serve the Retail market. Cisco group-based policy standards has dramatically simplified PCI compliance.

Cisco leverages its security portfolio and networking equipment to grow its NAC offering. Through pxGrid, Cisco ISE is integrated with more than 100 security partners and orchestrated with other security solutions, both Cisco's and other security vendors.

Most of Cisco's ISE revenues are currently derived from physical appliance sales. However, the company is focusing on developing innovations for virtual appliance, cloud services and IoT. The company has made further investments in IoT, BYOD and segmentation.

Cisco continues to innovate ISE through internal development as well as key acquisitions. Some of these acquisitions are technologies that are used across its security portfolio. For example:

- Duo Security (August 2, 2018 - announced intent to aqcuire) - helps defend organizations against data breaches by making security easy and effective
- Skyport Systems (January 24, 2018) - provides cloud-managed, hyper-converged systems that run and protect business-critical applications.
- Perspica, Inc. (October 19, 2017) - provides machine learning and data processing technology and expertise.
- Observable Networks, Inc. (July 13, 2017) - technology is based on dynamic behavioral modeling of all devices on the network. Cisco is using this technology to extend its Stealthwatch solution into the cloud with highly scalable behavior analytics and comprehensive visibility.

- Viptela Inc. (May 1, 2017) - provides a compelling software-defined wide area network (SD-WAN) solution that simplifies management. The cloud-first approach also aligns with Cisco's Digital Network Architecture transition to software-driven, automated networks that are more flexible, responsive and dynamic.

- ContainerX, Inc. (August 30, 2016) - technology to help enterprises manage, orchestrate and integrate containers across data centers.

- Jasper Technologies, Inc. (February 3, 2016) – the industry's leading IoT service platform in terms of number of enterprises and service providers.

Product Quality

Cisco's ISE architecture goes beyond the traditional Authentication, Authorization and Accounting (AAA). Cisco ISE offers a broad and comprehensive range of features which it continues to expand. Cisco offers scalability ranging from small sites to millions of users. For example, the upper limit of Cisco's ISE deployments is upward of 500,000 concurrent endpoints, scalable to 1.5 million endpoints. ISE offers the ability to profile and obtain the contextual identity of any device that connects to the network. Cisco provides profiles for specific verticals, such as Healthcare and Manufacturing. It offers authentication methods for both passive and active identity. The Cisco physical appliance node deployment architecture provides redundancy. Cisco continues to develop threat-centric NAC enhancements with its growing intelligence ecosystem, TALOS. The ISE pxGrid partner ecosystem is growing.

Customers invest in Cisco ISE for several reasons:

- The company offers a comprehensive solution from endpoint to an application in the data center.

- ISE addresses numerous secure access use cases and integrates across a vast set of security and networking solutions.

- Superior visibility, through device profiling and device-profile feed service, reduces the number of unknown endpoints.

- Cisco's market-leading AnyConnect, with over 120 million endpoints, provides visibility.

- ISE is the policy controller for Software-defined Access that allows for extremely granular segmentation options.

Through integration, open systems, and native features, ISE enables extensive automation that makes it less human-resource intensive to provide secure services and easier for workers to access the services they require from anywhere. ISE represents

numerous integrated technologies with the flexibility to craft services for virtually any size or type of operation, regardless of industry or size.

Implementation Excellence

Deploying and implementing a NAC solution can be a daunting task for many customers. The shortage of security professionals makes it difficult for organizations to have the necessary expertise.

ISE provides customers with a Secure Access Wizard (SAW). This tool enables configuration of all necessary settings plus basic customization of Guest, BYOD and Secure Access (802.1X) flows. The tool configures ISE and the Wireless Controller in a matter of minutes. Simplifying the deployment of its NAC Solution is an ongoing development.

Cisco ISE provides a centralized dashboard that provides comprehensive monitoring, customizable reporting, and alarms for all of its native functions. Cisco drives industry standards through its commitment to delivering a simple, open and automated security architecture. The company offers out of the box simplicity for guest administration and onboarding, BYOD, and secure access. Technical support is available from both internal customer service and highly-trained and certified partners.

Cisco touts its high scalability which allows organizations to use fewer NAC appliances and scale to 1,500,000 total and 500,000 concurrent endpoints and devices. ISE is vendor-neutral in its support for access control and segmentation with market-leading technologies. Cisco’s pxGrid enables integration with virtually any security intelligence technology.

Brand Strength

Cisco ISE is the NAC market leader with more deployments than any other vendor and is trusted to deliver, support, and continuously improve its solution to meet current and future access control and security requirements. Cisco leverages its well-known and broad security portfolio integrating ISE with Cisco's AMP, CTA, Stealthwatch and Firepower next generation firewall and intrusion prevention technologies.

Unlike competitors who offer point solutions, ISE benefits from being a centerpiece of a comprehensive security strategy framework that covers the campus, network, data center and cloud. It is well established with large organizations. Cisco offers engineering, network design and maintenance, and professional services for enterprises.

Strategic Partnerships

Cisco ISE integrates with over 100 ecosystem partners to provide an all-encompassing NAC solution. The company has an extensive network of highly trained partners on ISE. ISE has a broad integration partner ecosystem covering 50+ partner product integrations

in 14 distinct technology areas. ISE can send and receive context from ecosystem partners to make better secure network access policy decisions. The ISE pxGrid has over 100 partner integrations and is growing.

Cisco recently announced a partnership with McAfee. Cisco pxGrid integrates with the McAfee OpenDXL security fabric. This interoperability delivers unprecedented breadth in multi-vendor collaboration and simplifies security vendor integration for customers. The integration helps respective threat response ecosystem partners collaborate through ISE and McAfee ePO. The result is a combined threat response partner community of more than 100 security vendors along with contributions from an open source community.

Conclusion

NAC is a mature product category but vendors need to innovate to meet the changing needs of the market. The NAC market is evolving as enterprise networks expand beyond the traditional secure walls. NAC vendors must contend with the emerging trends of IoT, mobility, BYOD, IT and OT convergence, and cloud usage. Security orchestration and integration with other security solutions is an important NAC function. Cisco has a broad security product portfolio, but also works with other security vendors to increase NAC efficacy.

Cisco is addressing the specific needs of its customers in all vertical markets with an open and flexible NAC architecture. Cisco ISE is a comprehensive and scalable solution with a wide set of features and functions. The company is investing in Software-defined Access for intent-based networking. In addition to its internal technology development, Cisco is making strategic acquisitions for technologies that will enhance all of its security products. It is leveraging these improvements into ISE. Cisco is driving widespread adoption of ISE with its growing partner ecosystem.

With its strong overall performance, Cisco has achieved a leadership position in the NAC market with a market share of 34.3%, and Frost & Sullivan is proud to bestow the 2018 Market Leadership Award to Cisco.

Significance of Market Leadership

Ultimately, growth in any organization depends upon customers purchasing from a company, and then making the decision to return time and again. Loyal customers become brand advocates; brand advocates recruit new customers; the company grows; and then it attains market leadership. To achieve and maintain market leadership, an organization must strive to be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition. This three-fold approach to delivering market leadership is explored further below.

Understanding Market Leadership

As discussed on the previous page, driving demand, strengthening the brand, and differentiating from the competition all play a critical role in a company's path to market leadership. This three-fold focus, however, is only the beginning of the journey and must be complemented by an equally rigorous focus on the customer experience. Best-practice organizations, therefore, commit to the customer at each stage of the buying cycle and continue to nurture the relationship once the customer has made a purchase. In this way, they build a loyal, ever-growing customer base and methodically add to their market share over time.

Key Performance Criteria

For the Market Leadership Award, we focused on specific criteria to determine the areas of performance excellence that led to the company's leadership position. The criteria we considered include (although not limited to) the following:

Criterion	Requirement
Growth Strategy Excellence	Demonstrated ability to consistently identify, prioritize, and pursue emerging growth opportunities
Implementation Excellence	Processes support the efficient and consistent implementation of tactics designed to support the strategy
Brand Strength	The possession of a brand that is respected, recognized, and remembered
Product Quality	The product or service receives high marks for performance, functionality, and reliability at every stage of the life cycle
Product Differentiation	The product or service has carved out a market niche, whether based on price, quality, or uniqueness of offering (or some combination of the three) that another company cannot easily duplicate
Technology Leverage	Demonstrated commitment to incorporating leading-edge technologies into product offerings, for greater product performance and value
Price/Performance Value	Products or services offer the best value for the price, compared to similar offerings in the market
Customer Purchase Experience	Customers feel they are buying the most optimal solution that addresses both their unique needs and their unique constraints
Customer Ownership Experience	Customers are proud to own the company's product or service, and have a positive experience throughout the life of the product or service
Customer Service Experience	Customer service is accessible, fast, stress-free, and of high quality

Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Our analyst team strives to follow a 10-step process (illustrated below) to evaluate Award candidates and assess their fit with our best practice criteria. The reputation and integrity of our Awards are based on close adherence to this process.

STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify Award recipient candidates from around the globe	• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 360-degree research**	Perform comprehensive, 360-degree research on all candidates in the pipeline	• Interview thought leaders and industry practitioners • Assess candidates' fit with best-practice criteria • Rank all candidates	Matrix positioning of all candidates' performance relative to one another
3	**Invite thought leadership in best practices**	Perform in-depth examination of all candidates	• Confirm best-practice criteria • Examine eligibility of all candidates • Identify any information gaps	Detailed profiles of all ranked candidates
4	**Initiate research director review**	Conduct an unbiased evaluation of all candidate profiles	• Brainstorm ranking options • Invite multiple perspectives on candidates' performance • Update candidate profiles	Final prioritization of all eligible candidates and companion best-practice positioning paper
5	**Assemble panel of industry experts**	Present findings to an expert panel of industry thought leaders	• Share findings • Strengthen cases for candidate eligibility • Prioritize candidates	Refined list of prioritized Award candidates
6	**Conduct global industry review**	Build consensus on Award candidates' eligibility	• Hold global team meeting to review all candidates • Pressure-test fit with criteria • Confirm inclusion of all eligible candidates	Final list of eligible Award candidates, representing success stories worldwide
7	**Perform quality check**	Develop official Award consideration materials	• Perform final performance benchmarking activities • Write nominations • Perform quality review	High-quality, accurate, and creative presentation of nominees' successes
8	**Reconnect with panel of industry experts**	Finalize the selection of the best-practice Award recipient	• Review analysis with panel • Build consensus • Select recipient	Decision on which company performs best against all best-practice criteria
9	**Communicate recognition**	Inform Award recipient of Award recognition	• Inspire the organization for continued success • Celebrate the recipient's performance	Announcement of Award and plan for how recipient can use the Award to enhance the brand
10	**Take strategic action**	Upon licensing, company is able to share Award news with stakeholders and customers	• Coordinate media outreach • Design a marketing plan • Assess Award's role in future strategic planning	Widespread awareness of recipient's Award status among investors, media personnel, and employees

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages more than 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.