2017 North American IoT Security Platform for Industrial Manufacturing & Automation Product Leadership Award
Contents
Background and Company Performance ................................................................. 3

Industry Challenges ................................................................................................. 3

Product Family Attributes and Business Impact ...................................................... 3

Conclusion .................................................................................................................. 7

Significance of Product Leadership .......................................................................... 8

Understanding Product Leadership ......................................................................... 8

Key Benchmarking Criteria ....................................................................................... 9

Best Practices Award Analysis for Mocana Corp ....................................................... 9

Product Family Attributes ....................................................................................... 9

Business Impact ......................................................................................................... 9


The Intersection between 360-Degree Research and Best Practices Awards ........... 11

Research Methodology .............................................................................................. 11

About Frost & Sullivan .............................................................................................. 11


Background and Company Performance

**Industry Challenges**

Current enterprise security models and best practices that feature information technology/operational technology (IT/OT) approaches such as layered network defenses, threat analytics, threat mitigation, protocol filtering, and air gaps (to separate the enterprise networks from the OT networks) are not sufficient enough to secure mission-critical Internet of Things (IoT) and embedded systems used in OT environments against cyber-attacks. One curious aspect of industrial IoT is that even though companies are connecting different systems to the Internet, the attack vectors that they need to worry about are not necessarily Internet-based. That is, the primary attack vectors are going to be social engineering and physical security breaches—hackers taking over devices (e.g., valves, controllers, and security cameras) and industrial control systems by getting behind firewalls. The fundamental problem is the overall weakness of IT/OT security approaches, which, therefore, calls for a new IoT security approach involving a device-to-cloud architecture.

Another factor that makes the aforementioned approaches ineffective is that the devices and industrial control systems needing protection have very limited CPU and memory, which makes it difficult to load cryptography, encryption, and other software security features into the devices. These constraints represent an incredibly high level of risk for manufacturing facilities, oil refineries, gas utilities, and all other industrial spaces that depend on this sort of security to ensure safety and reliability and minimize loss of lives, loss of critical services, and downtime of an entire plant. Chief risk officers, at the board-level in manufacturing and industrial companies, are demanding cybersecurity audits to understand their cyber posture, the impact of risk, and what they should do to manage it. Under such circumstances, companies that can provide a comprehensive IoT security platform that addresses the aforementioned challenges where the cybersecurity software is loaded onto devices while requiring minimal processing power and memory to provide secure device-to-cloud communications will secure a leadership position in the market.

**Product Family Attributes and Business Impact**

**Match to Needs**

Founded in 2002 as an embedded security software company for military applications, Mocana today delivers deep cybersecurity and embedded systems expertise to various manufacturing facilities via its comprehensive, device-to-cloud IoT security platform at a time when numerous other existing security approaches are protecting the gateway to the cloud but leaving all other devices and systems unsecure. These devices that are not securely connected have no device-level integrity built in to protect them. Mocana’s platform is strikingly different because its software sits on the device, on the gateway, and on the cloud, thereby going beyond the traditional perimeter-based security approaches and enabling secure device-to-cloud communications.

Mocana follows a Federal Information Processing Standard (FIPS)-based approach, and its software relies on a FIPS 140-2 validated cryptographic engine that uses a comprehensive
set of asymmetric and symmetric ciphers and standard X.509 certificate management protocols. Its cryptographic software authenticates individual devices and gives them an identity by creating a unique private key and a certificate. Each device is enrolled by a manufacturer, and when sold, the end user is able to enroll and sign it using its own certificate authority. This method results in three different certificates: one for the device, one for the manufacturer, and one for the end user. At this point, Mocana begins hashing and creating certificates on the BIOS, firmware, and kernel. A single keyed-hash message authentication code (MAC) at the top then allows having a certificate that has hashed all of the different certificates, ensuring that nothing has changed on the device, which gives it integrity. Most lateral hacks attempt to update the firmware on a device with a virus or malware, and Mocana’s approach can prevent that from happening.

Frost & Sullivan applauds Mocana for demonstrating powerful product leadership here by fortifying the unprotected devices/endpoints that have minimal CPU and memory with an X.509 certificate, the ability to encrypt, and provision of secured transport from that endpoint to whatever it is connecting to, whether a gateway or directly with the cloud. The volume of actionable security insights available to manufactures, moreover, helps to improve the safety, availability, visibility, integrity, control, and confidentiality of their devices, control systems, gateways, and cloud applications.

**Design**

Mocana differentiates itself from the competition by providing value-added product attributes and IoT security-specific features. Precisely because most devices have minimal processing power and memory, Mocana has designed its cryptography engine with a tiny, lightweight footprint of less than 30KB. Its software offers high performance and is fast and responsive for hashes and advanced cryptographic functions. In addition, the software modules that sit on the device, gateway, and cloud are customizable whereby customers can deploy only the code they need to implement the specific functions required.

Mocana’s comprehensive, full-stack IoT security platform that is highly flexible and modular in nature supports a variety of complex networking environments such as secure sockets layer (SSL), secure shell (SSH), multicast, Internet protocol security (IPSec), wireless, simple certificate enrollment protocol (SCEP), and enrollment over secure transport (EST). What largely differentiates the platform from competing products is its ability to operate across multi-vendor environments because it is integrated with more than 70 chipsets, 30 operating systems, and real-time operating systems (RTOS).

Mocana stays abreast of the latest trends and strives to incorporate additional functionalities so that its software remains on par with the latest industry requirements and technological advancements. For instance, its new platform (the latest version of its security software solution) has two added functionalities, NanoTAP 1.2 and NanoAIDE, which allow companies to use hardware with a much higher level of security and to automate certificate management. NanoTAP is an abstraction layer that makes it easy for customers to use hardware-based security modules such as trusted platform module (TPM) and TrustZone in their security design. NanoAIDE supports the EST protocol for automated certificate management to help companies scale in managing millions of
certificates in IoT devices. And, most recently, Mocana announced an IoT security development kit that is customized for a Raspberry Pi, a series of small single-board computers, integrated with the Infineon OPTIGA TPM chip that supports a variety of Wi-Fi modules and on-board certificate management. The kit allows developers new to IoT security to use sample applications and test cryptographic controls on a resource-constrained IoT device. By virtue of these superior functionalities, Frost & Sullivan believes Mocana has engineered a comprehensive IoT security platform that provides device integrity as opposed to competing platforms that provide only data security. By and large, these unique product design attributes are set to help Mocana increase adoption of its IoT security platform.

**Product/ Service Support**

Mocana focuses on working closely with its customers to ensure they gain maximum value from its solution. The company offers a service experience by way of technical support and professional services packages provided through its highly trained engineers. The support packages are designed to address the needs and constraints of various company types that cover small, medium, and large operations. The technical support packages consist of three levels of support (silver, gold, and platinum) so that customers can choose the support that best fits their needs. As part of the professional services, Mocana’s team of engineers, with their deep cyber security expertise, helps customers initiate their development as soon as possible and even validate that Mocana’s security modules have been implemented according to their published guidelines. These dedicated resources are available on-site to support and address customers’ development needs and accelerate the development process and minimize implementation risks.

**Customer Acquisition**

Mocana prides itself on its extensive customer list. It currently supports about 200 customers, and approximately 80% of them are from industrial manufacturing and automation. Some of the leading companies from this vertical that have deployed Mocana’s IoT Security Platform are Panasonic, Siemens, Emerson, GE, Samsung, Bosch, Yokogawa and Schneider Electric. These major device manufacturers are selling into process and discrete manufacturing. For example, Mocana has teamed with GE Digital to integrate Mocana’s solution into a variety of GE industrial controllers and the GE Predix Machine. Its software is implemented on PLCs, gateway controllers, thermostats, HVAC systems and industrial IoT devices to secure and encrypt communications from the endpoint to IoT clouds and supervisory control and data acquisition (SCADA) systems. Mocana’s software delivers key generation, encryption, decryption, sign, and verify messages.

**Sales Strategy**

The company’s primary go-to-market strategy is through direct sales to large industrial manufacturers such as divisions or large companies with $1 billion in revenues where Mocana sells software to their cyber architects, chief information security officers, chief risk officers, and manufacturing product managers. The company also has a channel strategy to address contract manufacturers who want to buy through distribution. While
Mocana’s focus is on companies that are building devices, either IoT devices or industrial control devices, it is also working with a number of telecom and cloud providers that sell to companies that build out or manage critical infrastructure, smart buildings, and Smart Cities. Frost & Sullivan believes that in today’s world where the digital transformation is causing industry convergence and expanded customer bases for many future-ready businesses, the various layers of Mocana’s customer engagement model will result in rising adoption of its IoT Security Platform across a wide scope of customers.

**Business Model**

Mocana’s business model is straightforward: It sells production licenses of its software as well as development licenses. Customers purchase the license and earn the ability to customize the source code, compile it, build/implement as binaries into their device, and, once it is built into the device, whoever buys the device has perpetual use of the software. For some companies in the telecom and networking industry, where they have a strong understanding of the number of units (e.g., set-top boxes), Mocana offers a royalty model. Other customers pay a flat fee for licensing to produce their products in a certain quantity for certain product lines (i.e., product-specific licensing). Such a straightforward business model makes Mocana attractive to various types of customers, both prominent ones as well as the lesser known.

**Expansion Approach**

With regards to expansion into more target accounts, Mocana works in concert with its partners. The company has a business development and partnership strategy that hinges on close working relationships, especially with chip and RTOS companies. That said, the company has built an extensive ecosystem of partners across the globe and has many integration partners. It has forged strong partnerships with some of the most prominent chipset manufacturers in the industry such as Intel, Infineon, NXP, Qualcomm, and ARM, followed by operating system and RTOS companies such as QNX, Microsoft, Wind River, DDC-I, and Green Hills. Other partners include many of the chip companies that provide hardware-based root of trust (a set of functions, in the trusted computing module, trusted by the operating system) such as Gemalto, Atmel, and ST Micro.

With such a robust portfolio of customers and integration partners that the company continuously expands, Mocana is expected to further strengthen its position in the North American market.

**Growth Potential**

An increase in attacks to enterprises that involve IoT, growing vulnerability of IoT device manufacturers to new threats, and expanded IoT security budgets are expected to drive growth for Mocana in the next two to three years.

Mocana’s IoT Security Platform, focused primarily on large industrial device manufacturers, is currently on about 100 million devices securing IoT endpoints, programmable logic controllers (PLCs), remote terminal units (RTUs), controllers, and gateways. The company plans to have security built into billions of devices by teaming up with large industrial and IoT companies through product strategy and by targeting new
end markets. Mocana has been successful in promoting product leadership not only in industrial manufacturing and automation but also in drawing the attention of leaders from a wide range of other industries such as energy, oil and gas, utilities, aerospace and defense (on avionics, radar, weather, flight safety navigation systems on the aircraft and ruggedized vehicles), medical (building stronger security in to MRI machines), and telecommunications and networking. The company caters to market leaders such as General Dynamics, L3 Aviation Products, Northrop Grumman, HTC, Avaya, Ruckus Wireless, and Motorola, to name a few. In the entertainment sector, the applications are on set-top boxes. Smart building and smart cities represent another big area for company growth, for instance, in upgrading safety and fire systems in large commercial buildings and homes.

Many mid-sized companies and some of the larger ones (from telecommunications and networking) are building out their new product lines with stronger IoT security. In the industrial control space, one market characteristic is the high volume of installed legacy systems, of which many brownfield devices in industrial environments need to be upgraded, and energy companies are currently doing so. Mocana is expected to benefit from, first, the many companies that will be launching their own IoT platforms, and second, from companies that will be upgrading existing brownfield devices. In 2018, Mocana will integrate further into the distribution channel, which is expected to generate new areas of growth.

From a product strategy perspective, Mocana is continuing to build new functionality and platform support through operating systems, chip vendors, and roots of trust. In fact, one of the functionalities Mocana is building is a new management and analytics platform that will add significant value to its customers who will not only have strong security built into their devices but will also gain detailed security data down to the device process level. Currently, its customers do not get such details from network-based threat analytics.

Overall, macroeconomic trends, a strong product strategy, and promising applications in new end markets are expected to boost Mocana’s growth potential.

**Conclusion**

Offering one of the most highly flexible, comprehensive, full-stack IoT security platforms available on the market today, Mocana has ramped up its capabilities to render unmatched product value and to consolidate its position in the IoT security for industrial manufacturing and automation space. Mocana’s competitive edge results from a unique device-to-cloud security model that outpaces traditional perimeter-based security approaches to deliver device-level integrity. Overcoming the challenge of devices and industrial control systems having minimal memory and processing power, Mocana’s cybersecurity software is easily embedded into them to prevent hackers from taking over control. Mocana has remained true to its core mission of shifting the mindset from security to trust as its platform currently protects 100 million devices and makes them trustworthy. With its strong overall performance, Mocana has earned Frost & Sullivan’s 2017 Product Leadership Award.
Significance of Product Leadership
Ultimately, growth in any organization depends upon customers purchasing from a company and then making the decision to return time and again. A comprehensive product line, filled with high-quality, value-driven options, is the key to building an engaged customer base. To achieve and maintain product excellence, an organization must strive to be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Product Leadership
Demand forecasting, branding, and differentiating all play a critical role in finding growth opportunities for your product line. This three-fold focus, however, must be complemented by an equally rigorous focus on pursuing those opportunities to a best-in-class standard. Customer communications, customer feedback, pricing, and competitor actions must all be managed and monitored for ongoing success. If an organization can successfully parlay product excellence into positive business impact, increased market share will inevitably follow over time.
Key Benchmarking Criteria

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

### Product Family Attributes

- **Criterion 1: Match to Needs**
  Requirement: Customer needs directly influence and inspire the design and positioning of the product family.

- **Criterion 2: Reliability and Quality**
  Requirement: Products consistently meet or exceed customer expectations for performance and length of service.

- **Criterion 3: Product/Service Value**
  Requirement: Products or services offer the best value for the price, compared to similar offerings in the market.

- **Criterion 4: Positioning**
  Requirement: Products or services address unique, unmet need that competitors cannot easily replicate or replace.

- **Criterion 5: Design**
  Requirement: The product features an innovative design, enhancing both visual appeal and ease of use.

### Business Impact

- **Criterion 1: Financial Performance**
  Requirement: Overall financial performance is strong in terms of revenues, revenue growth, operating margin, and other key financial metrics.

- **Criterion 2: Customer Acquisition**
  Requirement: Product strength enables acquisition of new customers, even as it enhances retention of current customers.

- **Criterion 3: Operational Efficiency**
  Requirement: Staff is able to perform assigned tasks productively, quickly, and to a high quality standard.

- **Criterion 4: Growth Potential**
  Requirements: Product quality strengthens brand, reinforces customer loyalty, and enhances growth potential.

- **Criterion 5: Human Capital**
  Requirement: Company culture is characterized by a strong commitment to product quality and customer impact, which in turn enhances employee morale and retention.

### Best Practices Award Analysis for Mocana

**Product Family Attributes**

- **Criterion 1: Match to Needs**
  Requirement: Customer needs directly influence and inspire the design and positioning of the product family.

- **Criterion 2: Reliability and Quality**
  Requirement: Products consistently meet or exceed customer expectations for performance and length of service.

- **Criterion 3: Product/Service Value**
  Requirement: Products or services offer the best value for the price, compared to similar offerings in the market.

- **Criterion 4: Positioning**
  Requirement: Products or services address unique, unmet need that competitors cannot easily replicate or replace.

- **Criterion 5: Design**
  Requirement: The product features an innovative design, enhancing both visual appeal and ease of use.

**Business Impact**

- **Criterion 1: Financial Performance**
  Requirement: Overall financial performance is strong in terms of revenues, revenue growth, operating margin, and other key financial metrics.

- **Criterion 2: Customer Acquisition**
  Requirement: Product strength enables acquisition of new customers, even as it enhances retention of current customers.

- **Criterion 3: Operational Efficiency**
  Requirement: Staff is able to perform assigned tasks productively, quickly, and to a high quality standard.

- **Criterion 4: Growth Potential**
  Requirements: Product quality strengthens brand, reinforces customer loyalty, and enhances growth potential.

- **Criterion 5: Human Capital**
  Requirement: Company culture is characterized by a strong commitment to product quality and customer impact, which in turn enhances employee morale and retention.
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 select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

<table>
<thead>
<tr>
<th>STEP</th>
<th>OBJECTIVE</th>
<th>KEY ACTIVITIES</th>
<th>OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Monitor, target, and screen</td>
<td>Identify Award recipient candidates from around the globe</td>
<td>Pipeline of candidates who potentially meet all best-practice criteria</td>
</tr>
<tr>
<td>2</td>
<td>Perform 360-degree research</td>
<td>Perform comprehensive, 360-degree research on all candidates in the pipeline</td>
<td>Matrix positioning of all candidates’ performance relative to one another</td>
</tr>
<tr>
<td>3</td>
<td>Invite thought leadership in best practices</td>
<td>Perform in-depth examination of all candidates</td>
<td>Detailed profiles of all ranked candidates</td>
</tr>
<tr>
<td>4</td>
<td>Initiate research director review</td>
<td>Conduct an unbiased evaluation of all candidate profiles</td>
<td>Final prioritization of all eligible candidates and companion best-practice positioning paper</td>
</tr>
<tr>
<td>5</td>
<td>Assemble panel of industry experts</td>
<td>Present findings to an expert panel of industry thought leaders</td>
<td>Refined list of prioritized Award candidates</td>
</tr>
<tr>
<td>6</td>
<td>Conduct global industry review</td>
<td>Build consensus on Award candidates’ eligibility</td>
<td>Final list of eligible Award candidates, representing success stories worldwide</td>
</tr>
<tr>
<td>7</td>
<td>Perform quality check</td>
<td>Develop official Award consideration materials</td>
<td>High-quality, accurate, and creative presentation of nominees’ successes</td>
</tr>
<tr>
<td>8</td>
<td>Reconnect with panel of industry experts</td>
<td>Finalize the selection of the best-practice Award recipient</td>
<td>Decision on which company performs best against all best-practice criteria</td>
</tr>
<tr>
<td>9</td>
<td>Communicate recognition</td>
<td>Inform Award recipient of Award recognition</td>
<td>Announcement of Award and plan for how recipient can use the Award to enhance the brand</td>
</tr>
<tr>
<td>10</td>
<td>Take strategic action</td>
<td>Upon licensing, company is able to share Award news with stakeholders and customers</td>
<td>Widespread awareness of recipient’s Award status among investors, media personnel, and employees</td>
</tr>
</tbody>
</table>
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.

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.

http://www.frost.com