2016 North American Embedded Security for IIoT Customer Value Leadership Award
Contents

Background and Company Performance ................................................................. 3

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

   Customer Impact and Business Impact .......................................................... 3

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

Significance of Customer Value Leadership ....................................................... 8

Understanding Customer Value Leadership ....................................................... 8

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

Best Practice Award Analysis for Symantec Corporation ................................... 9

   Decision Support Scorecard ......................................................................... 9

   Customer Impact ......................................................................................... 10

   Business Impact ......................................................................................... 10

   Decision Support Matrix ............................................................................ 11

The Intersection between 360-Degree Research and Best Practices Awards ........ 12

   Research Methodology .............................................................................. 12


About Frost & Sullivan ...................................................................................... 14
Background and Company Performance

*Industry Challenges*

The control system environment is evolving into a complex and integrated sphere with a significant mix of architectures, legacy, and hybrid systems, as well as devices, requiring higher levels of visibility and understanding of the control system environment. As the Industrial Internet of Things (IIoT) takes precedence across diverse manufacturing environments, technologies such as bring your own devices (BYODs), mobile, and on-the-go operations, as well as cloud operations, make operations more flexible and productive. However, as threats continue to become more targeted, the associated costs and burden of complying with these norms becomes a focus point for all value chain participants, including customers, system integrators, and the original equipment manufacturers (OEMs). Solution providers that combine these capabilities into a unified solution offering will leverage both internal and external value.

*Customer Impact and Business Impact*

*Price/Performance Value*

The critical infrastructure industry has primarily been focused on continuous process operation and is currently witnessing a global transformation in terms of digitization and its perception towards cybersecurity. Today’s manufacturing floor comprises a gamut of industrial control systems (ICS) that include both legacies and greenfield solutions, each with its own protocols and operational criteria. As the IIoT ecosystem takes precedence, the associated consequences move beyond downtime and irreparable damage to safety and costs.

Symantec’s customer-centric approach to operational technology (OT) security has been established by constantly meeting and understanding customers’ key requirements. Through these interactions, the company has managed to design and develop solutions that focus on the OT security with value derived from its experience and expertise in IT security. Its solution offering not only caters to the new IIoT technologies, but also provides effective protection for existing legacy systems. Its IIoT solution suite comprises of the following key components:

**Embedded Critical System Protection:** This solution comprises of a host firewall, configuration control, file integrity monitoring, intrusion detection, operating system hardening, application whitelisting, and automatic sandboxing; thereby, enabling granular-level control and protection to zero day attacks. Additionally, the embedded solution can identify intruder activity, policy violations, and changes to files in real time.

**Device Certificates:** Device certificates provide identity and authentication of hardware devices to prevent unauthorized access. The solution is based on Public Key Infrastructure (PKI) which enables it to protect distributed hardware devices.
Code Signing: Code signing enables users to validate that the code running on the device has been authorized by them and not replaced by an attacker or an unauthorized third party.

Symantec’s security philosophy for the IIoT ecosystem is to build in security by following a “Secure by Design” approach, enabling it to protect the devices, communication systems, and manage and control its security systems.

Best Practices Example: Symantec is able to detect more threats with its cross-control point visibility and remediation capabilities when compared to its peers.

Operational Efficiency

Manufacturing units are moving to smarter operation modules, creating an increase in the number of intelligent endpoints that act as portals for vulnerabilities. In this complex and intricate control systems environment, device protection and protection management solutions are required to aid in effective implementation and continuous availability of systems.

Symantec’s Threat Protection solution seamlessly secures the customer endpoints, proactively blocking out threats across the various endpoints and prioritizing the incidents; therefore, equipping customers with a centralized and unified incident management tool. It also contains a forensics and remediation capability that helps customers manage their logs and provide remediation policies. Furthermore, the Threat Protection solution allows customers to extend security to both on premise and in the cloud and virtualized environments. For example, Symantec’s Mobility suite offers customers the option to manage devices and apps, secure data, and implement threat protection across a broad range of devices. This capability to provide a unified managed protection for mobility enables customers to protect their systems from vulnerabilities brought in through BYOD requirements.

Symantec’s go-to market strategy focuses on understanding the industry’s individual ecosystem and its sales and engineering cycles, and delivering solutions that are tailored to match the industry’s specific security requirements. Symantec’s IIoT strategy moves beyond protecting the device and communication systems to being able to detect anomalies and embed security into the customer’s devices. From a vertical market standpoint, Symantec has released its in-vehicle analytics based anomaly detection solution for the automotive space that can baseline the car and detect any anomalies based on patterns. Going forward, Symantec is looking to extend its anomaly detection solution to other verticals as well.
**Best Practices Example:** In 2015, Symantec’s intrusion prevention solution across different endpoints was able to block more than 700 million attempts by malware to conduct command and control (C&C) activity or carry out other malicious activity on users’ computers.

**Customer Service Experience**

As critical industries begin to take notice of the detrimental effects of cyberattacks, it becomes imperative to enhance existing security measures by deploying security readiness assessments and ensuring the companies are well equipped to not only protect their assets and resources, but also effectively detect and respond to breaches.

Symantec’s cybersecurity services extend from security monitoring to incident response and simulation and threat intelligence. DeepSight™ Intelligence is Symantec’s threat intelligence platform that collects, verifies, and analyzes the data to ensure accurate and timely information is provided to customers. Its monitoring services are built on an extensive collation of threat intelligence that uses network sensors to gather information from about 150 countries and external sites such as blogs and security agencies. This provides customers with timely insights of current vulnerabilities and threat trends, helping them to be better informed and prepared. Symantec’s simulation service helps with training customers to better understand the threats they are facing and the appropriate mitigation steps that can be pursued. The simulation tools are designed on an interactive virtual platform that caters to all types of users and provides them with real-life situations so the user is better informed of how a cyberattack can happen. The simulation tool continuously monitors and tracks the user’s progress through the attack scenarios, enabling it to collaboratively develop skills and identify talent gaps. Symantec’s services are developed by working closely with its customers to develop security solutions that are best suited to their requirements; thus, helping them to be better informed, prepared, and responsive to the threats.

**Best Practices Example:** Symantec’s DeepSight™ Intelligence services provide comprehensive vulnerability coverage for more than 19,000 vendors across 60,000 technologies.

**Customer Acquisition**

End users are sometimes apprehensive to patch the software of their ICSs because critical infrastructure environments operate 24/7. Furthermore, as they are unaware of the vulnerability of attacks, a significant time lag exists between threat identification and rectification. It is imperative for solution providers to empower the end user with proactive security control and management capabilities.

To deliver incremental value for customers, Symantec has partnered with Rockwell Automation to deliver endpoint security. Symantec’s Embedded Security: Critical Systems
Protection (SES:CSP) provides host-based intrusion prevention and detection and controls application behavior by whitelisting or sandboxing them. It allows policy-based behavior detection and control for hosts/devices, making it useful for the ICS ecosystem where signatures and patches are not always updated. The solution also includes configuration monitoring; host firewall; file integrity monitoring; and File, System, and Admin Lockdown to help identify any changes and policy violations in the system. Additionally, the SES:CSP does not require regular updates and can run independently (without the requirement of the management console) as required by the customer. The SES:CSP solution has been tested and verified with Rockwell’s Factory Talk and PlantPAX products.

**Best Practices Example:** The Rockwell partnership is helping Symantec gain more market penetration in the industrial automation space, including industries such as automotive, oil and gas, and power.

**Brand Equity**

While there are a number of solution providers entering the network security management space, to build a business case for adoption among end users, solution providers are required to understand customers’ desired outcomes and exhibit unique product attributes that cater to their immediate needs.

Symantec has a dedicated team that focuses on developing security solutions that are designed horizontally, but can be applied vertically. For example, authenticating devices solves issues across different industries, such as automotive, ICS, and healthcare, to name a few. Its breadth of solutions and constant collaboration with customers, as well as industry peers, helps the company focus on understanding the customers’ security requirements and developing appropriate solutions. Case in point; Symantec is a part of the Cyber Threat Alliance, a coordinated industry initiative that shares threat intelligence. Its cybersecurity knowledge and experience will aid in delivering its vision of being able to provide chief information security officers (CISO) with a single view of the overall company’s security posture that includes both the IT and the OT security aspects.

**Best Practices Example:** Symantec provides the industry with one of the largest, unclassified, non-government security intelligence networks. It monitors, analyzes, and processes over 10 trillion security events in a year.

**Growth Potential**

The pressing security requirements in critical infrastructure industries have resulted in a number of niche solution providers developing innovative products to ensure secure communication within the enterprise. For new entrants in this space, it is imperative to leverage foundation capabilities to create a solution offering that is repeatable across a gamut of applications.
Understanding the increasing presence of industries adopting and developing the IoT ecosystem, Symantec has developed a specific solution suite that can cater to the growing and dynamic requirements of its customers. Leveraging its experience and expert teams, Symantec is able to protect applications and devices, authenticate systems, provide visibility into existing and future security concerns, and manage the overall security posture of the company. In addition to the company’s existing capabilities, such as device security, certificate for authentication, and code protection, Symantec is developing OT security analytics capabilities that can proactively aid in identifying abnormal behavior and attacks in the network which they are testing with partners. In addition, as part of its overall Enterprise security portfolio it is developing a number of unified security applications. A couple of examples are:

**SymGauge:** measures various security parameters and benchmarks them.

**Targeted Attack Detection:** detects the source and associated information about new attacks.

**Best Practices Example:** There are approximately 1.3 billion IoT devices that currently embed Symantec Device Certificates for authentication purposes.

**Conclusion**

As manufacturers within critical industries move towards a smarter and digital era of interconnectivity and integration, an increasing number of threat vectors and vulnerabilities become inevitable. Symantec’s customer-centric approach and partnerships with manufacturers from various industries, such as automotive, ICS, and semiconductors, has enabled it to embed security into its devices, provide authentication solutions, and develop analytic capabilities. With its strong overall performance, Symantec has earned Frost & Sullivan’s 2016 Customer Value Leadership Award.
Significance of Customer Value Leadership

Ultimately, growth in any organization depends upon customers purchasing from your company, and then making the decision to return time and again. Delighting customers is therefore the cornerstone of any successful growth strategy. To achieve these dual goals (growth and customer delight), an organization must be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Customer Value Leadership

Customer Value Leadership is defined and measured by two macro-level categories: customer impact and business impact. These two sides work together to make customers feel valued, and confident in their products’ quality and long shelf life. This dual satisfaction translates into repeat purchases and a high lifetime customer value.
Key Benchmarking Criteria

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

Customer Impact
- Criterion 1: Price/Performance Value
- Criterion 2: Customer Purchase Experience
- Criterion 3: Customer Ownership Experience
- Criterion 4: Customer Service Experience
- Criterion 5: Brand Equity

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

Best Practice Award Analysis for Symantec

Decision Support Scorecard

To support its evaluation of best practices across multiple business performance categories, Frost & Sullivan employs a customized Decision Support Scorecard. This tool allows our research and consulting teams to objectively analyze performance, according to the key benchmarking criteria listed in the previous section, and to assign ratings on that basis. The tool follows a 10-point scale that allows for nuances in performance evaluation; ratings guidelines are illustrated below.

RATINGS GUIDELINES

The Decision Support Scorecard is organized by Customer Impact and Business Impact (i.e., the overarching categories for all 10 benchmarking criteria; the definitions for each criteria are provided beneath the scorecard). The research team confirms the veracity of this weighted scorecard through sensitivity analysis, which confirms that small changes to
the ratings for a specific criterion do not lead to a significant change in the overall relative rankings of the companies.

The results of this analysis are shown below. To remain unbiased and to protect the interests of all organizations reviewed, we have chosen to refer to the other key players as Competitor 2 and Competitor 3.

### DECISION SUPPORT SCORECARD FOR CUSTOMER VALUE LEADERSHIP AWARD

<table>
<thead>
<tr>
<th>Measurement of 1–10 (1 = poor; 10 = excellent)</th>
<th>Customer Impact</th>
<th>Business Impact</th>
<th>Average Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Customer Value Leadership</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Competitor 2</td>
<td>7</td>
<td>7</td>
<td>7.0</td>
</tr>
<tr>
<td>Competitor 3</td>
<td>7</td>
<td>6</td>
<td>6.5</td>
</tr>
</tbody>
</table>

**Customer Impact**

**Criterion 1: Price/Performance Value**
Requirement: Products or services offer the best value for the price, compared to similar offerings in the market

**Criterion 2: Customer Purchase Experience**
Requirement: Customers feel like they are buying the most optimal solution that addresses both their unique needs and their unique constraints

**Criterion 3: Customer Ownership Experience**
Requirement: Customers are proud to own the company’s product or service, and have a positive experience throughout the life of the product or service

**Criterion 4: Customer Service Experience**
Requirement: Customer service is accessible, fast, stress-free, and of high quality

**Criterion 5: Brand Equity**
Requirement: Customers have a positive view of the brand and exhibit high brand loyalty

**Business Impact**

**Criterion 1: Financial Performance**
Requirement: Strong overall financial performance in terms of revenues, revenue growth, operating margin and other key financial metrics

**Criterion 2: Customer Acquisition**
Requirement: Customer facing processes support the efficient and consistent 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: Customer focus strengthens brand, reinforces customer loyalty and enhances growth potential

Criterion 5: Human Capital
Requirement: Company culture is characterized by a strong commitment to quality and customers, which in turn enhances employee morale and retention

Decision Support Matrix
Once all companies have been evaluated according to the Decision Support Scorecard, analysts can then position the candidates on the matrix shown below, enabling them to visualize which companies are truly breakthrough and which ones are not yet operating at best-in-class levels.

DECISION SUPPORT MATRIX FOR CUSTOMER VALUE LEADERSHIP AWARD

<table>
<thead>
<tr>
<th>Business Impact</th>
<th>Customer Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Symantec</td>
</tr>
<tr>
<td>Low</td>
<td>Competitor 2</td>
</tr>
<tr>
<td></td>
<td>Competitor 3</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Frost & Sullivan 2016
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.
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.

<table>
<thead>
<tr>
<th>STEP</th>
<th>OBJECTIVE</th>
<th>KEY ACTIVITIES</th>
<th>OUTPUT</th>
</tr>
</thead>
</table>
| 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 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  
- Select winner | 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 may 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 |
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 almost 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.