FROST & SULLIVAN

BEST PRACTICES AWARDS

CISCO

2020 GLOBAL NETWORK ACCESS CONTROL MARKET LEADERSHIP AWARD

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. The premise of network access control is the security principle that end users/endpoints can be blocked, quarantined, or redirected to different parts of a network if there is an Indication of Compromise (IOC) or vulnerabilities. However, the networks have expanded beyond the "traditional" endpoints of servers, PCs and virtual desktops to encompass tablets, smartphones, and IoT devices. The majority of NAC deployments use the 802.1X protocol, an IEEE 802.1X open-standard protocol for port-based network access control.

The IoT and Bring Your Own Device (BYOD) trends present potential threat vectors that organizations need to manage. According to Frost & Sullivan, there will be 60 billion connected devices by 2024. Most of these will be IoT devices. The high growth of IoT poses challenges to enterprise networks since these are mostly non-802.1X compliant. 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 devices and OS's and their diversity increases, the ability of an organization to see and control devices declines.

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. OT networks were isolated silos, but are 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. The migration to the cloud by customers has accelerated in the last year. 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 are compounded by the severe shortage of skilled professional security experts. Organizations are in need of better

security tools and automated systems to alleviate these limitations. The level of expertise required from a network engineer is very high.

Organizations have invested in many different security technologies. Improved orchestration and integration with other security solutions such as Next Generation Fire Wall (NGFW), Security Information and Event Management (SIEM), and threat intelligence networks will increase NAC efficacy and justify its investment.

The Zero Trust security model has been gaining momentum over the course of the last year. Greater traction in this space will accelerate in the next year. NAC is a critical element in a ZT strategy due to its capability to have visibility and control of devices on a network and NAC's capacity to orchestrate and integrate other security solutions.

NAC is a fast-growing market. In 2019, revenues grew 16.1% to $1.3 billion. Frost & Sullivan projects a compound annual growth rate from 2019 to 2024 of 14.3%. The high growth rate and size of the NAC market has attracted more vendors in the last few years. The NAC market has over 13 vendors. Consequently, establishing a leadership position in such a competitive market is challenging both incumbent and new vendors in NAC.

Market Leadership of Cisco

Cisco is the leading vendor in the NAC market. The company holds 33.4% market share in 2019 and has held that top spot for several years. In 2019, Cisco's NAC revenues outpaced the overall market gaining 0.85 basis points of market share, the most of any vendor. Among the Fortune 100, 100% use Cisco Security.

Cisco leverages its broad security portfolio and position as the leader in networking equipment and services. It is the largest enterprise and security vendor by revenue and is well established with large organizations. Cisco NAC is an integrated and open solution providing visibility, technology integration, automation, and granular policy control from a user and their device right to a resource or application. The solution is based on Identity Services Engine (ISE) that comprises applications, services, and network controller features.

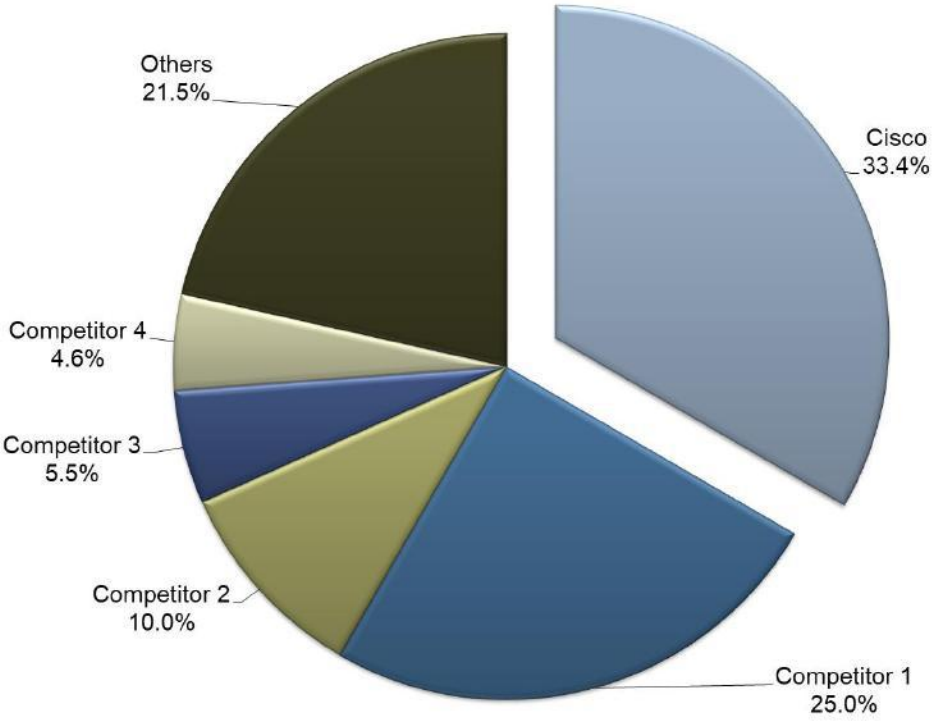
The NAC market is dominated by Enterprise and Large Enterprise customers, organizations with 2,500 or more employees. This is Cisco's primary customer base. The upper limit of Cisco's NAC deployments is upward of 500,000 concurrent endpoints, scalable to 2 million endpoints. Cisco is able to effectively serve these large organizations. Cisco is the dominant NAC player in Enterprise and Large Enterprise segments. It also dominates every vertical market and geographic region.

Cisco has a highly comprehensive NAC solution it continues to develop. ISE integrates with other Cisco technologies such as Advanced Malware Protection (AMP) and Stealthwatch. Cisco has focused on growing its third-party ecosystem and partnerships to increase visibility and automate threat containment to embrace a platform approach. ISE 2.7 extends to the industrial market. Cisco is focused on emerging IoT, especially Healthcare.

Cisco continues to enhance its NAC solution and target new developments. Customers are accelerating their migration to the cloud, and Cisco has stated they are committed to enable this transition across their portfolio. There is a growing interest in Zero Trust security model by customers. Cisco is integrating the technology from the acquisition of Duo Security. This acquisition provided a zero-trust security model, cloud-delivered technology, SaaS, and Software Defined Perimeter (SDP). ISE is extending the zero-trust model into the workplace to enable endpoint visibility and network segmentation necessary components to achieve access based on least privilege.

In the company's 2019 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.

Percentage of Revenue: NAC Market, 2019



Cisco's total security segment grew 16.1%% in fiscal 2019, compared to total corporate revenue growth of 5.0%. Frost & Sullivan estimates that Cisco NAC had revenues of $450 million in calendar 2019, growing 19.1% over 2018. 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's NAC solution is broad and comprehensive. The NAC solution 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 NAC offerings are expanding 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 Cyber Vision and MedicalNAC product offerings. Cisco partners with clinics, hospitals and medical equipment manufacturers to develop a holistic solution. Cisco's NAC solution combines Cisco Stealthwatch Enterprise, the Cisco Identity Services Engine, and Cisco TrustSec (SDA?) technology.

Most of Cisco's revenues attributed to the ISE product line are currently derived from physical appliance sales and term based software licenses. 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. With the acquisition of Duo Security, Cisco bolsters its development in cloud services, SaaS and zero trust security.

- Duo Security (August 2, 2018) - leading provider of unified access security and multi-factor authentication delivered through the cloud. According to the company, "Integration of Cisco's network, device and cloud security platforms with Duo Security's zero-trust authentication and access products will enable Cisco customers to easily and securely connect users to any application on any networked device."
- Sentryo (August 8, 2019) - Sentryo (Cyber Vision) technology, enhances security with increased device visibility in OT environments. According to Cisco, "This provides control systems engineers deeper visibility into assets to simultaneously optimize and secure their industrial networks and extend zero trust in the workplace."

Product Quality

Cisco's NAC architecture goes beyond the traditional Authentication, Authorization and Accounting (AAA). Cisco NAC offers a broad comprehensive range of features which it continues to expand. Cisco offers scalability ranging from small sites to millions of users. Visibility for ISE offers the ability to profile any device that connects to the networks. Cisco provides profiles for specific verticals, such as medical and industrial. It offers authentication methods for both passive and active identity. The Cisco physical and virtual 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's NAC for several reasons:

- The company offers a comprehensive a solution from endpoint to an application in the data center.
- The Cisco NAC solution involves many components and touches several different teams within an organization.
- The 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.
- Cisco ISE is the controller for Cisco SDA that allows for segmentation based enforcement options.

Cisco is developing its zero trust security with a holistic approach. This combines Cisco's core foundational solutions:

Duo for Workforce: identity-based approach to application access control.

Tetration for Workloads: host-based segmentation, combining visibility and enforcement.

SD-Access and ISE for Workplace: a fundamental component of NAC to start building a software-defined network (SDN) "fabric.

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 network and security portfolio integrating NAC with Cisco DNA Center, AMP, Cisco CTA, Stealthwatch and Firepower next generation firewall and intrusion prevention technologies. The company continues to strengthen its brand with the acquisition of Duo Security.

Cisco NAC benefits from the company being the leader in networking equipment and services, and the largest enterprise and security vendor by revenue. 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 a comprehensive all-encompassing NAC solution. The company has a trained partner network with over 700 highly trained partners on ISE and TrustSec.

The Cisco Security Technology Alliance (CSTA) is an active and growing ecosystem. Cisco actively partners with more than 100 security vendors to integrate their products with Cisco's security products. The standards are driven by Cisco's Platform Exchange Grid (pxGrid), an open, scalable, and IETF standards-driven platform. The CSTA continues to grow with currently over 175 development partners representing 300 plus product-to-product integrations to automate threat containment and simplify security operations.

Conclusion

NAC is a mature market but vendors need to innovate to meet the changing needs of its customers. 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. An emerging trend is zero trust security. Cisco is addressing zero trust with NAC as the foundational technology and integrating its security portfolio through NAC. 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 solution with a wide set of features and functions. The company is investing in IoT, BYOD and segmentation. 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 NAC. Cisco is driving wide spread adoption of its NAC solution 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 2020 Market Leadership Award to Cisco.

Significance of Market Leadership

Ultimately, growth in any organization depends on 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, and the company grows, and then attains market leadership. To achieve and maintain market leadership, an organization must strive to be best in class in 3 key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Market Leadership

Driving demand, strengthening the brand, and differentiating from the competition all play critical roles 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. Organizations that demonstrate best practices, 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.

Key Performance Criteria

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

Criterion	Requirement
Growth Strategy Excellence	There is a 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 brand 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	There is a 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 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

Frost & Sullivan analysts follow a 10-step process to evaluate award candidates and assess their fit with best practices criteria. The reputation and integrity of the 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 world	• Conduct in-depth industry research • Identify emerging industries • Scan multiple regions	Pipeline of candidates that potentially meet all best practices 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 practices 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 practices 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 practices 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 practices award recipient	• Review analysis with panel • Build consensus • Select recipient	Decision on which company performs best against all best practices criteria
9	**Communicate recognition**	Inform award recipient of award recognition	• Present award to the CEO • 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 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 the 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, resulting in 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, helps clients 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 practices models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages nearly 60 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on 6 continents. To join Frost & Sullivan's Growth Partnership, visit http://www.frost.com.