FROST & SULLIVAN

FROST & SULLIVAN BEST PRACTICES AWARDS

IOT CYBERSECURITY - NORTH AMERICA

Visionary Innovation Leadership 2019

NXM

FROST & SULLIVAN

2019 BEST PRACTICES AWARD

Contents

Background and Company Performance

Industry Challenges

Market Overview

IoT is increasingly permeating every aspect of consumer and enterprise activities. With the growth of microelectronics, ubiquitous connectivity, and predictive computing, IoT is poised for rapid growth. Frost & Sullivan expects the total number of IoT devices to grow from approximately 12.4 billion devices in 2016 to over 45.4 billion devices in 2023, at a global compound annual growth rate (CAGR) of 18.6%. The future of IoT involves billions of connected devices communicating with one another, regardless of the manufacturer, operating system, chipset, or physical transport mode. While it is hard to categorize IoT as an industry, the ecosystem for IoT has evolved since the days of traditional machine-to-machine (M2M) communications. Today, IoT is about developing ecosystems that help organizations convert real-time data into actionable intelligence.

The Evolution of IoT

'Smart' connected devices that think, transact, and exchange data are the next evolution of IoT. As IoT matures, the emphasis will be on implementing approaches that enable IoT devices to interact with – and learn from – other IoT endpoints and data sources to enable proactive decision making without human intervention. However, the need for cybersecurity will further intensify as more IoT devices are given the ability to make intelligent decisions. For example, IoT devices that engage in financial transactions could be attractive targets for hackers and other bad actors that may want to steal funds stored on digital wallets on these devices. As more IoT devices operate autonomously and exchange data, it becomes critical to implement suitable privacy controls to ensure that sensitive information is not exposed or shared with unauthorized users at any point during the data journey.

IoT Cybersecurity Essentials

IoT devices often exist outside the protective barriers of corporate firewalls and lack the computing and storage resources to host security software. Therefore, cybersecurity implementations must work within the unique constraints of IoT. Communication from different types of devices can have unintended consequences such as cross-device contamination and misinterpretation of data service requests. All of these possibilities must be considered when implementing IoT cybersecurity frameworks. The existing centralized cybersecurity mechanisms may not be suitable in addressing the evolving cybersecurity requirements in the IoT. For example, a centrally administered security solution may not be scalable to support millions of IoT devices on enterprise networks. Additionally, a central repository of sensitive data establishes a single point of vulnerability for hackers to exploit. Therefore, Frost & Sullivan firmly believes that IoT cybersecurity approaches that go beyond the centralized client-server mechanisms must be evaluated for the next-generation of IoT.

Need for Distributed Cybersecurity

Blockchain-based distributed implementations that do not have a single point of failure can adequately support autonomous communication, collaboration and commerce activities. A distributed, decentralized implementation is highly secure and particularly arduous for bad actors to compromise a single device ID (in contrast to gaining unauthorized access to a centralized platform that hosts the security credentials for multiple devices). Secure device identity validated in real time by a community of approved industry participants can introduce high levels of trust to help secure autonomous IoT transactions. Any such implementation must protect IoT devices through the lifecycle of their deployments. The system must also have the ability to identify asset malfunctions to detect cybersecurity threats and respond to them expeditiously. Many open-source security options are available for IoT; however, Frost & Sullivan believes that open-source implementations need considerable adaptation and optimization in order to deliver scalable and effective protection for IoT.

Focus on the Future and Best Practices Implementation

NXM Labs

NXM Labs Inc. is an Autonomous Security software company that enables IoT devices to operate and communicate with each other and their surroundings automatically and securely without human intervention. By combining blockchain-based implementations with advanced cryptographic methodologies, NXM enables the creation of highly secure, fully distributed and decentralized ecosystems of self-governing, autonomous IoT devices. NXM is compatible with ARM's Platform Security Architecture (PSA), as well as Intel's Software Guard Extension (SGX) and Memory Protection Extension (MPX) frameworks and those of other chip makers. NXM's software-based technology is anchored in silicon and takes advantage of the hardware accelerated security capabilities of today's chips. The company is working with various industry bodies to certify its technology on multiple platforms.

Key Innovations

The company's **NXM SecureSuite** platform addresses the full spectrum of security, device deployment and data management requirements of IoT operations. The solution has been purpose-built for enterprise IoT deployments and is based on a distributed trust system that is extremely difficult to undermine. Networks of self-governing IoT devices, wherein each device assigns its own machine ID and acts as an intelligent node in a consensus-based P2P network, are central to NXM's autonomous security technology. Complementary innovations that enable NXM to offer unparalleled security for IoT device networks include:

1) Agile (variable) cryptography capabilities for remote upgrading of cryptographic algorithms to dynamically update or change the security mechanisms of devices at any time to adjust to new regulations and guard against future threats, including quantum computers;

2) Innovative usage of smart contracts and machine learning to enable exceptional data

privacy protection by separating machine data from personal private confidential information at the chip level in a manner that conforms to all global privacy standards, and in doing so creating high-value anonymized data sets that can be readily monetized;

3) A service-oriented blockchain to enable flexible deployment and control mechanisms;

4) 5G-ready architecture for device-level operations and virtualization capabilities that act as a bridge between 4G and 5G networks; and

5) A hybrid blockchain architecture combined with faster proof-of-authority (PoA) consensus and advanced blockchain infrastructure to support high-speed operations.

Offensive Cybersecurity

It can take months before a malware infection is detected in IoT networks. Therefore, while detection is important, the focus should be on *preventing* IoT cybersecurity incidents to effectively secure IoT networks. NXM employs a unique offensive security model based on blockchain network enforcement. In NXM's system, interactions through smart contracts require cryptocurrency gas (tokens), which allows gas to be used as a control mechanism to delimit interactions and shape the device behavior. Gaining unauthorized access to a single NXM-enabled device will require a large amount of cryptocurrency. This makes it extremely unattractive for hackers to circumvent cybersecurity controls in NXM-enabled deployments. Provisions can be made such that by cutting the source of cryptocurrency any bad actor can be immediately stopped and contained programmatically without the need for human intervention. As the ledger of devices is distributed in NXM-enabled deployments, a compromised device cannot erase traces of its activity from all the other nodes. This provides for efficient post-incident forensics capabilities, which is an important benefit.

Customizable Implementations

NXM's solutions can be used across multiple industry verticals to address the network security, data privacy, and integrity requirements of next-generation IoT. The company is collaborating with major industry players to develop solutions for industry verticals that can deploy millions if not billions of devices. NXM's IoT cybersecurity implementations, which currently run on Ethereum, are blockchain agnostic. NXM can work with other platforms such as IBM Hyperledger Fabric and Corda, as well as those of other leading solution providers, to expand the total addressable market opportunity for the company. Commercial deployments of NXM's software platform have already begun, starting with a high-speed automotive router to enable ultra-secure wireless connectivity and deployment of trusted connected car applications.

Moreover, the Company has partnered with Sprint, a tier-I carrier in the U.S. to launch a 5G-Ready Connected Car Platform based on its autonomous security IP. NXM has recently signed a global agreement with IBM and is in discussions with other IoT platform management providers. The Company has also started licensing its technology to original device manufacturers to create secure edge devices that can be warrantied against unauthorized hardware access and marketed as being highly resistant to hacking. Early

success with the leading IoT industry ecosystem participants is a promising validation for NXM's IoT cybersecurity implementations.

Ecosystem-centric Approach

NXM SecureSuite is a pioneering implementation that offers a revolutionary approach to IoT security at scale. The company's high-speed blockchain-enabled router, an integral part of its connected car solution, is an important proof point to demonstrate how the technology can work at scale. NXM has adopted an ecosystem-centric approach and engages with hardware, telecommunications and software/cloud vendors to develop a collaborative ecosystem that leverages the superior characteristics of its blockchain-enabled implementation. Not only does NXM help secure the IoT, it also enables the monetization of fully anonymized and targeted machine data. Frost & Sullivan's research confirms the ability of NXM to deliver the optimum set of capabilities to fully address the autonomous IoT security concerns, while supporting data-centric business models for IoT industry participants.

Competitive Differentiators

The application of traditional, IT-centric cybersecurity models by competing cybersecurity solution providers hinders the development of cross-vertical, intelligent IoT solutions. In contrast, NXM by design is created for scalable global machine-to-machine communications, without human intervention. The company continues to invest aggressively in new product enhancements to support its long-term growth strategy and ensure that all customers – regardless of their size or location – receive high quality service and support. NXM believes that IoT security must be comprehensive in nature and that point solutions create gaps in security that can be exploited.

As a company with a 360 degree approach to IoT cybersecurity, NXM provides the security fabric to ensure cybersecurity all the way from the hardware to the cloud ("chip-to-cloud"), which is a clear differentiator for the company. While there are several competing approaches to handle authentication and encryption at scale in IoT, Frost & Sullivan believes that NXM will demonstrate strong growth momentum consistent with the proliferation of autonomous IoT.

Conclusion

The proliferation of independent, autonomous IoT devices is driving new opportunities for data sharing and connected operations. However, intelligent IoT deployments create demands for high-performance cybersecurity that cannot be offered by legacy IoT cybersecurity implementations. By addressing the cybersecurity needs of automated IoT through blockchain-based implementations, NXM has enhanced value to customers. The company has developed specific strategies and working prototypes to secure IoT implementations that are automated, scalable, and economical. With its strong overall performance, Frost & Sullivan is proud to recognize NXM Labs with the 2019 Frost & Sullivan 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.