FROST & SULLIVAN

2018 North American IoT Cybersecurity Visionary Innovation Leadership Award

FROST & SULLIVAN

2018 BEST PRACTICES AWARD

NORTH AMERICAN IOT CYBERSECURITY VISIONARY INNOVATION LEADERSHIP AWARD

2018 BEST PRACTICES AWARDS

Contents

Background and Company Performance

Industry Challenges

In an era of digitization, cybersecurity implementations must fundamentally transform to deliver protection in enterprise networks that have become increasingly perimeter-less and more exposed to cyber-threats. Threat monitoring and assessment solutions cannot afford to ignore any given device type, network segment, or workload in order to adequately protect the enterprise network. However, the reality is that unknown assets and unmanaged networks are still discovered in enterprise networks monitored by vulnerability scanners and solutions. In fact, cyber-criminals have successfully used 'leak paths', such as those left open by contractors, to illegally obtain sensitive information or to disrupt network operations, even in networks that have deployed IT security solutions. The problem is not only the 'visibility gap'. Quite often, the isolation that exists between the various security tools and solutions must be removed in order to increase threat detection and response capabilities. For example, a lack of data normalization between cybersecurity tools and solutions can create inefficiencies in intrusion detection and response (IDR) operations.

The following tools are currently used for securing modern IT networks:

- Endpoint Security solutions
- Identity and Access Management solutions
- Network Access Control (NAC) solutions
- Network Firewalls and Gateways
- User and Entity Behavior Analytics (UEBA) platforms
- Security Information and Event Management (SIEM) solutions
- Security Operations, Analytics and Reporting (SOAR) products
- Application Security solutions
- Virtualization solutions

Each of these platforms offers a different vantage point of the network and adds to the security of the business IT network. However, the deployment of multiple systems requires organizations to train the workforce on every single toolset used for cybersecurity protection. This is a significant operational challenge. The shortage of a skilled workforce is a major industry issue in the North American cybersecurity markets.

The number of security alerts generated by security analytics tools continues to increase exponentially. However, it is simply not possible for security analysts to evaluate each and every alert that is generated due to the extremely large volumes. While incident response automation and orchestration can help to a degree, triaging, prioritizing, and investigating security alerts needs a certain level of human involvement. Optimizing the volume of alerts generated while operating within the constraints of cybersecurity best practices is a clear industry challenge.

As the walls come down between IT and IoT networks, the exchange of IP-enabled traffic can lead to the 'bleed-over' of malware from the IT environment to the OT environment. Integration of the IoT with enterprise IT creates additional challenges, including:

- Monitoring and securing the large volume of digital traffic generated by IoT systems;
- Malware-centric security approach is rendered ineffective as attacks on different IoT devices are often unique;
- Anti-malware software on endpoints can interfere with the operation of IoT devices;
- The inability of first-generation, traditional firewalls and NACs to identify, classify, and contextualize IoT devices prevents effective administration of security policies;
- Active vulnerability scanning is often disabled for the IoT assets and not used due to the fear of interference with connected device operations; and
- Connected device firmware is not always up-to-date and security patches are not applied regularly.

Today's modern networks can be secured by leveraging advanced AI and ML-based technologies that present new opportunities for cybersecurity threat detection and incident response. For example, by adopting an analytics-based, behavior-centric approach, as opposed to a signatures-based, malware-centric approach, cybersecurity providers can ensure that their solutions address scale and diversity challenges. Such solutions must consider network traffic as a 'source of truth' to expose the behavior of attackers and identify cyber-attacks with complete fidelity and independence. This is critical given that perimeter-based security mechanisms rely on identifying known threats and are at a higher risk of missing new forms of threats. A comprehensive understanding of the network through real-time network infrastructure monitoring is the foundation for effective cybersecurity.

Exhibit summarizes the key industry challenges in network cybersecurity.

Efficiency & Effectiveness	Disconnected Detection	Device Fragmentation
- Optimizing the cybersecurity functions - Implementations must help optimize the threat detection, classification and response functions while simultaneously reducing the workload of security professionals	- Data reconciliation and harmonization - Reducing inefficiencies such as duplicate alarms due to independent, non-collaborative and uncoordinated security operations in enterprise networks	- Protecting the diverse and fragmented IoT - Multiple device types, different deployment models, lack of endpoint security, limited processing and compute capacities are the prime IoT-specific cybersecurity challenges

Source: Frost & Sullivan

Focus on the Future and Best Practices Implementation

Vectra Networks (Vectra) is the leading provider of AI-based solutions that enable enterprises to detect and respond to advanced cyber-attacks in real time. The company offers the Cognito™ AI-powered cyber-attack detection and threat hunting platform that combines artificial intelligence, machine learning, and behavioral traffic analysis to expose the fundamental behaviors of attackers. Frost & Sullivan's research indicates that Cognito is a highly differentiated offering that applies ML and AI to address the broadest range of security use cases and deliver real-world efficiency in security functions. The key success factors for Vectra are presented below.

Focus on the Future

The Cognito platform includes Cognito Detect™ to find and stop attackers in real time, and Cognito Recall™, an efficient way to hunt for threats. Together, these two solutions help enterprises significantly improve their threat detection, prevention, prediction and response capabilities in manners best suited to their unique network characteristics and requirements.

Cognito Detect provides enterprise-wide visibility, exposing cyber-attackers. It analyzes network metadata, relevant logs and cloud events to gain high-fidelity visibility into the actions of all cloud and data center workloads and user and IoT devices. With Cognito Detect, security analysts have the most relevant context available for analysis and can take immediate action. Cognito Detect can be augmented by custom-matching indicators of compromise with threat indicators harvested from intelligence operations as well as feeds to conclusively detect known threats. Cognito Detect also enhances existing security investments. It enables enterprises to increase the value from their security teams and tools by providing the intelligence to block new classes of threats with existing enforcement points and by providing a clear starting point for a more extensive search with Cognito Recall or other tools.

Cognito Recall provides a more efficient way for professional threat hunters to begin their investigations into advanced cyberattacks that are identified by Cognito Detect. With Cognito Recall, Tier-3 security analysts can conduct deeper, productive investigations. Leveraging the virtually limitless scale of the cloud, Cognito Recall enables professional threat hunters to store and search enriched metadata from network traffic for as long as they need it, while Vectra manages the cloud infrastructure. For more intelligent investigation of device activity, Cognito Recall associates rich network metadata with device names, not just IP addresses. This enables professional threat hunters to quickly and easily get a view of device activity over time, which greatly improves the investigative process.

Best Practices Implementation

Vectra continues to innovate and invest in the Cognito platform to address the emerging

cybersecurity needs of enterprise customers. For example, Vectra is expected to introduce an API Wizard that will provide a simple tool for enterprise customers to integrate with third-parties for extraction or reading-in of security information. Cognito is also expected to leverage additional data sets beyond what it uses today to enhance its algorithm, including DNS logs and cloud events such as AWS CloudTrail.

Vectra realizes that it is essential to provide appropriate context to security events or alarms generated in order to help triage and prioritize response. In the absence of the ability to properly detail how big a problem really is, the avalanche of security alerts generated by various incident detection and response tools and platforms can often bury security analysts. With the proliferation of IoT data, this problem is only likely to escalate. However, with Vectra, enterprises get a unique ability to understand the threat severity levels to determine which alerts to prioritize. As enterprise IT networks continue to grow with hyper-connectivity, enterprises are increasingly seeking solutions to optimize their security operations. In this environment, Frost & Sullivan believes that the Vectra Cognito platform is extremely well positioned to gain traction in the worldwide cybersecurity market.

Cognito does not replace existing tools such as SIEM solutions used for security analytics. In fact, Cognito improves the operations of existing security analytics products by providing the ideal starting point for an investigation in these tools which, ultimately, has proven to enhance the efficiency of security personnel. Existing data repositories are not designed to function as real-time incident investigation and response tools, which creates a dangerous gap, sometimes lasting several months, between the time attackers infiltrate and spread inside of a network, and the moment they exfiltrate with stolen assets. Thus, the Cognito platform's ability to compress the active phase of an attack to reduce dwell time is one of the most important benefits.

Cognito leverages a combination of supervised and unsupervised machine learning algorithms. With supervised algorithms, Cognito can detect attacker behavior immediately. And, with unsupervised algorithms, Cognito requires approximately a one-week learning period and continuously adapts to the local environment to detect attacker behavior. The learning period for unsupervised algorithms ranges from five to ten days, which is noticeably lower that competing implementations, and continues to demonstrate ongoing improvement. Customer feedback indicates that implementations that rely solely on unsupervised algorithms have a longer learning period and may require additional manual threat hunting that needs to be done by security analysts to triage and correlate the detections. The Cognito algorithms are designed to define explicit attacker behaviors (such as external IP controlling an internal device or an internal host communicating to a new IP address or domain) rather than simple anomalies, which is a key reason for the superior performance of Cognito.

Summary

The exhibit below summarizes the key benefits of the Vectra Cognito cybersecurity solution for enterprises.

Automates Threat Detection	Always-learning behavioral models use AI to efficiently find hidden and unknown attackers in real time. This enables quick, decisive action, and provides a clear starting point for manual threat hunting.
Empowers Threat Hunters	Cognito enables professional threat hunters to launch deeper and broader investigations of incidents detected by Cognito and other security enforcement points. This facilitates hunting for undetected cyberattacks retrospectively.
Provides Enterprise-wide Visibility	Real-time collection, analysis, and storage of rich network metadata, relevant logs and cloud events provides high-fidelity visibility into the actions of all cloud and data center workloads and IoT devices, leaving cyber-attackers with nowhere to hide.
Captures Once, Does many Things	The Cognito platform collects and analyzes rich network metadata, augmented by relevant logs and cloud events, to enable real-time automated threat detection, manual threat hunting, retrospective threat hunting, and incident investigations.

Competitive Analysis

The ability to address a broad range of cybersecurity use cases is a differentiator for Vectra. Vectra's competitors, particularly in the behavioral analytics space, are good at handling a relatively small number of security use cases. However, with Cognito, enterprises can expose the widest range of fundamental attack behaviors in network traffic, including:

- command-and-control and other hidden communications,
- internal reconnaissance,
- lateral movement
- abuse of account credentials,
- data exfiltration,

- early indicators of ransomware activity,
- botnet monetization, and
- attack campaigns, including the mapping of all hosts and their associated attack indicators.

Cognito competes with the UEBA providers by addressing two of the most important use cases that UEBA products address. These include credential theft and abuse, and insider threats. Cognito uses an advanced approach to ensure that all possible misuse or threats related to credential abuse and insider threats are identified. For example, to address the most harmful form of credential abuse, which is stolen admin credentials, the Cognito platform includes algorithms that learn the normal administrators and associated protocols, enabling Cognito to detect both a suspicious admin and suspicious admin protocol use. Through internal reconnaissance and lateral movement detections, Cognito can uncover hidden attackers and insiders as advanced hackers usually quietly watch and learn the tools that an organization uses and then blend in to remain hidden. This is critical, since an attacker that has gained this mode of access to internal networks is, for all intents and purposes, an 'insider.'

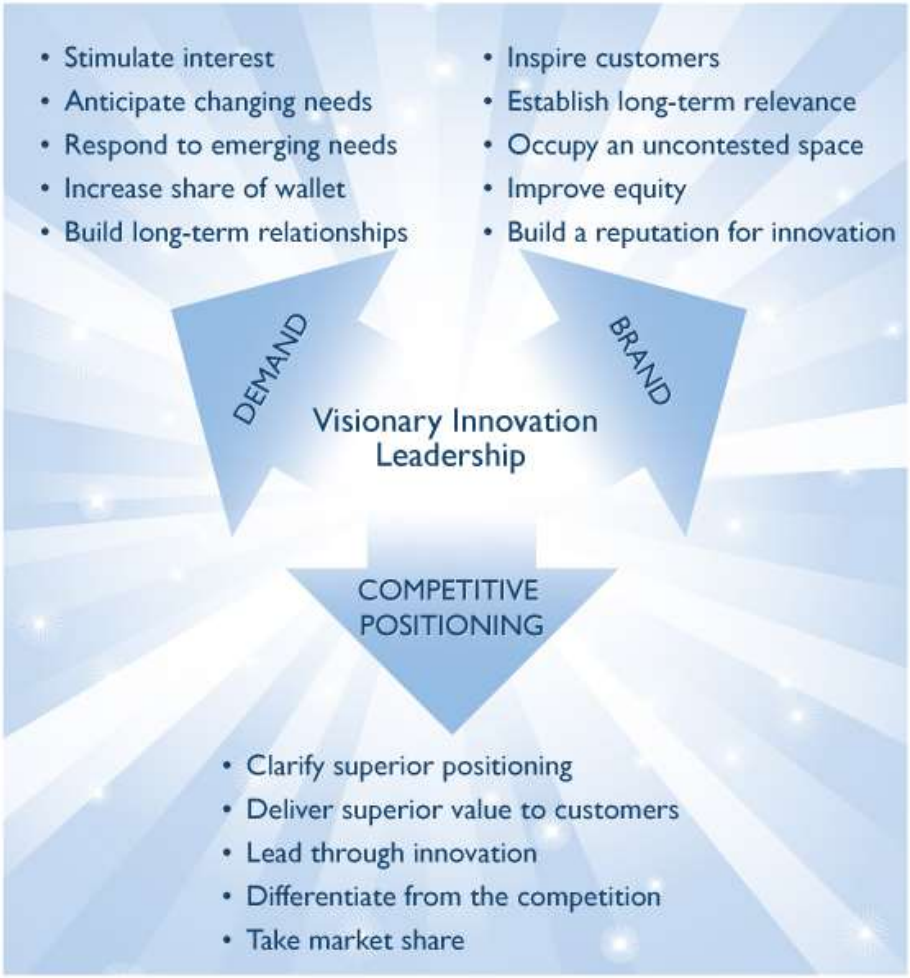
Cybercriminals are using increasingly sophisticated tools and malware and constantly change their attack methods to evade detection. A significant share of malware used in cyberattacks is either unique to the organization, or as is the case of the IoT, specific to the endpoint. These threat vectors are therefore new and have never before been observed or identified. Therefore, perimeter defense solutions which rely on signatures and reputation lists of known threats are inadequate in the dynamic cybersecurity threat landscape. The ability to offer an unparalleled level of flexibility and agility for a wide variety of use cases is a strategic advantage for Vectra. The adoption of Cognito in verticals such as Healthcare, Education, Media and Entertainment, and Industrial Automation is a clear testament to the proven capabilities of its implementations and success of its go-to-market strategy.

Conclusion

By monitoring, analyzing and contextualizing all network traffic, cloud and log events, Cognito enhances the cybersecurity posture of enterprise networks. Vectra continues to raise the bar in AI-driven threat detection and response, and is expected to maintain its growth on the strength of its cutting-edge Cognito platform. With its strong overall performance, Vectra is recognized with Frost & Sullivan's 2018 Visionary Innovation Leadership Award.

Significance of Visionary Innovation Leadership

A Visionary Innovation Leadership position enables a market participant to deliver highly competitive products and solutions that transform the way individuals and businesses perform their daily activities. Such products and solutions set new, long-lasting trends in how technologies are deployed and consumed by businesses and end users. Most important, they deliver unique and differentiated benefits that can greatly improve business performance as well as individuals' work and personal lives. These improvements are measured by customer demand, brand strength, and competitive positioning.



Understanding Visionary Innovation Leadership

Visionary Innovation is the ability to innovate today in the light of perceived changes and opportunities that will arise from Mega Trends in the future. It is the ability to scout and detect unmet (and as yet undefined) needs and proactively address them with disruptive solutions that cater to new and unique customers, lifestyles, technologies, and markets. At the heart of visionary innovation is a deep understanding of the implications and global ramifications of Mega Trends, leading to correct identification and ultimate capture of niche and white-space market opportunities in the future.

Key Benchmarking Criteria

For the Visionary Innovation Leadership Award, Frost & Sullivan analysts independently evaluated two key factors—Focus on the Future and Best Practices Implementation—according to the criteria identified below.

Focus on the Future

Criterion 1: Focus on Unmet Needs

Requirement: Implementing a robust process to continuously unearth customers' unmet or under-served needs, and creating the products or solutions to address them effectively

Criterion 2: Visionary Scenarios through Mega Trends

Requirement: Incorporating long-range, macro-level scenarios into the innovation strategy, thereby enabling "first-to-market" growth opportunity solutions

Criterion 3: Growth Pipeline

Requirement: Best-in-class process to continuously identify and prioritize future growth opportunities leveraging both internal and external sources

Criterion 4: Blue Ocean Strategy

Requirement: Strategic focus on creating a leadership position in a potentially "uncontested" market space, manifested by stiff barriers to entry for competitors

Criterion 5: Growth Performance

Requirement: Growth success linked tangibly to new growth opportunities identified though visionary innovation

Best Practices Implementation

Criterion 1: Vision Alignment

Requirement: The executive team is aligned along the organization's mission, vision, strategy, and execution.

Criterion 2: Process Design

Requirement: Processes support the efficient and consistent implementation of tactics designed to implement the strategy.

Criterion 3: Operational Efficiency

Requirement: Staff performs assigned tactics seamlessly, quickly, and to a high-quality standard.

Criterion 4: Technological Sophistication

Requirements: Systems enable companywide transparency, communication, and efficiency.

Criterion 5: Company Culture

Requirement: The executive team sets the standard for commitment to customers, quality, and staff, which translates directly into front-line performance excellence.

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.

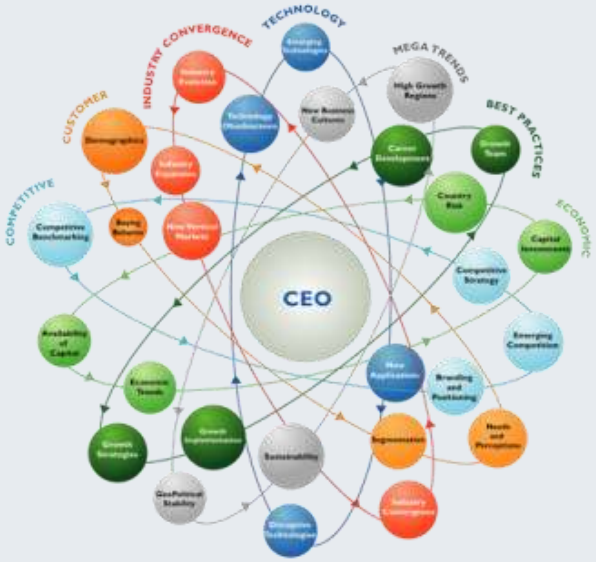
	STEP	OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify Award recipient candidates from around the globe	• Conduct in-depth industry research • Identify emerging sectors • Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 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 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	• 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 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.