2019 GLOBAL EMAIL SECURITY
ENABLING TECHNOLOGY LEADERSHIP AWARD

CISCO
Contents

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

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

Technology Leverage and Customer Impact ....................................................... 4

Conclusion ........................................................................................................ 8

Significance of Enabling Technology Leadership ............................................... 9

Understanding Enabling Technology Leadership ............................................. 9

Key Benchmarking Criteria ............................................................................... 10

Best Practices Award Analysis for Cisco ......................................................... 10

Decision Support Scorecard ............................................................................. 10

Technology Leverage ....................................................................................... 11

Customer Impact ............................................................................................ 11

Decision Support Matrix .................................................................................. 12


The Intersection between 360-Degree Research and Best Practices Awards .......... 14

Research Methodology ..................................................................................... 14

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

Industry Challenges

Email is still the number one threat vector. It is the most used mode of corporate communication and remains the de facto standard for B2B and B2C communications. Email-based threats have become big business targeting specific verticals as well as individuals. The need for secure email has never been stronger.

In the last few years the complexity and volume of threats have increased significantly. In particular, there has been an increase in sophisticated and highly targeted email-borne attacks. Many attacks use social engineering techniques. For businesses of all sizes, this is a serious problem as the legitimate communication channel they rely on extensively, email, is also the channel-of-choice for delivering malware.

The constantly evolving threat landscape requires continuous investment and innovation. Attackers are focusing more on people and less on systems. As evidence, there has been an increase in ransomware, Business Email Compromise (BEC), which includes spoofing, spear phishing, and other zero-day malware phishing attacks. Consequently with this evolution, traditional security solutions designed to protect systems and infrastructure are insufficient.

In the last year hackers have innovated in impersonation, including external customers and brand names with phony URLs and email header domains. One technique for impersonation is attackers glean information from social media sites to identify individuals within an organization in order to target them. Bad actors are using multi-prong attack methods. Large transactional attacks combine techniques such as email and phone calls. Many phishing scams enter an organization via email with attachments and/or links to websites that host malware or are fake sites used to gather users’ credentials (i.e., for use in account takeover exploits).

Internal emails can spread spam and malware. Consequently, mitigating email-borne threats that could and do come through corporate email systems is an escalating challenge. For these reasons, enterprises must take very seriously the effectiveness of email security solutions.

The most significant trend in the email security market is the acceleration of organizations migrating to the cloud. More IT organizations are moving their security to the cloud, including email security. Customers are adopting cloud mailbox services and migrating their email security to the cloud. This adds new levels of complexity to security. Microsoft Office 365 is the dominant cloud email product.

Office 365 solves a small piece of the email security problem with its own native security features. Those features may be adequate for organizations seeking general protections. But risk and risk tolerance varies by organization. Some will require more robust capabilities. Migration to cloud-based services, like Office 365, places the service outside of an organization’s security perimeter and opens it up to more frequent and easier cyber-
attacks. Email security vendors need to develop functions and features that augment Office 365 and other cloud email services. This includes delivering email security as a cloud Software-as-a-Service (SaaS) solution. Email security vendors also need to transition from on-premises solutions to cloud based solutions. The cloud is driving new email security strategies. A cloud SaaS solution for email security requires the vendor to offer scalability and threat intelligence.

The email security market is saturated and mature. Security vendors are forced to compete not only among each other, but also email service providers like Office 365 and G Suite with their own built-in security capabilities. Organizations are looking for integrated solutions that enable them to consolidate vendors and increase operational efficiencies while gaining stronger, comprehensive security. In such a competitive environment email security vendors need to differentiate.

Email security is more effective in an environment where security layers share data between each other. Product complexity is increasing as communication tracking and forensics become required and commonplace. Common platforms reduce security services administrative overhead. Email security is converging with other security solutions such as UTM, DLP, NGFW, SIEM, and CASB. Organizations seek to increase operational efficiencies while gaining stronger, comprehensive security.

Threats will continue evolving and becoming more blended, employing a multi-prong strategy. This necessitates more cross-product integration to successfully protect against increasingly sophisticated threats. Email vendors also need to build out global intelligence networks which feed analytical tools. Advanced analytics provides real-time and adaptive threat detection and response, and customized attack profiling. Integrating threat intelligence with other security solutions improves visibility and control.

**Technology Leverage and Customer Impact**

Cisco is the leader in networking equipment and services, and the largest enterprise and security vendor by revenue. Security products include firewall, intrusion prevention, remote access, virtual private networks, unified clients, cloud security, CASB, network access control (NAC), web gateways and email gateways, advanced threat solutions, endpoint security and endpoint management. The Advanced Malware Protection (AMP) Everywhere integrated security architecture solution is the glue across all of Cisco’s portfolio. Cisco Talos threat intelligence organization services most of Cisco security products, with pxGrid as the standard API.

Cisco Email Security defends against phishing, business email compromise, and ransomware. The company offers on-premises, hybrid and cloud solutions. Cisco Cloud Email Security can also be wrapped around other cloud service offerings, like Office 365, to enhance protection and controls of cloud-based email services.

Cisco is responding to the accelerating cloud migration. The company has been building out data centers globally, especially in EMEA and APAC, for scalability and to meet local
data privacy regulations.

Cisco has a comprehensive roadmap for email security which is based on a well-thought out integration strategy. This strategy includes integrating email innovations with organically developed technologies and those from acquisitions. The strategy is also focused on stronger partnerships and customer engagement.

![Percentage of Revenue Email Security Market: Global 2018](image)

Source: Frost & Sullivan

Cisco is making the transition from on-premises to cloud solutions. While email security sales dipped in 2017 due to this transition, in 2018 Cisco saw triple digit growth for its Cloud Email Security solution. The innovations and aggressive roadmap Cisco has laid out resulted in renewed growth and market share gain in email security in 2018. Cisco has established a strong position in a crowded email security market which has over 30 competitors. The momentum Cisco has demonstrated in 2018 bodes well for continued growth. Cisco is on the verge of double digit market share in email security.

**Commitment to Innovation**

Cisco has been striving to further integrate email security with its product lines and technologies, such as Talos, AMP, Umbrella, and SWG service, for up-to-date information on Indicators of Compromise (IoC). These technologies provide vital information for email security. Currently Cisco has email security integrations for Web Reputation &
Categorization, URL Re-writes, AMP Reputation, ThreatGrid File Analysis, AMP for Endpoints and Cisco Threat Response (CRT).

CRT has feeds from Talos and inputs of IoC from other products. Cisco Umbrella is a cloud security platform that provides customers with the first line of defense against internet-based threats, protecting their users when they connect using any device, in any place, at any time. Stealthwatch is a single, agentless solution that provides visibility across the extended network, including endpoints, branch, data center, and cloud. Umbrella essentially provides “north-south” protection while Stealthwatch provides “east-west” protection.

At least twice a year Cisco holds internal hackathons among different engineering teams. The company has been able to productize these ideas which integrate different product groups. This is considered an internal version of “Shark Tank”. The API for CTR went through this process.

There are further integrations on Cisco’s roadmap.

**Stage Gate Efficiency**

Cisco has a broad roadmap for email security. The various integrations with other products and technologies are in well-thought phases. The company has been hitting its targets.

Several new features and enhancements will be rolling out on a quarterly basis over the course of the company’s fiscal year 2020. Cisco has an integration strategy for many different technologies. A first phase has been the integration with AMP. A second phase is to integrate with Cisco threat response, through API two-way exchange between email and other products such as SWG and AMP.

**Commercialization Success**

Cisco has a long history of bringing new technologies to market. These are from both organic sources (internal development) and inorganic (via acquisition).

- In June 2013 Cisco unveiled pxGrid, a new framework for sharing context-aware information with a variety of third-party security providers.
- In 2013 Cisco acquired SourceFire. In a matter of a few months the technology was integrated into AMP for advanced malware protection, including file reputation function.
- In August 2015 Cisco acquired OpenDNS for its technology that provides advanced threat protection for any device, anywhere, anytime. With this acquisition Cisco
announced the first technology integration of Cisco AMP Threat Grid with OpenDNS services.

- In December 2015 Cisco acquired Lancope for its Stealthwatch system. Cisco had a longtime relationship with Lancope so Stealthwatch integrated quite well with a variety of existing Cisco solutions. By early 2016 Cisco had Stealthwatch in the market.

- In July 2017 Cisco acquired Observable Networks for technology based on dynamic behavioral modeling of all devices on the network. This was quickly integrated into Umbrella, Meraki, ISE, and Stealthwatch

- Cisco Threat Response is an internal development, launched in 4Q 2018. All Cisco customers have complimentary access.

- In August 2018 Cisco acquired Duo Security unified access security and multi-factor authentication delivered through the cloud. The company is in the process of integrating this technology with email security after integrating it with other Cisco solutions.

Cisco also has an extensive partner and OEM integration program. This includes DMARC, phishing protection, data loss prevention, anti-virus and more.

**Application Diversity**

Cisco’s strategy is to provide complete end-to-end protection. Many of the technologies that email security has been integrated with or will be integrated are used across other security solutions such as NAC, SIEM, CASB, NGFW, Endpoint protection, web security, and others. These technologies include ISE (pxGrid), Stealthwatch, AMP, and Talos. Stealthwatch has plugins for ISE, cognitive threat analytics, PXGrid and more.

**Customer Ownership Experience**

Cisco makes its customers part of the development process. The company holds semi-annual CISO events around the world for feedback on Cisco deployment and also competitor products for industry requirements. Customer forums are geo-specific. Cisco has internal discussions with Cisco field engineers for customer feedback and sponsors forums with its business partners and Managed Security Service Providers. MSSPs are viewed as customers as they purchase and use Cisco products in the services they offer to their customers. By engaging customers during the development process, especially premier customers, Cisco builds customer loyalty.

**Customer Service Experience**

Cisco is focused on building relationships with its customers. In addition to seeking feedback from customers and engaging them in the development process, as noted previously, Cisco also conducts in-person meetings. The company keeps customers up to date on the roadmap. A large number of customers are involved in beta testing.
Conclusion

With its strong overall performance, Cisco has earned Frost & Sullivan’s 2019 Enabling Technology Leadership Award in Email Security. The is the result of long-term planning and development, innovation, and key acquisitions. Cisco has been leveraging its position in the communications and networking space to grow its security leadership, especially with enterprise and large enterprise customers. In the last year the company has made a fast transition to the cloud with its email security solution. In the face of a rapidly evolving threat landscape and increasingly sophisticated threats, Cisco is increasing the efficacy of its email solution by drawing on the capabilities of its company-wide technologies. Cisco has the broadest security product portfolio. By increasing integration among these solutions with email security, Cisco offers its customers improving protection by sharing data, knowledge and analytics. Cisco engages its key customers in the development process thereby gaining knowledge via feedback and building customer relationships and loyalty. Cisco’s email security is on a high growth path due to its integration strategy.
Significance of Enabling Technology Leadership

Ultimately, growth in any organization depends on customers purchasing from a company and then making the decision to return time and again. In a sense, then, everything is truly about the customer. Making customers happy is the cornerstone of any successful, long-term growth strategy. To achieve these goals through enabling technology leadership, an organization must be best in class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.

Understanding Enabling Technology Leadership

Product quality (driven by innovative technology) is the foundation of delivering customer value. When complemented by an equally rigorous focus on the customer, companies can begin to differentiate themselves from the competition. From awareness, to consideration, to purchase, to follow-up support, organizations that demonstrate best practices deliver a unique and enjoyable experience that gives customers confidence in the company, its products, and its integrity.
Key Benchmarking Criteria

For the Enabling Technology Leadership Award, Frost & Sullivan analysts independently evaluated Technology Leverage and Customer Impact according to the criteria identified below.

Technology Leverage
- Criterion 1: Commitment to Innovation
- Criterion 2: Commitment to Creativity
- Criterion 3: Stage Gate Efficiency
- Criterion 4: Commercialization Success
- Criterion 5: Application Diversity

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

Best Practices Award Analysis for Cisco

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 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 considers Technology Leverage and Customer Impact (i.e., 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, Frost & Sullivan has chosen to refer to the other key participants as Competitor 1 and Competitor 2.

<table>
<thead>
<tr>
<th>Measurement of 1–10 (1 = poor; 10 = excellent)</th>
<th>Technology Leverage</th>
<th>Customer Impact</th>
<th>Average Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabling Technology Leadership</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>Competitor 1</td>
<td>6</td>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>Competitor 2</td>
<td>8</td>
<td>6</td>
<td>7</td>
</tr>
</tbody>
</table>

**Technology Leverage**

**Criterion 1: Commitment to Innovation**

Requirement: Conscious, ongoing adoption of emerging technologies that enable new product development and enhance product performance.

**Criterion 2: Commitment to Creativity**

Requirement: Technology leveraged to push the limits of form and function in the pursuit of white space innovation.

**Criterion 3: Stage Gate Efficiency**

Requirement: Adoption of technology to enhance the stage gate process for launching new products and solutions.

**Criterion 4: Commercialization Success**

Requirement: A proven track record of taking new technologies to market with a high rate of success.

**Criterion 5: Application Diversity**

Requirement: The development and/or integration of technologies that serve multiple applications and can be embraced in multiple environments.

**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 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.

**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 practices 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 world | • Conduct in-depth industry research  
• Identify emerging industries  
• Scan multiple regions | Pipeline of candidates that potentially meet all best practices 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 practices 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 practices 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 practices 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 practices award recipient | • Review analysis with panel  
• Build consensus  
• Select recipient | Decision on which company performs best against all best practices criteria |
| 9 Communicate recognition | Inform award recipient of 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 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 the 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, resulting in 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, helps clients 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 practices models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages nearly 60 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on 6 continents. To join Frost & Sullivan’s Growth Partnership, visit http://www.frost.com.