FROST & SULLIVAN

CORE SECURITY

2017 Global Network Threat Protection Solutions Technology Leadership Award

Contents

Background and Company Performance

Industry Challenges

Cybersecurity risk factors continue to increase as hackers evolve attacks into more customized and inventive threat patterns unknown and unrecognized by an enterprise's security monitoring systems. With these customized threats as top-of-mind, enterprises must implement threat detection and monitoring that can understand cyber-attackers' tactics, techniques, and procedures. Threat detection and a solid understanding of these attacks will then lead to necessary actions, such as strengthening prevention policies, minimizing impact to essential systems, and remediating compromised endpoints and systems.[1]

However, gathering the breadcrumbs left by cyber-attackers, filtering through the information, and correlating a vast stream of disparate data to identify any indicators of compromise (IoC) or emerging threats, are laborious but essential responsibilities that many enterprises lack the resources to undertake. Enterprises turn to managed security service providers (MSSPs) to fill this void and deliver valuable threat intelligence services.[2] Threat intelligence services implement three major tools to help enterprises protect their networks. Through threat research, intelligence gathering occurs through investigating security events, malware, exploits, vulnerabilities, and attack behaviors across any system type. Threat detection services combine security events with gathered threat intelligence to identify targeted attacks and advanced threats—these methods help to find attacks and threats which would have necessitated analysis from multiple data sources. Threat remediation services provide enterprises with instructions and guidance to mitigate any detected risks within their systems and research how these threats could affect an enterprise's operations.[3]

Frost & Sullivan research identifies the major deliverables from threat intelligence services as offloading threat detection to a third-party, identifying any under-reported threats and their purpose, gauging the potential system impact, and creating actionable mitigation or remediation procedures. MSSPs can also help enterprises focus on both outside network threats and threats carried out from within an enterprise's network through behavioral analysis to detect abnormal activity. Frost & Sullivan research estimates the North American market for threat intelligence services through MSSPs at $795 million, with market demand leading to a compound annual growth rate of 11.12% through 2020, accumulating revenues of over $1.3 billion. MSSPs looking to distinguish themselves from competitors must invest in delivering demonstrable customer value on a continuous basis through highly accurate and comprehensive threat intelligence protocols.

[1] See Frost & Sullivan's "Threat Intelligence Services Underlie Managed Security Services Growth," *Stratecast Perspectives & Insight for Executives,* Vol. 16, Number 40, Nov. 2016.
[2] See Frost & Sullivan's "Threat Intelligence Services Underlie Managed Security Services Growth."
[3] See Frost & Sullivan's "Threat Intelligence Services Underlie Managed Security Services Growth."

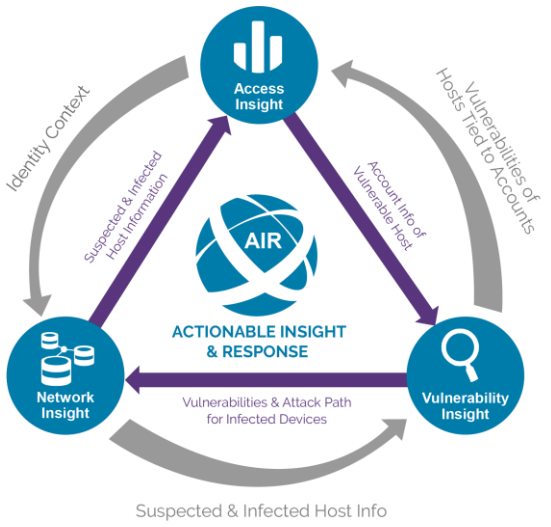
Technology Leverage and Business Impact

Core Security formed in mid-2016 as result of a series of strategic acquisitions and vision realignment towards a more holistic view of network threats, vulnerabilities and access control risks. The company offers enterprise customers threat-aware identity, access, authentication, threat, network detection and response, and vulnerability management solutions through its comprehensive Actionable Insight and Response Platform (AIR). AIR provides customers insights into their network security, identity and access control systems, and threat vulnerability assessments in one comprehensive platform, aggregating and monitoring all three security aspects in real-time to identify potential threats and attack patterns previously unknown to an enterprise's network protection system.

Comprehensive Network Security through Actionable Insight

Typical security solutions only look at one aspect of an enterprise such as identity and access management, network monitoring, endpoints, or vulnerability assessment. Core Security offers its customers with a comprehensive security solution, allowing them to break down the siloed security operations and bring all of their security operations together in one platform. The company's proprietary AIR Platform brings together three core threat detection capabilities: Network Insight, Access Insight, and Vulnerability Insight. Core Access Insight provides customers with a real-time, multi-view of their identity systems, access controls, and related resources to automatically evaluate and govern access permissions, remediate improper access, and simulate the behavioral patterns of potential attackers. Core Vulnerability Insight consolidates a security team's multiple system vulnerability scans, identifies, and eliminates potential cyber-attack paths through modeling threat scenarios and simulated attack patterns, as well as helps to prioritize vulnerabilities based on threat level and potential damage through flexible reporting options. Finally, Core Network Insight discovers hidden infections based on device communication activity—through either malware or advanced persistent threat behaviors—can terminate all device communication and present evidence of the attack to security operators. Operators can then prioritize the at-risk systems or devices through flexible remediation workflows, eliminating multiple false positives and remediating the most damaging threats early.

Actionable Insight and Response Platform



Source: Core Security

Through data accumulation from all three insight areas, operators develop a more vivid picture from which they can identify any vulnerability type, pinpoint unusual access behaviors, and simulate the "blast radius" of systems potentially affected by malicious threats. Core Security relies on its deep packet inspection, machine learning capabilities, and vulnerability analytics to determine at-risk devices, help decouple the associated identity, roles, and credentials available to attackers within a customer's network and what importance they may have.

The company's key differentiator lies in its reliance on identity as the core of its insights and analysis—allowing for surgically precise actions to stop an attack without completely interrupting a customer's business activity. No other threat prevention solution can act on attacks through the identity layer, positioning Core Security far ahead of competing solutions. AIR offers customers with a myriad of benefits to bolstering their threat protections. The platform's continuous monitoring and comprehensive visibility allows operators to monitor all devices, applications, infrastructure, and find access risks to understand and identify the root causes of possible threats. The platform empowers operators to act quickly in response to any identified threats and provides an automated governance process that will guide operators through remediation processes to stop all identified cyber-attacks. Finally, Core Security's AIR Platform allows operators to view these prioritized threats in one simple interface, showing more severe threats first and a full mitigation workflow procedure ready to address each threat.

Embracing Technological Innovation

Core Security's AIR Platform leverages key Mega Trends within its platform technology to differentiate its offering from any similar threat protection program. The company utilizes the Internet of Things to monitor, signal, and support network-connected devices as a way to protect against infection by malicious code. Core Security takes this technical functionality further, harnessing their "Identity of Things" capability to find and locate who exactly is attacking a particular device or system through AIR's integrated insight functions. The Big Data analytics features offer Core Security's customers much more perspective on their network data than other solutions. Security operators can now understand the devices connected to their network and their status, as well as highlight threat indicators and how to watch for suspicious activity on those devices. Additionally, AIR can help operators to understand the interconnected relationships between their access control systems, network controls, and individual user accounts and find potential risks by understanding all vulnerabilities within these systems.

Core Security leverages its first-mover advantage among threat protection solutions by building upon the inter-relationships between all types of network technologies. Through its strategic acquisitions of companies such as Damballa for threat discovery and multiple partnership alliances with other enterprise cybersecurity firms, the company continues to broaden and deepen its understanding of just how to secure enterprises and find malicious attack patterns. AIR's platform structure, built to run independent of any one operating system, allows for the platform to integrate within network architectures of all types. This easy deployment makes it simple for Core Security to reach out to any security-first

organization needing a more regulated identity and access credential visibility and control, regardless of industry. As such, Core Security serves customers within the financial services, oil and gas, and energy sectors, with growing interest from healthcare, technology developers, as well as global manufacturing and industrial customers due to the high value placed on network intelligence and access control in these markets.

High-Value Technology Offerings and Security Expertise

Core Security's comprehensive threat protection security solution appeals to both new and existing customers due to its ease of use, scalability, and low total cost of ownership. The company offers customers the ability to adopt portions of the AIR Platform offering and scale up to the full AIR usage when the customer chooses. The solution provides a flexible, simple deployment, where Core Security's AIR integration teams merely need access to customers' network data, allowing it to begin performing its analytics functions. Vulnerability detection capabilities only need these teams to input the network collectors so it can start adding the automated patterns for detection, while internal and external network detection sensors gather the necessary insight data—all completed within hours. This quick and seamless installation process makes it easy for customers to switch to Core Security's AIR solution. The AIR solution also receives automatic software updates from Core Security, while the company similarly maintains communication and customer relationships with its Customer Success Management team. The Customer Success Management teams work closely with the implementation teams to understand how the customer's installation process occurred and any potential future needs. Customers can also reach out to Core Security's robust customer service organization through Help Desk ticketing for any particular issues.

Core Security showcases its depth of intelligence knowledge through its thought leadership expertise. The company hosts a blog series on its website to inform subscribers of the latest innovations within the security market—its readership base currently exceeds 50,000 registered subscribers. Core Security also participates in digital marketing efforts to accelerate its organic growth through digital advertising practices. Its executive team also serves as subject matter experts through appearances at regional and global events, such as trade shows and conferences, offering industry perspectives through keynote or guest speaking engagements and panel discussions. Executives have also joined multiple security industry working groups to remain a prominent voice and advocate for thought leadership within the network security space.

Conclusion

Traditional network security solutions are falling behind on their ability to identify malicious threats to enterprise networks. As hackers create more customized and sophisticated attack patterns, these attacks can bypass traditional network protections undetected, potentially causing substantial data loss and information security breaches across multiple systems. Capitalizing on its history of threat intelligence protections, Core Security offers its comprehensive Actionable Insight and Response Platform for complete network security. By bringing together network security, identity and access control, and threat vulnerability identification, the platform can analyze all of an enterprise's network data and quickly identify threats before enacting remediation and mitigation procedures to minimize the impact to operations and halt these attacks.

Because of its robust threat intelligence analysis and commitment to protecting all network systems, Core Security is recognized with Frost & Sullivan's 2017 Technology Leadership Award.

Significance of Technology Leadership

Technology-rich companies with strong commercialization strategies benefit from the increased demand for high-quality, technologically innovative products. Those products help shape the brand, leading to a strong, differentiated market position.

Understanding Technology Leadership

Technology Leadership recognizes companies that lead the development and successful introduction of high-tech solutions to customers' most pressing needs, altering the industry or business landscape in the process. These companies shape the future of technology and its uses. Ultimately, success is measured by the degree to which technology is leveraged and the impact that technology has on growing the business.

Key Benchmarking Criteria

For the Technology Leadership Award, Frost & Sullivan analysts independently evaluated two key factors—Technology Leverage and Business Impact—according to the criteria identified below.

Technology Leverage

Criterion 1: Commitment to Innovation
Criterion 2: Commitment to Creativity
Criterion 3: Technology Incubation
Criterion 4: Commercialization Success
Criterion 5: Application Diversity

Business Impact

Criterion 1: Financial Performance
Criterion 2: Customer Acquisition
Criterion 3: Operational Efficiency
Criterion 4: Growth Potential
Criterion 5: Human Capital

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

Frost & Sullivan Awards follow a 10-step process to evaluate Award candidates and assess their fit with select best practice 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 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 about 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	• 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 can 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 players 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.