Vendor Landscape: Email Security Gateway

The emails that you want are only the tip of the iceberg that you get.
Introduction

Email security is as important today as it ever was. Organizations must implement an Email Security Gateway (ESG) to protect their most widely used business tool: email.

This Research Is Designed For:

- Enterprises seeking to select a solution for ESG.
- The following ESG use cases:
  - Information Security Managers who have decided to select and deploy an ESG but are unfamiliar with the space.
  - Information Security Managers who have decided to upgrade or switch ESG vendors and require advisory research.
  - Organizations looking to optimize their email security.
  - Organizations looking to resolve email-based cyber attacks and data breaches.

This Research Will Help You:

- Understand what’s new in the ESG market.
- Evaluate ESG vendors and products for your enterprise needs.
- Determine which products are most appropriate for particular use cases and scenarios.
Executive summary

Info-Tech evaluated 12 competitors in the ESG market, including the following notable performers:

**Champions:**
- **Barracuda** offers one of the strongest targeted attack detection capabilities backed with a comprehensive features offering.
- **Cisco** is a commanding player within the ESG market, seen to be a strategic vendor for additional non-security product areas.
- **Symantec** is a strong mature competitor within the ESG marketplace and larger information security industry.

**Value Award:**
- **Barracuda** offers some of the most comprehensive threat detection capabilities while still maintaining competitive pricing, ensuring applicability to all sizes of organizations.

**Trend Setter Award:**
- **Clearswift** has developed innovative and extremely impressive detection capabilities. ImageLogic, its proprietary image detection, in addition to its proprietary redactive DLP capability, demonstrate Clearswift’s ability to provide the latest solutions.

---

**Info-Tech Insight**

1. **Get it out to the cloud**
   Cloud adoption among business functions is already high. Moving email to the cloud is just another step. Take this into consideration when selecting an ESG.

2. **The professional attack**
   They are advancing every day without fail. Advanced Persistent Threats (APTs) and Zero-Day attacks are changing the way organizations deal with threats. Recognize the need for greater visibility and tools that stay on top of these developments.
How to use this Vendor Landscape

There are multiple ways you can use this Info-Tech Vendor Landscape in your organization. Choose the option that best fits your needs:

**Do-It-Yourself**

Use this Vendor Landscape to help you complete your purchasing decision. The slides in this deck will walk you through our recommended evaluated vendors in this market space with supporting tools and deliverables ready for you to make your decision.

**Free Guided Implementation**

We recommend that you supplement the Vendor Landscape with a **Guided Implementation**.

At no additional cost to you*, our expert analysts will provide telephone assistance to you and your team at key milestones in the decision to review your materials, answer your questions, and explain our methodologies.

*Gold and Silver level subscribers only
Book a free guided implementation today!

Info-Tech is just a phone call away and can assist you with your project. Our expert Analysts can guide you to successful project completion. For most members, this service is available at no additional cost.*

Here’s how it works:

1. **Enroll in a Guided Implementation for your project**

   Send an email to GuidedImplementations@InfoTech.com
   
   Or call 1-888-670-8889 and ask for the Guided Implementation Coordinator.

2. **Book your analyst meetings**

   Once you are enrolled in a Guided Implementation, our analysts will reach out to book a series of milestone-related telephone meetings with you and your team.

3. **Get advice from a subject matter expert**

   At each Guided Implementation point, our Consulting Analyst will review your completed deliverables with you, answer any of your questions, and work with you to plan out your next phase.

*Gold and Silver level subscribers only
Guided Implementation points in the ESG Vendor Landscape

**Book a Guided Implementation Today:** Info-Tech is just a phone call away and can assist you with your evaluation. Our expert Analysts can guide you to successful technology selection.

*Here are the suggested Guided Implementation points for the ESG Vendor Landscape:*

<table>
<thead>
<tr>
<th><strong>Section 1:</strong> Shortlist Assistance and Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get off to a productive start: Discuss the market space and how vendors are evaluated. Decide on which deployment option suits you best and narrow down the options based on customized requirements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Section 2:</strong> RFP and Budget Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interpreting and acting on RFP results: Review vendor RFPs and ensure the solution is meeting your needs. Discuss average pricing of solutions and what can fit into your budget.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Section 3:</strong> Negotiation and Contract Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchase optimization: Review contracts and discuss best practices in negotiation tactics to get the best price for your solution.</td>
</tr>
</tbody>
</table>

To enroll, send an email to [GuidedImplementations@InfoTech.com](mailto:GuidedImplementations@InfoTech.com) or call 1-888-670-8889 and ask for the Guided Implementation Coordinator.
Market overview

**How it got here**

- Email Security Gateways developed steadily over the 2000s in reaction to the increase in spam and other unwanted emails, as well as new email-based threat developments.
- Development of authentication methods, machine learning, blacklisting, whitelisting, and content filtering moved from the frontier defenses of ESGs to necessary stakes.
- The number of market competitors decreased due to the need for large intelligence gathering capabilities to stay up to date on the latest threats and attack campaigns.
- Proliferation of botnets to create *zombie* attacks as well as to compromise whitelisted domains underscore the need for active content filtering and behavioral analysis.
- The recent development of spear phishing (targeted email attacks) has resurfaced the need for ESGs to protect against the most costly of user credential compromise or intellectual property theft.

**Where it’s going**

- The threat landscape is becoming more advanced, fast paced, and reactive with more persistent adversaries. Traditional mass attacks and general spam are still a huge concern and nuisance.
- The proliferation of spear phishing, either by criminal organizations, hacktivist groups, or state sponsored groups, is developing into a standard attack method with commodity style markets selling and reselling these techniques.
- Vendors are placing a focus on integrated security solutions so that incoming and outgoing traffic across internet, email, and other streams can be analyzed across mediums with multiple tools to detect unidentified attacks. This can include integration with DLP, SIEM, IDPS, firewalls, and other security solution products.
- There is a general development by cloud ESG providers to become more robust in their offerings to meet the general market push by organizations to move to the cloud with other functions.

As the market evolves, capabilities that were once cutting edge become default and new functionality becomes differentiating. Anti-phishing with anti-spear-phishing has become a Table Stakes capability and should no longer be used to differentiate solutions. Instead, focus on dynamic content and URL execution and redactive outbound filtering to get the best fit for your requirements.
Email security gateway vendor selection / knock-out criteria: market share, mind share, and platform coverage

- ESG solutions must maintain conventional email security against vast amounts of spam and malware, as well as being equipped to detect spear phishing attacks while enabling easy management and easy reporting.
- For this Vendor Landscape, Info-Tech focused on those vendors that offer broad capabilities across multiple platforms and that have a strong market presence and/or reputational presence among small and mid-sized enterprises.

**Included in this Vendor Landscape:**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barracuda</td>
<td>A well developed offering of security features but not advanced enough for large enterprises.</td>
</tr>
<tr>
<td>Cisco</td>
<td>A strategic vendor based on nonsecurity-related offerings.</td>
</tr>
<tr>
<td>Clearswift</td>
<td>Advanced offerings for the highest of security needs.</td>
</tr>
<tr>
<td>Fortinet</td>
<td>Extremely low price point and focused on a UTM deployment model.</td>
</tr>
<tr>
<td>Google</td>
<td>Complete cloud-based business offering but with compliance and privacy concerns.</td>
</tr>
<tr>
<td>McAfee</td>
<td>One of the most viable security vendors, but at a cost.</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Selected primarily based on nonsecurity-related offerings that are considered essential.</td>
</tr>
<tr>
<td>Proofpoint</td>
<td>A pure play vendor with a focus on advanced technical offerings for large enterprises.</td>
</tr>
<tr>
<td>Sophos</td>
<td>Extremely strong security offering and decent price point but with no hosted offering.</td>
</tr>
<tr>
<td>Symantec</td>
<td>Widely known vendor with wealth of threat intelligence but lack of integrated capabilities.</td>
</tr>
<tr>
<td>Trend Micro</td>
<td>A purely email-focused vendor with encryption problems.</td>
</tr>
<tr>
<td>Websense</td>
<td>Compliance and targeted attack strengths but with vendor focus on UTM.</td>
</tr>
</tbody>
</table>
Email security gateway criteria & weighting factors

<table>
<thead>
<tr>
<th>Product Evaluation Criteria</th>
<th>Vendor Evaluation Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Features</strong></td>
<td>Vendor is committed to the space and has a future product and portfolio roadmap.</td>
</tr>
<tr>
<td><strong>Usability</strong></td>
<td>Vendor offers global coverage and is able to sell and provide post-sales support.</td>
</tr>
<tr>
<td><strong>Affordability</strong></td>
<td>Vendor is profitable, knowledgeable, and will be around for the long term.</td>
</tr>
<tr>
<td><strong>Architecture</strong></td>
<td>Vendor channel strategy is appropriate and the channels themselves are strong.</td>
</tr>
</tbody>
</table>

Criteria Weighting

- **Features**: 10%
- **Usability**: 30%
- **Affordability**: 20%
- **Architecture**: 40%
- **Product Viability**: 50%
- **Vendor Strategy**: 50%
- **Vendor Reach**: 25%
- **Vendor Channel**: 30%
- **Vendor Viability**: 30%
- **Vendor Strategy**: 30%
- **Vendor Reach**: 30%
- **Vendor Channel**: 30%
The Info-Tech Email Security Gateway Vendor Landscape

**The zones of the Landscape**

**Champions** receive high scores for most evaluation criteria and offer excellent value. They have a strong market presence and are usually the trend setters for the industry.

**Market Pillars** are established players with very strong vendor credentials, but with more average product scores.

**Innovators** have demonstrated innovative product strengths that act as their competitive advantage in appealing to niche segments of the market.

**Emerging Players** are comparatively newer vendors who are starting to gain a foothold in the marketplace. They balance product and vendor attributes, though score lower relative to market Champions.

For an explanation of how the Info-Tech Vendor Landscape is created, see [Information Presentation – Vendor Landscape](#) in the Appendix.
Balance individual strengths to find the best fit for your enterprise

<table>
<thead>
<tr>
<th>Product</th>
<th>Overall</th>
<th>Features</th>
<th>Usability</th>
<th>Afford.</th>
<th>Arch.</th>
<th>Overall</th>
<th>Viability</th>
<th>Strategy</th>
<th>Reach</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barracuda</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Cisco</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Clearswift</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Fortinet</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Google</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>McAfee</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Legend: 〇 = Exemplary, 〇 = Good, 〇 = Adequate, 〇 = Inadequate, 〇 = Poor

For an explanation of how the Info-Tech Harvey Balls are calculated, see Information Presentation – Criteria Scores (Harvey Balls) in the Appendix.
Balance individual strengths to find the best fit for your enterprise (continued)

<table>
<thead>
<tr>
<th>Product</th>
<th>Overall</th>
<th>Features</th>
<th>Usability</th>
<th>Afford.</th>
<th>Arch.</th>
<th>Overall</th>
<th>Viability</th>
<th>Strategy</th>
<th>Reach</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Proofpoint</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Sophos</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Symantec</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Trend Micro</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Websense</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

*The vendor declined to provide pricing and publicly available pricing could not be found.*

For an explanation of how the Info-Tech Harvey Balls are calculated, see Information Presentation – Criteria Scores (Harvey Balls) in the Appendix.
The Info-Tech ESG Value Index

**What is a Value Score?**

The Value Score indexes each vendor’s product offering and business strength relative to its price point. It does not indicate vendor ranking.

Vendors that score high offer more bang-for-the-buck (e.g. features, usability, stability, etc.) than the average vendor, while the inverse is true for those that score lower.

Price-conscious enterprises may wish to give the Value Score more consideration than those who are more focused on specific vendor/product attributes.

*The vendor declined to provide pricing and publicly available pricing could not be found.*

For an explanation of how Price is determined, see Information Presentation – Price Evaluation in the Appendix.

For an explanation of how the Info-Tech Value Index is calculated, see Information Presentation – Value Index in the Appendix.
Table Stakes represent the minimum standard; without these, a product doesn’t even get reviewed.

### The Table Stakes

<table>
<thead>
<tr>
<th>Feature</th>
<th>What it is:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Spam/Bulk Email Detection</td>
<td>Basic inbound blocking using multitude of triggers: IP address, content, header, and other reputation-based identifiers.</td>
</tr>
<tr>
<td>Anti-Phishing/ Spear Phishing</td>
<td>Heuristic detection techniques that recognize common characteristics of phishing attacks.</td>
</tr>
</tbody>
</table>

### What does this mean?

The products assessed in this Vendor Landscape™ meet, at the very least, the requirements outlined as Table Stakes.

Many of the vendors go above and beyond the outlined Table Stakes, some even do so in multiple categories. This section aims to highlight the products’ capabilities in excess of the criteria listed here.

---

If Table Stakes are all you need from your ESG solution, the only true differentiator for the organization is price. Otherwise, dig deeper to find the best price to value for your needs.
Advanced features are the capabilities that allow for granular market differentiation

**Scoring Methodology**

Info-Tech scored each vendor’s features offering as a summation of its individual scores across the listed advanced features. Vendors were given one point for each feature the product inherently provided. Some categories were scored on a more granular scale with vendors receiving half points.

<table>
<thead>
<tr>
<th>Feature</th>
<th>What we looked for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Time URL &amp; Malware Detection</td>
<td>Live detection and following of URL embedded links and execution of active content.</td>
</tr>
<tr>
<td>End-User Spam Visibility &amp; Controls</td>
<td>End-user email digest release capability and client integration for fine tuning.</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>Outbound content filtering based on policy configuration with notification or redactive functions.</td>
</tr>
<tr>
<td>Anti-Malware Signature Detection</td>
<td>Comprehensive signature malware detection capabilities through threat intelligence sourcing.</td>
</tr>
<tr>
<td>Anti-Malware Behavioral Detection</td>
<td>Active code detection and execution.</td>
</tr>
<tr>
<td>Encryption / Decryption</td>
<td>Advanced capabilities to encode data and information with visibility and controls.</td>
</tr>
</tbody>
</table>

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.
## Scoring Methodology

Info-Tech scored each vendor’s features offering as a summation of its individual scores across the listed advanced features. Vendors were given one point for each feature the product inherently provided. Some categories were scored on a more granular scale with vendors receiving half points.

## Advanced Features (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>What we looked for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DKIM &amp; SPF Support</td>
<td>Domain Keys Identified Mail and Sender Policy Framework encryption support.</td>
</tr>
<tr>
<td>Hosted Email Support</td>
<td>Integration and support capabilities with third-party hosted email providers.</td>
</tr>
<tr>
<td>Email Retention/Archiving</td>
<td>Inbound and outbound logging capabilities.</td>
</tr>
<tr>
<td>Hosted &amp; Hybrid Deployment Solutions</td>
<td>The ability to deploy in combination between a hosted and on-premise solution.</td>
</tr>
</tbody>
</table>

For an explanation of how Advanced Features are determined, see [Information Presentation – Feature Ranks (Stoplights)](#) in the Appendix.
Each vendor offers a different feature set; concentrate on what your organization needs

<table>
<thead>
<tr>
<th>Evaluated Features</th>
<th>Spam/ Bulk</th>
<th>Spear/ Phishing</th>
<th>Real Time URL &amp; Malware</th>
<th>End-User Spam Control</th>
<th>Data Loss Protection</th>
<th>Encryption/ Decryption</th>
<th>Anti-Mal. Signature</th>
<th>Anti-Mal. Behavioral</th>
<th>DKIM &amp; SPF</th>
<th>Hosted Email Support</th>
<th>Email Archiving</th>
<th>Hosted &amp; Hybrid Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barracuda</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clearswift</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend: 
- = Feature fully present
○ = Feature partially present/pending
■ = Feature absent

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.
Each vendor offers a different feature set; concentrate on what your organization needs (continued)

<table>
<thead>
<tr>
<th>Evaluated Features</th>
<th>Microsoft</th>
<th>Proofpoint</th>
<th>Sophos</th>
<th>Symantec</th>
<th>Trend Micro</th>
<th>Websense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spammers/Spam &amp; Malware</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Real Time URL Control</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>End-User Spam Control</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Data Loss Protection</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Real Time URL &amp; Malware</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Encryption/Decryption</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Anti-Mal. Signature</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Anti-Mal. Behavioral</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>DKIM &amp; SPF</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Hosted Email Support</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Email Archiving</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Hosted &amp; Hybrid Solutions</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

**Legend**
- ✔️ = Feature fully present
- ○ = Feature partially present/pending
- ❌ = Feature absent

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.
# Shortlist Assistance & Requirements

Arrange a call now: email GuidedImplementations@InfoTech.com or call 1-888-670-8889 and ask for the Guided Implementation Coordinator.

<table>
<thead>
<tr>
<th>Prior to the Guided Implementation</th>
<th>During the Guided Implementation</th>
<th>Value &amp; Outcome</th>
</tr>
</thead>
</table>
| 1. Have reasoning as to why a new solution is being discussed. | An Info-Tech Consulting Analyst will discuss with you:  
- Reviewing the market and understanding the rationale behind the evaluation.  
- Deciding on a deployment method.  
- Feature analysis. | At the conclusion of the Guided Implementation call, you will have:  
- An understanding of the market situation.  
- A narrowed list of vendors with customized evaluation tool.  
- An RFP template to distribute to vendors. |
| 2. Compile list of gaps. | | |
Regulatory and compliance issues carry specific requirements for any ESG that are mandatory solutions.

Look for solutions that not only have excellent inbound detection, but also outbound filtering and necessary audit controls.

**Exemplary Performers**

1. **Regulated Industries**
   - **Symantec**: Two OEM relationships supporting content encryption in addition to PGP and TLS provide strong data protection. Leveraging its DLP experience from its standalone product as well as archiving functions make Symantec well suited for regulated industries.

2. **Why Scenarios?**
   - In reviewing the products included in each Vendor Landscape™, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

3. **Websense**: Native DLP from Websense’s standalone product with up to 1,700 predefined compliance templates, customizable encryption triggers support native TLS, Park-and-Pull encryption, and SaaS archiving make Websense suited for regulated industries.

4. **Proofpoint**: User-transparent, central policy driven DLP provides a sophisticated channel solution with highlighted policy violation capability and addition of comments to incidents. A push based encryption supports multiple options including TLS, S/MIME, and PGP.

For an explanation of how Scenarios are determined, see [Information Presentation – Scenarios](#) in the Appendix.
Consider ESG deployment options based on your email future direction

Email is headed to the cloud. Make sure your ESG is ready for your future email needs.

Why Scenarios?
In reviewing the products included in each Vendor Landscape™, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

For an explanation of how Scenarios are determined, see Information Presentation – Scenarios in the Appendix.
Targeted attacks are on the rise with the majority being carried out by spear phishing.

ESG solutions must be able to adapt and react to these highly advanced and unique attack campaigns.

### Exemplary Performers

1. **Barracuda**
   - Leverages its threat intelligence along with Barracuda Labs and Real Time Protection. Advanced intent analysis and virtual sandboxing capabilities ensure targeted attack protection.

2. **McAfee**
   - Threat Response Updates with TrustedSource global and McAfee global threat intelligence as real time updating prevents zero-hour threats. Time of click URL redirection protects from targeted attacks.

3. **Websense**
   - Advanced Classification Engine combines URL and file sandboxing, real-time code scanning, real-time content classification, email and web reputation, and heuristics with anti-virus engines.

4. **Proofpoint**
   - Leverages data analytics to combat targeted attacks in addition to predictive sandboxing and dynamic URL rewriting capabilities.

5. **TrendMicro**
   - Uses enhanced web reputation, document exploit detection, sandbox execution analysis, and custom threat intelligence to provide comprehensive targeted attack security.

---

**Why Scenarios?**

In reviewing the products included in each Vendor Landscape™, certain use cases come to the forefront. Whether those use cases are defined by applicability in certain locations, relevance for certain industries, or as strengths in delivering a specific capability, Info-Tech recognizes those use cases as Scenarios, and calls attention to them where they exist.

For an explanation of how Scenarios are determined, see [Information Presentation – Scenarios](#) in the Appendix.
RFP & Budget Review

Arrange a call now: email GuidedImplementations@InfoTech.com or call 1-888-670-8889 and ask for the Guided Implementation Coordinator.

<table>
<thead>
<tr>
<th>Prior to the Guided Implementation</th>
<th>During the Guided Implementation</th>
<th>Value &amp; Outcome</th>
</tr>
</thead>
</table>
| 1. Collect RFPs from vendors based on the template provided. | An Info-Tech Consulting Analyst will discuss with you:  
• Reviewing price benchmarking.  
• Reviewing returned RFPs. | At the conclusion of the Guided Implementation call, you will have:  
• A narrowed list of vendors.  
• Clear understanding of the capabilities of the solutions on the shortlist.  
• A demo script to use during presentations with the final list of vendors. |
Symantec provides a wealth of threat intelligence, providing real time detection of the latest threats

**Champion**

<table>
<thead>
<tr>
<th>Product:</th>
<th>Symantec Messaging Gateway (SMG)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees:</td>
<td>21,500</td>
</tr>
<tr>
<td>Headquarters:</td>
<td>Mountain View, CA, USA</td>
</tr>
<tr>
<td>Website:</td>
<td>symantec.com</td>
</tr>
<tr>
<td>Founded:</td>
<td>1982</td>
</tr>
<tr>
<td>Presence:</td>
<td>SYMC</td>
</tr>
</tbody>
</table>

**Overview**

- One of the largest ESG players, Symantec commands a heavy market share and is a leader in email security. Symantec’s email security offerings are mature with on-premise, virtual, or SaaS deployment options and no organizational size preference.

**Strengths**

- A partnership with ZixCorp and Echoworx provided the Symantec Content Encryption service for clients in addition to Symantec’s own PGP encryption offering.
- Symantec leverages its DLP from its standalone product to support a deep content inspection engine with predefined content.
- Identification of anomalies and targeted attacks is performed by Symantec technology including Real Time Link Following and Skeptic heuristics and is supported by Symantec’s extensive Global Intelligence Network.

**Challenges**

- A lack of centralized management with unified reporting and administration capabilities stifles customers’ ability to manage hybrid deployments where on-premise, appliance, and cloud service are used in tandem.
- The third-party supported encryption functions lack client visibility and control over self-configuration and history or encryption use across communications.

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000

Pricing provided by vendor
Symantec hits on all the features

One of the largest vendors within the ESG marketplace, Symantec offers high vendor stability with a wide array of other security product offerings. Any sized customer can benefit from Symantec’s experience within information security.
**Barracuda is a high value shortlist candidate for any mid-sized and data regulated business**

**Champion**

Product: Barracuda Spam and Virus Firewall
Employees: 1,100
Headquarters: Campbell, CA, USA
Website: barracuda.com
Founded: 2003
Presence: CUDA

**Overview**

- Barracuda is an established security provider of economical and easy to use network and SaaS solutions. A high growth vendor and excellent shortlist for organizations seeking best bang for the buck.

**Strengths**

- Barracuda is able to support and manage its web security solution and ESG from one singular control panel, Barracuda Control Center, with the same look and feel that is used across all of Barracuda’s products.
- Service is sold per box, instead of by the user, allowing for high cost savings when scaling compared to other vendors.
- Unique support offerings include fourth year free of charge hardware replacement.

**Challenges**

- DLP capabilities are limited by predefined dictionaries, with keyword and expression filtering, resulting in higher than normal false positives. As well, compliance officer workflow is limited.
- The user interface is in need of reformatting to introduce more intuitive capabilities and cleaner color schemes. An updated UI is expected in 2014.
- Encryption capabilities are limited for large enterprises due to a lack of push-based encryption options.

3 year TCO for this solution falls into pricing tier 5, between $25,000 and $50,000

Pricing provided by vendor

$1 $1M+
Barracuda has deployment options to suit any sized organization

<table>
<thead>
<tr>
<th>Vendor Landscape</th>
<th>Product</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overall</td>
<td>Features</td>
</tr>
<tr>
<td></td>
<td>🟠</td>
<td>🟠</td>
</tr>
</tbody>
</table>

Deployment Option:  
- **On-Premise Appliance Offerings**: Barracuda Spam and Virus Firewall Models: 100, 200, 300, 400, 600, 800, 900, 1000
- **Virtual Appliance Platforms Being Supported**: Barracuda Spam and Virus Firewall Vx Models: V100, V300, V400, V600
- **Hosted Deployment Options**: Barracuda Email Security Service

Value Index

<table>
<thead>
<tr>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st out of 12</td>
</tr>
</tbody>
</table>

Info-Tech Recommends:

Barracuda is an overall strong shortlist candidate for any mid to large-sized organization with varying security needs. A somewhat smaller threat intelligence than other vendors must be considered. A simple interface that needs a refresh speaks to non-technical users without advanced requirements.
Cisco provides strong targeted attack protection and DLP with focus on mid-sized to large enterprises

**Champion**

- **Product:** Cisco Email Security (Formerly Ironport)
- **Employees:** 75,000+
- **Headquarters:** San Jose, CA, USA
- **Website:** cisco.com
- **Founded:** Entered ESG in 2007
- **Presence:** CSCO

---

**Overview**

- Cisco commands sizable force for on-premise appliance solutions for mid-sized to large organizations. It rebranded its email security from Ironport to Cisco Email Security in 2012. Cisco is seen as a strategic vendor due to its main focus on several other areas.

**Strengths**

- DLP controls are offered with more than 100 predefined dictionaries with custom policy creation. Integration with RSA DLP enables content aware matching that requires multiple evidences in a document to force a high severity rating.
- Advanced malware protection, through Sourcefire, enables URL rewriting, sandboxing, and exemplar detection of new threats.
- Native policy-based encryption, Cisco Registered Envelope Service manages recipient registration, authentication, and per-message/per-recipient encryption keys.

**Challenges**

- Cisco has considerable focus on mid-sized to large enterprises resulting in a lack of small enterprise scalability and understanding. Often, strong technical understanding is required.
- A lack of archiving and retention capabilities limits certain functionalities that many organizations require.
Cisco carries the Ironport torch forward with new ESA offerings

Vendor Landscape

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Overall</th>
<th>Features</th>
<th>Usability</th>
<th>Afford.</th>
<th>Arch.</th>
<th>Overall</th>
<th>Viability</th>
<th>Strategy</th>
<th>Reach</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>🟠</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟠</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
<td>🟢</td>
</tr>
</tbody>
</table>

Cisco offers multiple deployment options catering to all different organization configurations. With the recent acquisition of Sourcefire, Cisco continues to focus on its security offerings. Cisco is a strong shortlist candidate for any organization that is already a Cisco shop.
Sophos offers an easy-to-use yet robust email security solution with proprietary encryption

### Market Pillar

<table>
<thead>
<tr>
<th>Product:</th>
<th>Sophos Email Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees:</td>
<td>1,700</td>
</tr>
<tr>
<td>Headquarters:</td>
<td>Abington UK &amp; Burlington, MA, USA</td>
</tr>
<tr>
<td>Website:</td>
<td>sophos.com</td>
</tr>
<tr>
<td>Founded:</td>
<td>1985 with ESG in 2003</td>
</tr>
<tr>
<td>Presence:</td>
<td>Privately Held</td>
</tr>
</tbody>
</table>

**Overview**

- Sophos is a mature player with an established presence in offering small and mid-sized businesses simple and intuitive designs. Sophos has become a full network security vendor with multiple acquisitions in the data protection, MDM, and UTM space.

**Strengths**

- An intuitive interface allows ease of use for non-technical users. A 3-click design allows quick access to all layers of the product.
- Sophos’s proprietary encryption, Secure PDF Exchange, encrypts the entire email and attachments into a PDF through a push-based, password-protected retrieval solution with customization.
- With a high availability model, all add-ons are included at no extra cost. DLP and encryption are included within the advanced license. As well, there are integration capabilities with LDAP, eDirectory, and Active Directory.

**Challenges**

- A focus on simplicity in its use and design restricts some of the more advanced requirements of larger enterprises, such as dashboard customization and advanced reporting. More features are available only in the UTM product.
- There is currently no hosted or SaaS offering available, though UTM can be deployed via Amazon Web Service.
- There is no sandboxing or dynamic URL rewriting features, limiting the ability to detect advanced malware or phishing attacks.

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000

Pricing provided by vendor

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000

Pricing provided by vendor

Vendor Landscape: Email Security Gateway

Info-Tech Research Group
Sophos complements its strong security offerings with a solid email appliance

Sophos is a strong competitor within the ESG market. Its push into the UTM market space signals a shift to offering a larger variety of security products. Consider Sophos for mid-sized organizations with normal security requirements and the possibility of other security product purchases.
Fortinet provides strong spam and spear phishing detection at extremely attractive prices

**Market Pillar**

- **Product:** FortiMail
- **Employees:** 2,300
- **Headquarters:** Sunnyvale, CA, USA
- **Website:** fortinet.com
- **Founded:** 2000
- **Presence:** FTNT

**Overview**

- Fortinet is a worldwide provider of network security with specialization in unified threat management products. It focuses on mid-market enterprises ranging from 250 to 2,500 seats. FortiMail is an affordable option for reasonable security needs.

**Strengths**

- URL checking blocks spam and malware sites, with granular administrative controlled blocking of adult/abusive websites based on a subset of the web filtering database, in addition to URL rewriting and following capabilities.
- FortiMail provides Identity-Based Encryption (IBE) in addition to S/MIME and TLS, to enforce policy-based encryption.
- Pay per box rather than user makes it an affordable product.
- Granular customization options of email digest can alleviate IT burden.

**Challenges**

- Fortinet's antivirus and antimalware engine, FortiGuard, lacks in size and research capabilities in comparison to other vendors within this vendor landscape.
- The FortiMail option tends to be a shortlist candidate for customers already using other Fortinet products, such as its UTM.
- No SaaS offering restricts customers’ ability to adopt cloud functions, however, partners do offer hosted solutions.

3 year TCO for this solution falls into pricing tier 4, between $10,000 and $25,000

Pricing provided by vendor

3 year TCO for this solution falls into pricing tier 4, between $10,000 and $25,000

Pricing provided by vendor
For modest security requirements, Fortinet delivers a great deal of bang for your buck

For Info-Tech Recommends:

FortiMail can be a strong candidate for smaller organizations on a budget with limited security requirements. Fortinet focuses solely on network security with various product offerings. FortiMail is generally a shortlist candidate for customers already using Fortinet products.
Microsoft is able to provide broad features while still ensuring security in a hosted service

**Market Pillar**

- **Product:** Exchange Online Protection
- **Employees:** 100,000+
- **Headquarters:** Redmond, WA, USA
- **Website:** [microsoft.com](http://microsoft.com)
- **Founded:** 1975
- **Presence:** MSFT

**Overview**

- Microsoft’s subscription hosted email security service maintains protection features that are deployed across a global network of data centers. With Microsoft’s business email dominance, it is a strategic candidate for any hosted needs.

**Strengths**

- With a hosted solution, there is the ability to get email on virtually any mobile phone and options for voice mail, unified messaging, and archiving as well.
- Archiving and legal hold capabilities, plus unlimited storage, serves customers’ compliance needs.
- Emails and documents can be stored and shared in project-specific folders, enabling fast information flow.
- Familiar centralized management interface with Office 365.

**Challenges**

- General privacy issues surround moving email to a hosted service. Individual decisions must be made on the trust level of Microsoft.
- EOP lacks various advanced security features in DLP and targeted attack detection that many organizations may deem necessary to their email protection.
- A user per month billing schedule can become very expensive, however, EOP is included with the Office 365 subscription price.

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000

Pricing provided by vendor

$1 $1M+
For basic email hygiene, Microsoft may be enough for any Exchange environment

Vendor Landscape

<table>
<thead>
<tr>
<th>Product</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>Features</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Value Index

72

9th out of 12

Deployment Option:

<table>
<thead>
<tr>
<th>Vendor Solutions Being Offered:</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Premise Appliance Offerings</td>
</tr>
<tr>
<td>Virtual Appliance Platforms Being Supported</td>
</tr>
<tr>
<td>Hosted Deployment Options</td>
</tr>
</tbody>
</table>

Features

<table>
<thead>
<tr>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam/ Bulk</td>
</tr>
<tr>
<td>Spear/ Phishing</td>
</tr>
<tr>
<td>Real Time URL &amp; Malware</td>
</tr>
<tr>
<td>End-User Spam Control</td>
</tr>
<tr>
<td>Data Loss Protection</td>
</tr>
<tr>
<td>Encryption/ Decryption</td>
</tr>
<tr>
<td>Anti-Mal. Signature</td>
</tr>
<tr>
<td>Anti-Mal. Behavioral</td>
</tr>
<tr>
<td>DKIM &amp; SPF</td>
</tr>
<tr>
<td>Hosted Email Support</td>
</tr>
<tr>
<td>Email Archiving</td>
</tr>
<tr>
<td>Hosted &amp; Hybrid Solutions</td>
</tr>
</tbody>
</table>

Info-Tech Recommends:

Microsoft is a giant within the technology world. Its business products are highly used and as such Microsoft is seen as a strategic vendor. Generally, Microsoft is not chosen for its email security offerings and instead for its non-security product suites.
Trend Micro is a dedicated vendor for email security, ensuring continued success

**Innovator**

- **Product:** InterScan Messaging Security
- **Employees:** 5,217
- **Headquarters:** Tokyo, Japan
- **Website:** trendmicro.com
- **Founded:** 1988
- **Presence:** TYO: 4704

**Overview**

- Trend Micro is a well established player in the ESG market space with its InterScan Messaging Security. With various deployment options and a strong organizational focus on its ESG offerings, Trend Micro is a shortlist candidate for many organizations.

**Strengths**

- Administrative interface and controls are designed with ease of use while maintaining strong customization capabilities.
- Enhanced web reputation, document exploit detection, optional sandbox execution analysis, and custom threat intelligence provide comprehensive security from targeted attacks.
- Strong hybrid deployment options with Trend Micro’s cloud service and virtual appliance offer robust mail security.
- DLP filtering rules with customizable compliance templates.

**Challenges**

- Unable to support OpenPGP or S/MIME encryption, restricting some larger enterprise needs.
- No push-based encryption option and anything stronger than TLS requires the Email Encryption module.
- Advanced and compliance workflows for DLP are not comprehensive for some large enterprise needs unless integrated with Trend Micro’s Control Manager.

3 year TCO for this solution falls into pricing tier 5, between $25,000 and $50,000

Pricing provided by vendor
Trend Micro offers strong capabilities to complement depth of anti-malware strengths

<table>
<thead>
<tr>
<th>Vendor Landscape</th>
<th>Product</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overall</td>
<td>Features</td>
</tr>
<tr>
<td></td>
<td>🌟</td>
<td>🌟</td>
</tr>
</tbody>
</table>

**Deployment Option:**

**On-Premise Appliance Offerings**
InterScan Messaging Security (Software Appliance Only), InterScan Messaging Security Suite (software on Windows or Linux), ScanMail Suite for IBM Domino (software), ScanMail Suite for Microsoft Exchange (software)

**Virtual Appliance Platforms Being Supported**
InterScan Messaging Security Platforms Supported: Microsoft Hyper-V, VMware ESX, VMwareESXi v3.5, vSphere

**Hosted Deployment Options**
Hosted Email Security

**Value Index**

89
3rd out of 12

**Info-Tech Recommends:**

One of the most established players in the ESG market place with the InterScan product. A breadth of features coupled with the possibility of leveraging other security product offerings make Trend Micro a shortlist candidate.
McAfee excels in targeted attack detection through powerful threat intelligence and DLP

**Innovator**

- **Product:** McAfee Email Gateway
- **Employees:** 7,100
- **Headquarters:** Santa Clara, CA, USA
- **Website:** mcafee.com
- **Founded:** 1987
- **Presence:** (Intel Corp.) INTC

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000

**Overview**

- A subsidiary of Intel, McAfee offers a comprehensive suite of network and endpoint security products. The acquisition of Secure Computing and its IronMail product provided a strong combination for the email product with McAfee Email and Web Security platform.

**Strengths**

- McAfee supports a large threat intelligence engine combining its web, email, and other security products into its Global Threat Intelligence to provide real time threat detection and updates.
- Native DLP with predefined policies and dictionaries leverages McAfee’s standalone DLP product to offer content aware DLP.
- An integrated engine, McAfee Content Security Suite combines email, web, and DLP into a single pane offering with multiple deployment options.
- The only vendor to offer a blade form appealing to service providers.

**Challenges**

- No compliance-specific controls or workflow is available within the DLP solution in the ESG.

Pricing solicited from public sources
McAfee delivers strong features with a variety of deployment options

**Vendor Landscape**

**Product**

- **Overall**
- **Features**
- **Usability**
- **Afford.**
- **Arch.**

**Vendor**

- **Overall**
- **Viability**
- **Strategy**
- **Reach**
- **Channel**

**Deployment Option:**

- **On-Premise Appliance Offerings**
  - McAfee Email Gateway

- **Virtual Appliance Platforms Being Supported**
  - McAfee Email Gateway
  - Platforms Supported: VMware, vSphere, ESX

- **Hosted Deployment Options**
  - McAfee SaaS Email Protection and Continuity

**Value Index**

68

10th out of 12

**Features**

- Spam/ Bulk
- Spear/ Phishing
- Real Time URL & Malware
- End-User Spam Control
- Data Loss Protection
- Encryption/ Decryption
- Anti-Mal. Signature
- Anti-Mal. Behavioral
- DKIM & SPF
- Hosted Email Support
- Email Archiving
- Hosted & Hybrid Solutions

**Info-Tech Recommends:**

One of the most mature and capable vendors, McAfee commands strong influence and reputation within the information security sector. Under the control of Intel, McAfee can expect ongoing focus as Intel continues to market its security offerings more aggressively.
Websense ensures compliance while protecting against targeted attacks within numerous deployment options

**Innovator**

- Product: Websense Email Security Gateway
- Employees: 1,600
- Headquarters: San Diego, CA
- Website: websense.com
- Founded: 1994
- Presence: Privately Held

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000

### Overview
- Websense is a leader within the unified content security solution space with its TRITON management interface combining its ESG, web security, and DLP functions.

### Strengths
- Strong deployment options of on-premise, a SaaS offering, and a hybrid solution.
- The ESG embeds the same DLP capabilities as its standalone DLP solution with predefined compliance, machine learning, file/database fingerprinting, OCR, and drip DLP at no additional charge.
- A virtual sandbox, time of click detection, and static code analysis provide good targeted attack protection.

### Challenges
- Websense’s encryption offering through Voltage Security is not integrated into the TRITON management interface, limiting the visibility and controls around encryption.
- Websense is a relatively smaller and newer player within the ESG marketplace with its primary focus on web security.

Pricing provided by vendor

Pricing provided by vendor

$1

$1M+

$1
Websense focuses on content security and its ESG is no exception

<table>
<thead>
<tr>
<th>Vendor Landscape</th>
<th>Product</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overall</td>
<td>Features</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deployment Option:</th>
<th>Vendor Solutions Being Offered:</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Premise Appliance Offerings</td>
<td>Websense Email Security Gateway Models: V5000, V10000</td>
</tr>
<tr>
<td>Virtual Appliance Platforms Being Supported</td>
<td>Websense Email Security Gateway Anywhere (Hybrid) Platforms Supported: OVF, ESXi 4.0</td>
</tr>
<tr>
<td>Hosted Deployment Options</td>
<td>Websense Cloud Email Security Integrated Hybrid Offering</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam/ Bulk</td>
</tr>
<tr>
<td>Spear/ Phishing</td>
</tr>
<tr>
<td>Real Time URL &amp; Malware</td>
</tr>
<tr>
<td>End-User Spam Control</td>
</tr>
<tr>
<td>Data Loss Protection</td>
</tr>
<tr>
<td>Encryption/ Decryption</td>
</tr>
<tr>
<td>Anti-Mal. Signature</td>
</tr>
<tr>
<td>Anti-Mal. Behavioral</td>
</tr>
<tr>
<td>DKIM &amp; SPF</td>
</tr>
<tr>
<td>Hosted Email Support</td>
</tr>
<tr>
<td>Email Archiving</td>
</tr>
<tr>
<td>Hosted &amp; Hybrid Solutions</td>
</tr>
</tbody>
</table>

Value Index

83

4th out of 12

Info-Tech Recommends:

With the release and development of the TRITON management system, Websense has positioned itself as a strong full security suite vendor. A historical focus on web security and the now established TRITON management system enable Websense to provide a strong ESG offering.
Clearswift provides high-level email security with a focus on compliance needs

**Innovator**

- **Product:** Clearswift SECURE Gateway
- **Employees:** 160
- **Headquarters:** Theale, UK
- **Website:** clearswift.com
- **Founded:** 1996
- **Presence:** Privately Held

**Overview**

- Clearswift has established itself as a strong player within the email protection market specializing in data protection and governance. A proven track record of innovation and a security focus make Clearswift a shortlist candidate for any high demand organization.

**Strengths**

- Clearswift is the only vendor in this evaluation that has adaptive redaction content inspection of inbound & outbound messages. Specific content that violates DLP policies can be redacted out of the message allowing for message flow without data leakage.
- ImageLogic is Clearswift's proprietary detection engine that has the flexibility to stop images from leaving an organization while flowing around the business. An excellent tool for IP control.
- An intuitive web-based interface allows for centralized management with clear and concise dashboards and reporting.

**Challenges**

- A relatively small player among others in this vendor landscape, Clearswift is unable to leverage a broader security product portfolio. However, Clearswift is deeply focused on critical information protection.
- No SaaS-based option is available, with limited non-security features available, such as archiving.

3 year TCO for this solution falls into pricing tier 6, between $50,000 and $100,000

Pricing provided by vendor

Vendor Landscape: Email Security Gateway
Adaptive redaction sets Clearswift apart for specific use cases

<table>
<thead>
<tr>
<th>Vendor Landscape</th>
<th>Product</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overall</td>
<td>Features</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Vendor Landscape" /></td>
<td><img src="image" alt="Product" /></td>
</tr>
</tbody>
</table>

**Deployment Option:**

<table>
<thead>
<tr>
<th>On-Premise Appliance Offerings</th>
<th>Vendor Solutions Being Offered:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearswift SECURE Email Gateway</td>
<td>Clearswift SECURE Exchange Gateway Model: E500, E2000</td>
</tr>
<tr>
<td>Virtual Appliance Platforms Being Supported</td>
<td>Clearswift SECURE Email Gateway Platforms Supported: VMware, vSphere 5.1, and Microsoft Hyper-V 2012</td>
</tr>
<tr>
<td>Hosted Deployment Options</td>
<td>NA</td>
</tr>
</tbody>
</table>

**Features**

<table>
<thead>
<tr>
<th>Spam/ Bulk</th>
<th>Spear/ Phishing</th>
<th>Real Time URL &amp; Malware</th>
<th>End-User Spam Control</th>
<th>Data Loss Protection</th>
<th>Encryption/ Decryption</th>
<th>Anti-Mal. Signature</th>
<th>Anti-Mal. Behavioral</th>
<th>DKIM &amp; SPF</th>
<th>Hosted Email Support</th>
<th>Email Archiving</th>
<th>Hosted &amp; Hybrid Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
<td><img src="image" alt="Features" /></td>
</tr>
</tbody>
</table>

**Value Index**

<table>
<thead>
<tr>
<th>74</th>
<th>8th out of 12</th>
</tr>
</thead>
</table>

**Info-Tech Recommends:**

If you are in a highly regulated industry and have high security requirements, Clearswift is a top shortlist candidate for your organization. Its advanced capabilities lend themselves to large enterprises without specific offerings for SMBs. Clearswift is a small player within the ESG market, however, with little other security product offerings.
Proofpoint is a highly responsive and highly dedicated vendor

**Emerging Player**

- **Product:** Proofpoint Enterprise Protection
- **Employees:** 600
- **Headquarters:** Sunnyvale, CA, USA
- **Website:** proofpoint.com
- **Founded:** 2002
- **Presence:** PFPT

**Overview**

- A recent IPO in 2012 has enabled a continuation of high growth and established Proofpoint as a viable shortlist candidate.
- An almost dedicated email security firm, Proofpoint offers a wide selection of vertical add-ons to an ESG.

**Strengths**

- Proofpoint’s Targeted Attack Protection service, a recent release, enables high response times with in-depth reporting based on time of click URL inspection.
- Strong central policy-driven DLP provides a sophisticated outbound content inspection built on predefined dictionaries and policies.
- A push-based encryption offers many of the functions normally provided in a pull-based and policy-based encryption.

**Challenges**

- As a pure play vendor, Proofpoint can be limiting to many organizations looking to purchase or expand their security suites and integration capabilities with one vendor.
- A more technical and enterprise-based solution makes adoption by small to mid-sized businesses difficult.

The vendor declined to provide pricing, and publicly available pricing could not be found
Strong features make Proofpoint an option worth considering for standalone email security requirements

The vendor declined to provide pricing, and publicly available pricing could not be found

A focus on larger enterprise management seems to skip over SMBs. Proofpoint is a dedicated vendor demonstrating focus but limiting the ability to leverage a wide security suite offering.
Google gives peace of mind to hosted email while providing a breadth of additional features

**Emerging Player**

- **Product:** Google Apps
- **Employees:** 47,756
- **Headquarters:** Mountain View, CA, USA
- **Website:** google.com
- **Founded:** 1995
- **Presence:** GOOG

3 year TCO for this solution falls into pricing tier 8, between $250,000 and $500,000

**Overview**

- Google Apps is the suite of Google products designed for organizational use. Gmail is one of many customizable apps available in the larger service. A shortlist candidate for any hosted email needs, Gmail is the world’s largest email service.

**Strengths**

- Gmail is a hosted service where users can log in from any web browser on any device, accessing email that is stored securely at Google rather than on a computer or the organization’s mail server.
- Critical data is automatically backed up on Google servers.
- Google Apps is a comprehensive suite of functions receiving high adoption rates by businesses due to multiple features all designed with ease of use.
- Unlimited user accounts with mobile access and apps.

**Challenges**

- If purchased with Google Apps, Gmail can become expensive based on $50 per user per year, however, this does include base email functionality in addition to ESG capabilities.
- Potential compliance, privacy, and legal issues may arise for organizations in highly regulated industries due to loss of data control.
- Gmail lacks various advanced security features many organizations may deem necessary to their email protection.

Pricing solicited from public sources.
Google delivers basic email security to its hosted email users

<table>
<thead>
<tr>
<th>Vendor Landscape</th>
<th>Product</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>Features</td>
<td>Usability</td>
</tr>
<tr>
<td><img src="Image" alt="Vendor Landscape Image" /></td>
<td><img src="Table" alt="Product Table" /></td>
<td><img src="Vendor" alt="Vendor Table" /></td>
</tr>
</tbody>
</table>

**Value Index**

7

11th out of 12

**Deployment Option:**

<table>
<thead>
<tr>
<th>Vendor Solutions Being Offered</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Premise Appliance Offerings</td>
</tr>
<tr>
<td>Virtual Appliance Platforms Being Supported</td>
</tr>
<tr>
<td>Hosted Deployment Options</td>
</tr>
</tbody>
</table>

**Features**

<table>
<thead>
<tr>
<th>Spam/ Bulk</th>
<th>Spear/ Phishing</th>
<th>Real Time URL &amp; Malware</th>
<th>End-User Spam Control</th>
<th>Data Loss Protection</th>
<th>Encryption/ Decryption</th>
<th>Anti-Mal. Signature</th>
<th>Anti-Mal. Behavioral</th>
<th>DKIM &amp; SPF</th>
<th>Hosted Email Support</th>
<th>Email Archiving</th>
<th>Hosted &amp; Hybrid Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="Features" alt="Feature icons" /></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Info-Tech Recommends:**

As the largest corporation in this evaluation, Google is not necessarily known for its email security offering. Google should be considered as a strategic vendor for its business apps offering (Google Apps). Google is a candidate for any sized organization without any serious security requirements or privacy concerns.
Contract Review and Negotiation Tactics

Arrange a call now: email GuidedImplementations@InfoTech.com or call 1-888-670-8889 and ask for the Guided Implementation Coordinator.

<table>
<thead>
<tr>
<th>Prior to the Guided Implementation</th>
<th>During the Guided Implementation</th>
<th>Value &amp; Outcome</th>
</tr>
</thead>
</table>
| 1. Bring final contracts received from vendors on shortlist. | An Info-Tech Consulting Analyst will discuss with you:  
  • Reviewing your contracts, ensuring they are fair and in line with industry standards.  
  • The most effective negotiation tactics to get the best value for your purchase. | At the conclusion of the Guided Implementation call, you will have:  
  • Tactics on how to get a better price on your solution.  
  • Confidence in the solution you are purchasing. |
Identify leading candidates with the *Email Security Gateway Vendor Shortlist & Detailed Feature Analysis Tool*

The Info-Tech *Email Security Gateway Vendor Shortlist & Detailed Feature Analysis Tool* is designed to generate a customized shortlist of vendors based on *your* key priorities.

**This tool offers the ability to modify:**

**Overall Vendor vs. Product Weightings**

- Individual product criteria weightings:
  - Features
  - Usability
  - Affordability
  - Architecture

- Individual vendor criteria weightings:
  - Viability
  - Strategy
  - Reach
  - Channel
Appendix

1. Vendor Landscape Methodology: Overview
2. Vendor Landscape Methodology: Product Selection & Information Gathering
3. Vendor Landscape Methodology: Scoring
4. Vendor Landscape Methodology: Information Presentation
5. Vendor Landscape Methodology: Fact Check & Publication
6. Product Pricing Scenario
Vendor Landscape Methodology: Overview

Info-Tech’s Vendor Landscapes are research materials that review a particular IT market space, evaluating the strengths and abilities of both the products available in that space, as well as the vendors of those products. These materials are created by a team of dedicated analysts operating under the direction of a senior subject matter expert over a period of six weeks.

Evaluations weigh selected vendors and their products (collectively “solutions”) on the following eight criteria to determine overall standing:

• Features: The presence of advanced and market-differentiating capabilities.
• Usability: The intuitiveness, power, and integrated nature of administrative consoles and client software components.
• Affordability: The three-year total cost of ownership of the solution.
• Architecture: The degree of integration with the vendor’s other tools, flexibility of deployment, and breadth of platform applicability.
• Viability: The stability of the company as measured by its history in the market, the size of its client base, and its financial performance.
• Strategy: The commitment to both the market-space, as well as to the various sized clients (small, mid-sized, and enterprise clients).
• Reach: The ability of the vendor to support its products on a global scale.
• Channel: The measure of the size of the vendor’s channel partner program, as well as any channel strengthening strategies.

Evaluated solutions are plotted on a standard two by two matrix:

• Champions: Both the product and the vendor receive scores that are above the average score for the evaluated group.
• Innovators: The product receives a score that is above the average score for the evaluated group, but the vendor receives a score that is below the average score for the evaluated group.
• Market Pillars: The product receives a score that is below the average score for the evaluated group, but the vendor receives a score that is above the average score for the evaluated group.
• Emerging Players: Both the product and the vendor receive scores that are below the average score for the evaluated group.

Info-Tech’s Vendor Landscapes are researched and produced according to a strictly adhered to process that includes the following steps:

• Vendor/product selection
• Information gathering
• Vendor/product scoring
• Information presentation
• Fact checking
• Publication

This document outlines how each of these steps is conducted.
Vendor Landscape Methodology: Vendor/Product Selection & Information Gathering

Info-Tech works closely with its client base to solicit guidance in terms of understanding the vendors with whom clients wish to work and the products that they wish evaluated; this demand pool forms the basis of the vendor selection process for Vendor Landscapes. Balancing this demand, Info-Tech also relies upon the deep subject matter expertise and market awareness of its Senior, Lead, and Principle Research Analysts to ensure that appropriate solutions are included in the evaluation. As an aspect of that expertise and awareness, Info-Tech’s analysts may, at their discretion, determine the specific capabilities that are required of the products under evaluation, and include in the Vendor Landscape only those solutions that meet all specified requirements.

Information on vendors and products is gathered in a number of ways via a number of channels.

Initially, a request package is submitted to vendors to solicit information on a broad range of topics. The request package includes:
• A detailed survey.
• A pricing scenario (see Vendor Landscape Methodology: Price Evaluation and Pricing Scenario, below).
• A request for reference clients.
• A request for a briefing and, where applicable, guided product demonstration.

These request packages are distributed approximately twelve weeks prior to the initiation of the actual research project to allow vendors ample time to consolidate the required information and schedule appropriate resources.

During the course of the research project, briefings and demonstrations are scheduled (generally for one hour each session, though more time is scheduled as required) to allow the analyst team to discuss the information provided in the survey, validate vendor claims, and gain direct exposure to the evaluated products. Additionally, an end-user survey is circulated to Info-Tech’s client base and vendor-supplied reference accounts are interviewed to solicit their feedback on their experiences with the evaluated solutions and with the vendors of those solutions.

These materials are supplemented by a thorough review of all product briefs, technical manuals, and publicly available marketing materials about the product, as well as about the vendor itself.

Refusal by a vendor to supply completed surveys or submit to participation in briefings and demonstrations does not eliminate a vendor from inclusion in the evaluation. Where analyst and client input has determined that a vendor belongs in a particular evaluation, it will be evaluated as best as possible based on publicly available materials only. As these materials are not as comprehensive as a survey, briefing, and demonstration, the possibility exists that the evaluation may not be as thorough or accurate. Since Info-Tech includes vendors regardless of vendor participation, it is always in the vendor’s best interest to participate fully.

All information is recorded and catalogued, as required, to facilitate scoring and for future reference.
Vendor Landscape Methodology: Scoring

Once all information has been gathered and evaluated for all vendors and products, the analyst team moves to scoring. All scoring is performed at the same time so as to ensure as much consistency as possible. Each criterion is scored on a ten point scale, though the manner of scoring for criteria differs slightly:

- Features is scored via **Cumulative Scoring**
- Affordability is scored via **Scalar Scoring**
- All other criteria are scored via **Base5 Scoring**

In Cumulative Scoring, a single point is assigned to each evaluated feature that is regarded as being fully present, partial points to each feature that is partially present, and zero points to features that are deemed to be absent or unsatisfactory. The assigned points are summed and normalized to a value out of ten. For example, if a particular Vendor Landscape evaluates eight specific features in the Feature Criteria, the summed score out of eight for each evaluated product would be multiplied by 1.25 to yield a value out of ten.

In Scalar Scoring, a score of ten is assigned to the lowest cost solution, and a score of one is assigned to the highest cost solution. All other solutions are assigned a mathematically determined score based on their proximity to / distance from these two endpoints. For example, in an evaluation of three solutions, where the middle cost solution is closer to the low end of the pricing scale it will receive a higher score, and where it is closer to the high end of the pricing scale it will receive a lower score; depending on proximity to the high or low price it is entirely possible that it could receive either ten points (if it is very close to the lowest price) or one point (if it is very close to the highest price). Where pricing cannot be determined (vendor does not supply price and public sources do not exist), a score of 0 is automatically assigned.

In Base5 scoring a number of sub-criteria are specified for each criterion (for example, Longevity, Market Presence, and Financials are sub-criteria of the Viability criterion), and each one is scored on the following scale:

- 5 - The product/vendor is exemplary in this area (nothing could be done to improve the status).
- 4 - The product/vendor is good in this area (small changes could be made that would move things to the next level).
- 3 - The product/vendor is adequate in this area (small changes would make it good, more significant changes required to be exemplary).
- 2 - The product/vendor is poor in this area (this is a notable weakness and significant work is required).
- 1 - The product/vendor is terrible/fails in this area (this is a glaring oversight and a serious impediment to adoption).

The assigned points are summed and normalized to a value out of ten as explained in Cumulative Scoring above.

Scores out of ten, known as Raw scores, are transposed as-is into Info-Tech’s Vendor Landscape Shortlist Tool, which automatically determines Vendor Landscape positioning (see Vendor Landscape Methodology: Information Presentation - Vendor Landscape, below), Criteria Score (see Vendor Landscape Methodology: Information Presentation - Criteria Score, below), and Value Index (see Vendor Landscape Methodology: Information Presentation - Value Index, below).
Vendor Landscape Methodology: Information Presentation – Vendor Landscape

Info-Tech’s Vendor Landscape is a two-by-two matrix that plots solutions based on the combination of Product score and Vendor score. Placement is not determined by absolute score, but instead by relative score. Relative scores are used to ensure a consistent view of information and to minimize dispersion in nascent markets, while enhancing dispersion in commodity markets to allow for quick visual analysis by clients.

Relative scores are calculated as follows:

1. Raw scores are transposed into the Info-Tech Vendor Landscape Shortlist Tool (for information on how Raw scores are determined, see Vendor Landscape Methodology: Scoring, above).

2. Each individual criterion Raw score is multiplied by the pre-assigned weighting factor for the Vendor Landscape in question. Weighting factors are determined prior to the evaluation process to eliminate any possibility of bias. Weighting factors are expressed as a percentage such that the sum of the weighting factors for the Vendor criteria (Viability, Strategy, Reach, Channel) is 100% and the sum of the Product criteria (Features, Usability, Affordability, Architecture) is 100%.

3. A sum-product of the weighted Vendor criteria scores and of the weighted Product criteria scores is calculated to yield an overall Vendor score and an overall Product score.

4. Overall Vendor scores are then normalized to a 20 point scale by calculating the arithmetic mean and standard deviation of the pool of Vendor scores. Vendors for whom their overall Vendor score is higher than the arithmetic mean will receive a normalized Vendor score of 11-20 (exact value determined by how much higher than the arithmetic mean their overall Vendor score is), while vendors for whom their overall Vendor score is lower than the arithmetic mean will receive a normalized Vendor score of between one and ten (exact value determined by how much lower than the arithmetic mean their overall Vendor score is).

5. Overall Product score is normalized to a 20 point scale according to the same process.

6. Normalized scores are plotted on the matrix, with Vendor score being used as the x-axis, and Product score being used as the y-axis.

Vendor Landscape

- **Innovators**: solutions with below average Vendor scores and above average Product scores.
- **Champions**: solutions with above average Vendor scores and above average Product scores.
- **Emerging Players**: solutions with below average Vendor scores and below average Product scores.
- **Market Pillars**: solutions with below average Vendor scores and above average Product scores.
Vendor Landscape Methodology: Information Presentation – Criteria Scores (Harvey Balls)

Info-Tech’s criteria scores are visual representations of the absolute score assigned to each individual criterion, as well as of the calculated overall vendor and product scores. The visual representation used is Harvey Balls.

Harvey Balls are calculated as follows:

1. Raw scores are transposed into the Info-Tech Vendor Landscape Shortlist Tool (for information on how raw scores are determined, see Vendor Landscape Methodology: Scoring, above).
2. Each individual criterion raw score is multiplied by a pre-assigned weighting factor for the Vendor Landscape in question. Weighting factors are determined prior to the evaluation process, based on the expertise of the Senior or Lead Research Analyst, to eliminate any possibility of bias. Weighting factors are expressed as a percentage, such that the sum of the weighting factors for the vendor criteria (Viability, Strategy, Reach, Channel) is 100%, and the sum of the product criteria (Features, Usability, Affordability, Architecture) is 100%.
3. A sum-product of the weighted vendor criteria scores and of the weighted product criteria scores is calculated to yield an overall vendor score and an overall product score.
4. Both overall vendor score / overall product score, as well as individual criterion raw scores are converted from a scale of one to ten to Harvey Ball scores on a scale of zero to four, where exceptional performance results in a score of four and poor performance results in a score of zero.
5. Harvey Ball scores are converted to Harvey Balls as follows:
   - A score of four becomes a full Harvey Ball.
   - A score of three becomes a three-quarter full Harvey Ball.
   - A score of two becomes a half-full Harvey Ball.
   - A score of one becomes a one-quarter full Harvey Ball.
   - A score of zero becomes an empty Harvey Ball.
6. Harvey Balls are plotted by solution in a chart where rows represent individual solutions and columns represent overall vendor / overall product, as well as individual criteria. Solutions are ordered in the chart alphabetically by vendor name.

<table>
<thead>
<tr>
<th>Overall Harvey Balls represent weighted aggregates.</th>
<th>Overall Harvey Balls represent individual raw scores.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product</strong></td>
<td><strong>Vendor</strong></td>
</tr>
<tr>
<td><strong>Overall</strong></td>
<td><strong>Features</strong></td>
</tr>
<tr>
<td><img src="image" alt="Harvey Ball" /></td>
<td><img src="image" alt="Harvey Ball" /></td>
</tr>
</tbody>
</table>
Vendor Landscape Methodology: Information Presentation – Feature Ranks (Stoplights)

Info-Tech’s Feature Ranks are visual representations of the presence/availability of individual features that collectively comprise the Features’ criteria. The visual representation used is stoplights.

Stoplights are determined as follows:

1. A single point is assigned to each evaluated feature that is regarded as being fully present, partial points to each feature that is partially present, and zero points to features that are deemed to be fully absent or unsatisfactory.
   - Fully present means all aspects and capabilities of the feature as described are in evidence.
   - Fully absent means all aspects and capabilities of the feature as described are missing or lacking.
   - Partially present means some, but not all, aspects and capabilities of the feature as described are in evidence, or all aspects and capabilities of the feature as described are in evidence, but only for some models in a line.

2. Feature scores are converted to stoplights as follows:
   - Full points become a green light.
   - Partial points become a yellow light.
   - Zero points become a red light.

3. Stoplights are plotted by solution in a chart where rows represent individual solutions and columns represent individual features. Solutions are ordered in the chart alphabetically by vendor name.

For example, a set of applications is being reviewed and a feature of “Integration with Mobile Devices” that is defined as “availability of dedicated mobile device applications for iOS, Android, and BlackBerry devices” is specified. Solution A provides such apps for all listed platforms and scores “green,” solution B provides apps for iOS and Android only and scores “yellow,” while solution C provides mobile device functionality through browser extensions, has no dedicated apps, and so scores “red.”
Vendor Landscape Methodology: Information Presentation – Value Index

Info-Tech’s Value Index is an indexed ranking of solution value per dollar as determined by the raw scores assigned to each criteria (for information on how raw scores are determined, see Vendor Landscape Methodology: Scoring, above).

Value scores are calculated as follows:

1. The Affordability criterion is removed from the overall product score and the remaining product score criteria (Features, Usability, Architecture) are reweighted so as to retain the same weightings relative to one another, while still summing to 100%. For example, if all four product criteria were assigned base weightings of 25%, for the determination of the Value Score, Features, Usability, and Architecture would be reweighted to 33.3% each to retain the same relative weightings while still summing to 100%.

2. A sum-product of the weighted vendor criteria scores and of the reweighted product criteria scores is calculated to yield an overall vendor score and a reweighted overall Product score.

3. The overall vendor score and the reweighted overall product score are then summed, and this sum is multiplied by the Affordability raw score to yield an interim Value Score for each solution.

4. All interim Value Scores are then indexed to the highest performing solution by dividing each interim Value Score by the highest interim Value Score. This results in a Value Score of 100 for the top solution and an indexed Value Score relative to the 100 for each alternate solution.

5. Solutions are plotted according to Value Score, with the highest score plotted first, and all remaining scores plotted in descending numerical order.

Where pricing is not provided by the vendor and public sources of information cannot be found, an Affordability raw score of zero is assigned. Since multiplication by zero results in a product of zero, those solutions for which pricing cannot be determined receive a Value Score of zero. Since Info-Tech assigns a score of zero where pricing is not available, it is always in the vendor’s best interest to provide accurate and up to date pricing. In the event that insufficient pricing is available to accurately calculate a Value Index, Info-Tech will omit it from the Vendor Landscape.
Vendor Landscape Methodology: Information Presentation – Price Evaluation: Small Enterprise

Info-Tech’s Price Evaluation is a tiered representation of the three-year Total Cost of Ownership (TCO) of a proposed solution. Info-Tech uses this method of communicating pricing information to provide high-level budgetary guidance to its end-user clients while respecting the privacy of the vendors with whom it works. The solution TCO is calculated and then represented as belonging to one of ten pricing tiers.

Pricing tiers are as follows:
1. Between $1 and $2,500
2. Between $2,500 and $5,000
3. Between $5,000 and $10,000
4. Between $10,000 and $25,000
5. Between $25,000 and $50,000
6. Between $50,000 and $100,000
7. Between $100,000 and $250,000
8. Between $250,000 and $500,000
9. Between $500,000 and $1,000,000
10. Greater than $1,000,000

Where pricing is not provided, Info-Tech makes use of publicly available sources of information to determine a price. As these sources are not official price lists, the possibility exists that they may be inaccurate or outdated, and so the source of the pricing information is provided. Since Info-Tech publishes pricing information regardless of vendor participation, it is always in the vendor’s best interest to supply accurate and up to date information.

Info-Tech’s Price Evaluations are based on pre-defined pricing scenarios (see Product Pricing Scenario, below) to ensure a comparison that is as close as possible between evaluated solutions. Pricing scenarios describe a sample business and solicit guidance as to the appropriate product/service mix required to deliver the specified functionality, the list price for those tools/services, as well as three full years of maintenance and support.
Vendor Landscape Methodology: Information Presentation – Scenarios

Info-Tech’s Scenarios highlight specific use cases for the evaluated solution to provide as complete (when taken in conjunction with the individual written review, Vendor Landscape, Criteria Scores, Feature Ranks, and Value Index) a basis for comparison by end-user clients as possible.

Scenarios are designed to reflect tiered capability in a particular set of circumstances. Determination of the Scenarios in question is at the discretion of the analyst team assigned to the research project. Where possible, Scenarios are designed to be mutually exclusive and collectively exhaustive, or at the very least, hierarchical such that the tiers within the Scenario represent a progressively greater or broader capability.

Scenario ranking is determined as follows:

1. The analyst team determines an appropriate use case.
   
   For example:
   
   • Clients that have multinational presence and require vendors to provide four-hour onsite support.

2. The analyst team establishes the various tiers of capability.
   
   For example:
   
   • Presence in Americas
   • Presence in EMEA
   • Presence in APAC

3. The analyst team reviews all evaluated solutions and determines which ones meet which tiers of capability.
   
   For example:
   
   • Presence in Americas – Vendor A, Vendor C, Vendor E
   • Presence in EMEA – Vendor A, Vendor B, Vendor C
   • Presence in APAC – Vendor B, Vendor D, Vendor E

4. Solutions are plotted on a grid alphabetically by vendor by tier. Where one vendor is deemed to be stronger in a tier than other vendors in the same tier, they may be plotted non-alphabetically.
   
   For example:
   
   • Vendor C is able to provide four-hour onsite support to 12 countries in EMEA while Vendors A and B are only able to provide four-hour onsite support to eight countries in EMEA; Vendor C would be plotted first, followed by Vendor A, then Vendor B.

Analysts may also elect to list only the most Exemplary Performers for a given use case. One to three vendors will appear for each of these purchasing scenarios with a brief explanation as to why we selected them as top-of-class.
Vendor Landscape Methodology: Information Presentation – Vendor Awards

At the conclusion of all analyses, Info-Tech presents awards to exceptional solutions in three distinct categories. Award presentation is discretionary; not all awards are extended subsequent to each Vendor Landscape and it is entirely possible, though unlikely, that no awards may be presented.

Awards categories are as follows:

- **Champion Awards** are presented to those solutions, and only those solutions, that land in the Champion zone of the Info-Tech Vendor Landscape (see Vendor Landscape Methodology: Information Presentation – Vendor Landscape, above). If no solutions land in the Champion zone, no Champion Awards are presented. Similarly, if multiple solutions land in the Champion zone, multiple Champion Awards are presented.

- **Trend Setter Awards** are presented to those solutions, and only those solutions, that are deemed to include the most original/inventive product/service, or the most original/inventive feature/capability of a product/service. If no solution is deemed to be markedly or sufficiently original/inventive, either as a product/service on the whole or by feature/capability specifically, no Trend Setter Award is presented. Only one Trend Setter Award is available for each Vendor Landscape.

- **Best Overall Value Awards** are presented to those solutions, and only those solutions, that are ranked highest on the Info-Tech Value Index (see Vendor Landscape Methodology: Information Presentation – Value Index, above). If insufficient pricing information is made available for the evaluated solutions, such that a Value Index cannot be calculated, no Best Overall Value Award will be presented. Only one Best Overall Value Award is available for each Vendor Landscape.
Vendor Landscape Methodology: Fact Check & Publication

Info-Tech takes the factual accuracy of its Vendor Landscapes, and indeed of all of its published content, very seriously. To ensure the utmost accuracy in its Vendor Landscapes, we invite all vendors of evaluated solutions (whether the vendor elected to provide a survey and/or participate in a briefing or not) to participate in a process of fact check.

Once the research project is complete and the materials are deemed to be in a publication ready state, excerpts of the material specific to each vendor’s solution are provided to the vendor. Info-Tech only provides material specific to the individual vendor’s solution for review encompassing the following:

- All written review materials of the vendor and the vendor’s product that comprise the evaluated solution.
- Info-Tech’s Criteria Scores / Harvey Balls detailing the individual and overall vendor / product scores assigned.
- Info-Tech’s Feature Rank / stoplights detailing the individual feature scores of the evaluated product.
- Info-Tech’s Raw Pricing for the vendor either as received from the vendor or as collected from publicly available sources.
- Info-Tech’s Scenario ranking for all considered scenarios for the evaluated solution.

Info-Tech does not provide the following:

- Info-Tech’s Vendor Landscape placement of the evaluated solution.
- Info-Tech’s Value Score for the evaluated solution.
- End-user feedback gathered during the research project.
- Info-Tech’s overall recommendation in regard to the evaluated solution.

Info-Tech provides a one-week window for each vendor to provide written feedback. Feedback must be corroborated (be provided with supporting evidence), and where it does, feedback that addresses factual errors or omissions is adopted fully, while feedback that addresses opinions is taken under consideration. The assigned analyst team makes all appropriate edits and supplies an edited copy of the materials to the vendor within one week for final review.

Should a vendor still have concerns or objections at that time, they are invited to a conversation, initially via email, but as required and deemed appropriate by Info-Tech, subsequently via telephone, to ensure common understanding of the concerns. Where concerns relate to ongoing factual errors or omissions, they are corrected under the supervision of Info-Tech’s Vendor Relations personnel. Where concerns relate to ongoing differences of opinion, they are again taken under consideration with neither explicit nor implicit indication of adoption.

Publication of materials is scheduled to occur within the six weeks immediately following the completion of the research project, but does not occur until the fact check process has come to conclusion, and under no circumstances are “pre-publication” copies of any materials made available to any client.
Product Pricing Scenario

An organization is looking to implement a new email security gateway solution. It has a high-availability MS Exchange email server infrastructure supporting 2,000 users across the international organization.

- Message volumes are as follows:

<table>
<thead>
<tr>
<th>Description</th>
<th>Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total inbound messages (average)</td>
<td>100,000/day</td>
</tr>
<tr>
<td>Total inbound messages (peak)</td>
<td>250,000/day</td>
</tr>
<tr>
<td>% of I/B messages blocked as spam/malware/bulk (average)</td>
<td>60%</td>
</tr>
<tr>
<td>% of I/B messages blocked as spam/malware/bulk (peak)</td>
<td>90%</td>
</tr>
<tr>
<td>Outbound messages (average)</td>
<td>40,000/day</td>
</tr>
<tr>
<td>Outbound messages (peak)</td>
<td>60,000/day</td>
</tr>
</tbody>
</table>

The expected solution capabilities are as follows:

- Basic email anti-spam/bulk/phishing/malware capabilities
- Granular user/domain reporting and blocking
- High availability
- Gold level support services should include the following:
  - Implementation support
  - Technical documentation and guides
  - 24/7 Technical support by phone or online
- Licensing costs for host server operating systems not included
- If the solution requires the purchase of an addition host server, cost is not included