FROST & SULLIVAN

Honeywell

2018 Global Industrial Cybersecurity Solutions Customer Value Leadership Award

2018
BEST PRACTICES
AWARDS

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 Honeywell 9

Decision Support Scorecard *9*

Customer Impact *10*

Business Impact *10*

Decision Support Matrix *11*

Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices 12

The Intersection between 360-Degree Research and Best Practices Awards 13

Research Methodology *13*

About Frost & Sullivan 13

Background and Company Performance

Industry Challenges

Security is becoming one of the key areas to address in the industrial information technology (IT) and operational technology (OT) worlds as rapid advances in technological trends, such as digitalization and the Industrial Internet of Things (IIoT), continue. Today, almost all industrial companies are making efforts to gain faster returns on smaller investments. In line with this, they are looking to harness the power of Big Data to gain real-time, end-to-end visibility into the performance of their industrial processes and assets by connecting these assets. This has been scaling the IIoT ecosystem as more and more OTs, including supervisory control and data acquisition (SCADA) and industrial control systems (ICS) get connected and, in the process, make the ecosystem more complex to manage.

This is because an OT environment encompasses hundreds of thousands of field assets across several industrial sites, some of which may be located remotely. The fact that these field assets have been deployed by different vendors over the years further complicates the operations: different devices have different proprietary protocols—communications as well as software and hardware. As a result, data exchange and integration of security features is more difficult because of compatibility issues. Also, many industrial companies do not have an integrated policy in place that would protect their connected operations from cybersecurity risks. Although companies are embarking on their digital transformation journey, the majority have weak security practices that fail to scale security features with a growing ecosystem of connected industrial assets. In fact, they lack the confidence to embrace automation to remotely manage their assets and sites and secure their OT environment. Because OT infrastructure unifies with IT networks, the infrastructure is exposed to cybersecurity vulnerabilities that pose a severe threat to the reliability and availability of plants: the larger the OT infrastructure, the larger the attack surface. Companies, therefore, have a strategic imperative to secure their connected industrial operations from such threats. Nonetheless, the lack of adequate skill, paired with budgetary constraints, is making it difficult for security experts to shrink the attack surfaces and secure connected industrial operations.

In this context, with industrial companies connecting operations across multiple sites and field assets from multiple vendors on a global scale, a centralized, multi-site cybersecurity solution architected particularly for ICS environments is imperative to ensure the safety and integrity of OT infrastructure. Single-point tools, such as firewalls and anti-virus protection, are not enough to counter or prevent sophisticated malware attacks.

Customer Impact and Business Impact

Recognized for its pioneering innovations in the area of automation control, instrumentation, and services, Honeywell has been leveraging more than 50 years of in-depth know-how in

the industrial sector and over 15 years of experience in the industrial cybersecurity space to ensure industrial companies' smooth IIoT transformation with strengthened defense against cybersecurity threats and vulnerabilities.

Customer Ownership and Purchase Experience

According to a market survey conducted in North America by Frost & Sullivan's Manufacturing Leadership Council, more than 53% of participants agreed that in the next couple of years, cybersecurity is among the top 3 expertise needs as the industry further embraces the IIoT. Market surveys indicate that a considerable number of industrial companies have yet to incorporate cybersecurity solutions into their existing OT infrastructure as part of their digitalization strategy despite more instances of cybersecurity breaches on a global scale.

Honeywell's strategic move to acquire Nextnine Ltd. (Nextnine) in August 2017 positioned it to add Nextnine's flagship product, ICS Shield™, to its portfolio of industrial cybersecurity technologies. Combining ICS Shield with its set of multi-vendor industrial cybersecurity solutions resulted in Honeywell's launch of a top-down solution for security management of OT infrastructure in June 2018. Honeywell's enhancement of ICS Shield as an enterprise-wide solution to support a multi-vendor OT infrastructure and defend cybersecurity threats in numerous physical industrial sites has solidified its leadership in the industrial cybersecurity market. Honeywell equips industrial customers with the tools to bridge major gaps in cybersecurity and empowers industrial security experts to strike a balance between manufacturing and production priorities without ignoring cybersecurity measures.

Industrial customers can now enjoy peace of mind: Honeywell's solution ensures security of connected ICS operations encompassing numerous systems from several vendors across multiple sites without any interoperability or compatibility issues. To support multiple vendors, ICS Shield previously had to be installed either separately or multiple times just on one customer site, but Honeywell, leveraging its proven innovation excellence in this area, has modified the solution so that industrial customers can control remote field assets via a single security operations center for all industrial sites. Frost & Sullivan identified this as a critical market differentiator.

The fact that industrial customers do not have to waste time seeking different point solutions for industrial control systems sourced from different vendors simplifies a customers' buying experience. ICS Shield acts as a one-stop solution, functioning not just as an OT security operations management and monitoring tool but also to support compliance monitoring and reporting. Overall, this solution allows companies to assess their OT cyber security posture in a way that's much easier to understand and act on. With the right information, users can better protect themselves with the insight to drive immediate actions to reduce cyber vulnerabilities and threats.

In addition to having a subscription-based model for two of its software offerings, Risk Manager and Secure Media Exchange (SMX), Honeywell also has an outcome-based subscription contract model in place. The Assurance 360 Program covers security through CyberVantage™ Managed Security Services, and is driven by key performance indicators such as system uptime, which could be affected by cyber-attacks. Customers that purchase Honeywell's control system enjoy end-to-end automation service solutions in addition to cybersecurity services.

Improving Operational Efficiency with an End-to-End Industrial Cybersecurity Solution

Frost & Sullivan believes that Honeywell's holistic set of solutions for industrial cybersecurity, including security consulting services, managed security services, integrated security technology, and cybersecurity software, offers a superior value proposition to sourcing and managing multiple solutions. The integrated platform, including features to support response and recovery, situational awareness, endpoint protection, network security, architecture and design, and assessments and audits makes Honeywell a trusted partner by virtue of its unprecedented ability to meet all of its customers' industrial cybersecurity needs. It also reduces the need to hire or train additional security personnel to manually perform these functions, cutting overhead costs and securing multi-vendor access to ICS environments through a single entry point.

At the core of Honeywell's security solution is ICS Shield, the most widely installed OT cyber security management platform for securing connected ICS environments. It provides companies with the capability to discover, connect and protect assets across their operations environments. The ICS Shield cybersecurity software package includes secure remote access and secure file transfer, automated patch and antivirus updates, asset discovery, performance/health monitoring, vulnerability scanning, risk analysis and compliance reporting. Once ICS Shield discovers all components on the network, including software, hardware, and the different service configurations and codes, it facilitates enterprise-wide cybersecurity with secure access to field assets in remote locations from a single operations center while maintaining granularity. Customers can securely transfer files to devices on the network and sensitive data from plant facilities to headquarters without risk. It plays a critical role in compliance management by automating the security policy management process across the entire plant facility. This empowers control and operations teams to clearly understand their responsibilities and function without encroaching on the other's domain. According to the company, customers can get access to 24/7 proactive alerting for all monitored devices.

Customer Service Experience

Honeywell has enhanced its OT tailored cyber security software offerings with a variety of related services to provide a better customer experience. CyberVantage Security Consulting

Services, which offers access to skilled industrial cyber security experts, can help protect ICS environments against the latest cyber threats. Delivered by experts in both operational technology (OT) and information technology (IT), over 30 types of strategic and tactical cyber services are offered such as site assessments, penetration testing, compliance audits, system architecture design, wireless security, system hardening, network security and endpoint protection, network refreshment, application whitelisting and much more. Customers can leverage Honeywell's OT cyber expertise and testing facilities at one of its global Cyber Centers of Excellence to safely simulate, validate and protect their cross-vendor control environments.

In its bid to strengthen the security of industrial customers' OT infrastructure against sophisticated cyber-attacks, Honeywell has significantly enhanced its ICS managed service capabilities by introducing CyberVantage Managed Security Services in June 2018. The combination of new features, such as new threat detection and vulnerability identification lowers operational risks in ICS environments. These services provide 24x7 expertise to reduce operational downtime and lower cyber risk and include remote security services for: around the clock expertise to manage security tools, continuous monitoring and alerting, automated security updates, remote troubleshooting and support.

Growth Potential

Honeywell's investment of millions of dollars towards advanced cyber labs demonstrates its commitment to assisting industrial companies in their IIoT transformation by staying ahead of cyber threats and attacks. Following the success of their initial Industrial Cyber Security Center of Excellence (COE) launch in Atlanta, Honeywell established a second in Dubai in February 2018, the first of its kind in the Middle East, and another in Singapore in April 2018, positioning it to better assist customers as the demand for solutions rises in these regions. Comprising distributed control systems, cutting-edge industrial cybersecurity technologies and solutions, physical plant processes and third-party systems and equipment, the centers allow security experts to build and execute cyber-attacks against simulated ICS environments based on real-world customer environments.

Aware of the difficulties that commercial off-the-shelf products pose in terms of customization and programming when linked to industrial control, Honeywell encourages vendors to research and advance the capabilities of their solutions using the latest equipment in its labs. Dynamic ICS environments and technological trends require ICS cybersecurity consultants and experts to continuously update their knowledge base and skill sets so they can effectively implement the best solutions.

Honeywell ensures that its cybersecurity experts are aware of evolving security threats and provides hands-on training in its labs. The company is committed to ISA99 and IEC-62443 standards for industrial control system security, working closely with agencies such as the US Department of Homeland Security to improve ICS security. They continuously learn about new defence and response methods to prevent or counter attacks against ICS and

critical infrastructure. Unlike most hardware vendors who provide training pertinent only to their own equipment and IT environments they cater to, Honeywell is taking a much broader approach. Similarly, none of Honeywell's peers have established world-class COEs on a global scale.

As companies continue to digitize their industrial operations and harness Big Data to make informed decisions and enhance productivity, Honeywell's complementary cybersecurity products and services, combined with their significant install base and deep industry expertise, has positioned them very well for leading the next era of IIoT transformation.

Conclusion

Honeywell guides industrial customers along their IIoT transformation journey by enabling them to stay ahead of cybersecurity threats and attacks. The company's proven excellence in this area drove it to acquire leading industrial cybersecurity solutions provider Nextnine to gain access to ICS Shield™, its flagship industrial cybersecurity software solution which now has over 6000 installations world-wide. Honeywell has since enhanced ICS Shield features to make it more suitable for enterprise-wide deployment as a top-down solution for OT infrastructure security management. Launched in June 2018, this solution supports multi-vendor assets across distributed sites through a single security center for enterprise-wide visibility to OT cyber security. Industrial customers also enjoy a superior value proposition with reduced total cost of ownership, automated patching, remote field asset control, risk analysis, policy compliance and much more. Honeywell's recently launched CyberVantage Managed Security Services and Security Consulting Services empower industrial customers to manage cyberattacks and enjoy a more productive IIoT transformation.

With its strong overall performance, Honeywell has earned Frost & Sullivan's 2018 Customer Value Leadership Award.

Significance of Customer Value Leadership

Ultimately, growth in any organization depends upon customers purchasing from a 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 of 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

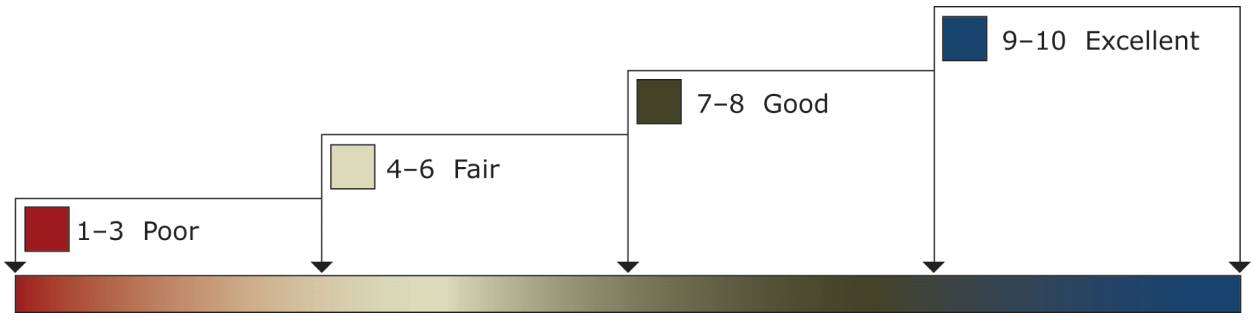
Criterion 1: Financial Performance
Criterion 2: Customer Acquisition
Criterion 3: Operational Efficiency
Criterion 4: Growth Potential
Criterion 5: Human Capital

Best Practices Award Analysis for Honeywell

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., these are the overarching categories for all 10 benchmarking criteria; the definitions for each criterion 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 participants as Competitor 2 and Competitor 3.

Measurement of 1–10 (1 = poor; 10 = excellent)			
Customer Value Leadership	Customer Impact	Business Impact	**Average Rating**
Honeywell	**8.9**	**8.8**	**8.9**
Competitor 2	8.3	8.5	8.4
Competitor 3	8.3	8.0	8.2

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 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: Overall financial performance is strong 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

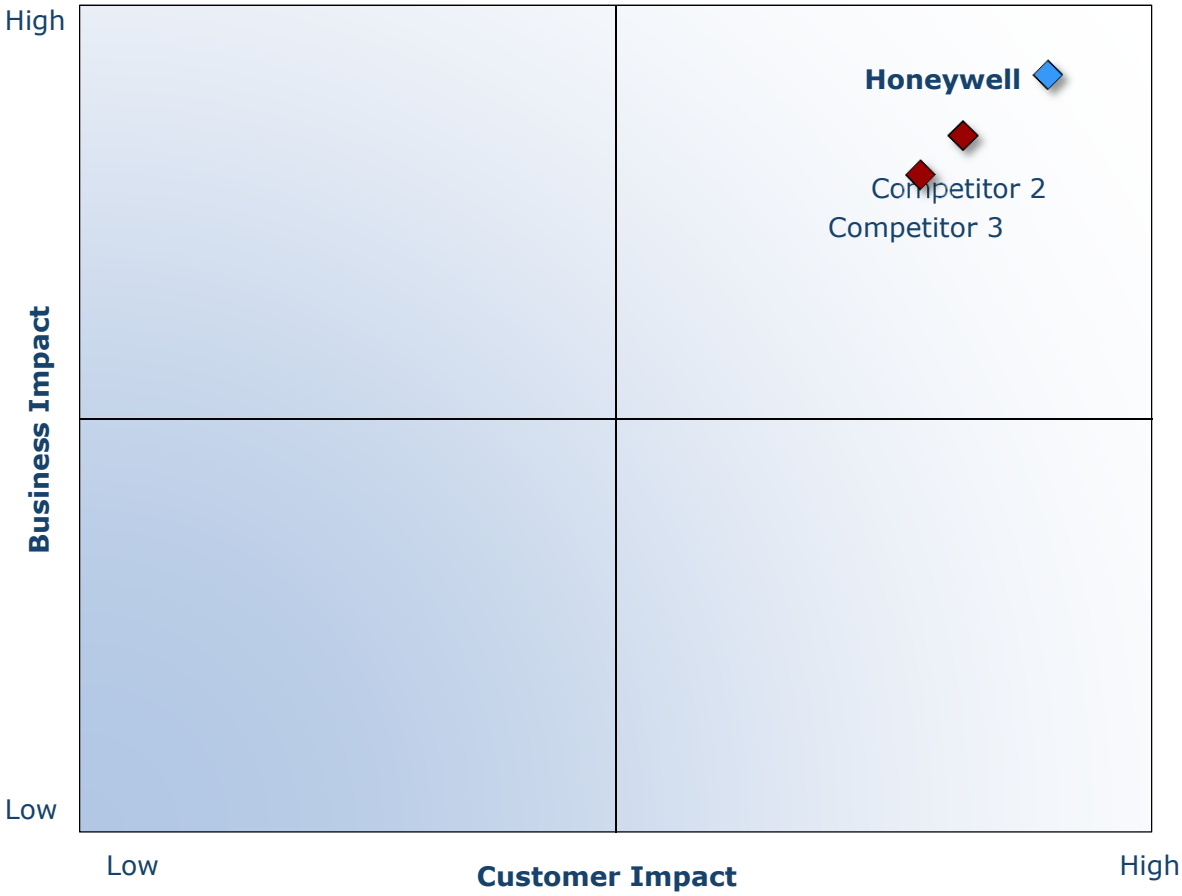
Requirements: Customer focus strengthens brand, reinforces customer loyalty, and enhances growth potential.

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 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.



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.

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

	STEP	OBJECTIVE	KEY ACTIVITIES	OUTPUT
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 participants 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.