Vendor Landscape: Secure Web Gateways

Just filter it.
Introduction

Secure Web Gateway (SWG) products are developing toward prevention techniques over conventional detection.

This Research Is Designed For:

✓ Enterprises seeking to select a solution for SWG.
✓ Their SWG use case may include:
  - IT leaders looking to enhance security against inbound and outbound malware threats.
  - IT leaders looking to monitor and limit employee web usage, as well as control employee access to some apps (e.g. social media).
  - Organizations with multiple remote users who require web protection even off the network.

This Research Will Help You:

✓ Understand what’s new in the SWG market.
✓ Evaluate SWG 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 SWG market, including the following notable performers:

Champions:
- **Barracuda**, with strong vendor developments accompanied by one of the strongest total risk management offerings.
- **Trend Micro**, as it moves to provide a more comprehensive security offering, it advances its web filtering capabilities.
- **Cisco**, the stability and strategic value of such a large vendor offers value.

Value Award:
- **Barracuda**, a strong feature offering with simple and low pricing.

Trend Setter Award:
- **iboss**, with numerous advanced features, such as 3D security, that were developed from an initial R&D phase for five years.

This Vendor Landscape was written with mid-market focus.

---

**Info-Tech Insight**

1. **Executable detection:**
   Malicious web scripts, either changing dynamically during browser execution or changing quickly on the server-side, can be undetected through simple JavaScript evaluation. Advanced sandboxing or emulation capabilities are needed to detect these obfuscated scripts.

2. **Endpoint support:**
   Business is about access. SWGs should support mobile and BYOD security and compliance through OS support and guest Wi-Fi support, enabling anywhere access.

3. **Web application support:**
   Productivity tools must be included in evaluating a product. Granular control options around specific applications are necessary.
Market overview

**How it got here**

- SWG has existed since the 1990s, stemming from the U.S. Congress passing the Communications Indecency Act. However, civil liberties groups argued that banning all indecency from the Internet was an infringement of free speech, and thus began the process of content filtering.
- Widespread web filtering is ubiquitous in some countries like China or Cuba, in an attempt to stop access to what is deemed objectionable.
- From web filtering of content, advancements in malware detection emerged, such as dynamic URL filtering, decryption support, and advanced techniques such as sandboxing or behavioral analysis.
- Organizations began to use SWGs as productivity controls to limit general internet distraction of employees, like placing time constraints on certain activities or restrictions on non-essential websites.
- Granular controls evolved around web-based applications or social media sites that would allow a certain level of use by an employee.

**Where it’s going**

- A gradual move toward consolidation in the market is slowly eliminating mid-sized players as they are acquired by large firms. M86 by Trustwave, Crossbeam by Blue Coat, ValidEdge by McAfee, and Cognitive Security by Cisco name a few acquisitions.
- The overall SWG marketplace is expanding from detection to prevention and response. Either integration or built-in native capabilities will further the security suite work that can be done by a SWG.
- Cloud services, currently varied among vendors, will become a common feature as services need to support traffic redirection to the cloud and user authentication.
- As greater use of smart mobile devices and BYOD takes hold, vendors will no longer be able to support only certain OSes. Vendors will overcome these architectural challenges to provide wide mobile and BYOD support.
- As vendors market their compressive UTM products more heavily, many SWG capabilities will be native to these products. Standalone SWG products, although still being offered, will not be a major focus from vendors.

---

**Info-Tech Insight**

As the market evolves, capabilities that were once cutting edge become default and new functionality becomes differentiating. Bandwidth utilization management has become a Table Stakes capability and should no longer be used to differentiate solutions. Instead, focus on browser code emulation and multiple mobile OS support to get the best fit for your requirements.
SWG vendor selection / knock-out criteria: market share, mind share, and platform coverage

- Advanced environment support (mobile OS, cloud, etc.) in addition to advanced executable detection are pushing vendors to offer more and more features in their SWG products. Content and context inspection and evaluation are now common in determining the nature and ultimate threat of inbound and outbound traffic.

- 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 mid and large-sized enterprises.

### Included in this Vendor Landscape:

- **Barracuda.** A strong and fast growth security vendor competing in the SWG market with the Barracuda Web Filter.
- **Blue Coat.** With both security and networking offerings, Blue Coat offers a multi part software and hardware SWG.
- **Cisco.** One of the largest network manufacturers, Cisco competes in various security spaces like SWG.
- **ContentKeeper.** Although one of the smaller sized vendors, ContentKeeper offers a feature-rich, robust SWG.
- **McAfee.** A subsidiary of Intel, McAfee is a strong player in the SWG market offering a family of products.
- **iboss.** Offerings in web security, mobile security, and advanced threat and data protection.
- **Sophos.** A security software and hardware vendor, Sophos offers an ecosystem of security including SWG.
- **Symantec.** The largest security software company leverages its global presence for the SWG enterprise market.
- **Trustwave.** A mostly compliance (PCI specifically) vendor, Trustwave entered the SWG market with its purchase of M86.
- **Trend Micro.** A diversified security vendor offering multiple SWG deployment options.
- **Websense.** With primary focus on its TRITON management (UTM product), Websense is a strong ecosystem vendor.
- **Zscaler.** The only fully cloud-based SWG vendor offers unique advantages but has not been fully hardened.
## SWG criteria & weighting factors

### Product Evaluation Criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>The solution provides basic and advanced feature/functionality.</td>
</tr>
<tr>
<td>Interface</td>
<td>The end-user and administrative interfaces are intuitive and offer streamlined workflow.</td>
</tr>
<tr>
<td>Affordability</td>
<td>Implementing and operating the solution is affordable given the technology.</td>
</tr>
<tr>
<td>Architecture</td>
<td>Multiple deployment options and extensive integration capabilities are available.</td>
</tr>
</tbody>
</table>

### Vendor Evaluation Criteria

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

### Criteria Weighting

- **Features**: 30%
- **Affordability**: 40%
- **Architecture**: 20%
- **Product**: 25%
- **Vendor**: 25%
The Info-Tech SWG 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>Vendor</th>
<th>Overall</th>
<th>Features</th>
<th>Interface</th>
<th>Afford.</th>
<th>Arch.</th>
<th>Overall</th>
<th>Viability</th>
<th>Focus</th>
<th>Support</th>
<th>Sales</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>
</tr>
<tr>
<td>Blue Coat</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>
</tr>
<tr>
<td>ContentKeeper</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>
</tr>
<tr>
<td>iboss</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: 🍊 =Exemplary, 🍊 =Good, 🍊 =Adequate, 🍊 =Inadequate, 🍊 =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>Vendor</th>
<th>Overall</th>
<th>Features</th>
<th>Interface</th>
<th>Afford.</th>
<th>Arch.</th>
<th>Overall</th>
<th>Viability</th>
<th>Focus</th>
<th>Support</th>
<th>Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sophos</td>
<td></td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Symantec</td>
<td></td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Trustwave</td>
<td></td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Trend Micro</td>
<td></td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Websense</td>
<td></td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Zscaler</td>
<td></td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Legend: 
- =Exemplary 
- =Good 
- =Adequate 
- =Inadequate 
- =Poor

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

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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>What it is:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clustering</td>
<td>The solution allows for multi-instance deployments to be managed via a single administrative interface.</td>
</tr>
<tr>
<td>Bandwidth Utilization Management</td>
<td>The solution can reduce bandwidth usage by controlling uplink and downlink traffic on certain websites and time-based policies.</td>
</tr>
<tr>
<td>Reporting</td>
<td>The solution offers real-time reporting and integrates with third-party reporting packages.</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>The solution allows and blocks end users from viewing websites from a variety of different categories.</td>
</tr>
<tr>
<td>Real-Time Inbound and Outbound Malware Detection</td>
<td>The solution can detect the traffic of inbound and outbound malware for multiple payload types and across multiple threat vectors.</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 SWG 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.

---

**Advanced Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>What we looked for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic URL Categorization</td>
<td>The solution performs real-time unknown URL categorization supported by an out-of-the-box library of policies.</td>
</tr>
<tr>
<td>Advanced URL Filtering</td>
<td>The solution supports real-time reputation filtering including Secure Socket Layer (SSL) inspection and/or certificate validation.</td>
</tr>
<tr>
<td>Advanced Malware Detection</td>
<td>Inspection of executable files and a behavioral analysis engine performing real-time analysis of web objects using browser code emulation.</td>
</tr>
<tr>
<td>Applications Control</td>
<td>The solution supports a breadth of enforcement actions across web-based applications.</td>
</tr>
<tr>
<td>Advanced Applications Control</td>
<td>The solution provides ICAP support, anti-circumvention support, and an auto-record function of all traffic session details.</td>
</tr>
<tr>
<td>DLP Functionality</td>
<td>The solution provides DLP functionality consisting of sensitive data detection with multiple enforcement actions.</td>
</tr>
</tbody>
</table>

For an explanation of how Advanced Features are determined, see [Information Presentation – Feature Ranks (Stoplights)](information-presentation---feature-ranks-stoplights) in the Appendix.
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.

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>What we looked for:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration</td>
<td>The solution supports integration with NAC, SIEM and AD or LDAP product offerings.</td>
</tr>
<tr>
<td>Mobile Device Support</td>
<td>Multiple OSes are supported and a guest registration portal is supported for public or guest internet access.</td>
</tr>
<tr>
<td>Rule-Based Policy Engine</td>
<td>The solution comes out of the box with a library of customizable policies covering device type, user ID/user group, and multiple attributes.</td>
</tr>
<tr>
<td>Reporting</td>
<td>Role-based administration with a customizable dashboard, reporting engine integration, and out-of-the-box compliance templates.</td>
</tr>
</tbody>
</table>
Each vendor offers a different feature set; concentrate on what your organization needs

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Barracuda</td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
</tr>
<tr>
<td>Blue Coat</td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="yellow" alt="Feature partially present/ pending" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
</tr>
<tr>
<td>Cisco</td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="yellow" alt="Feature partially present/ pending" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
</tr>
<tr>
<td>ContentKeeper</td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="yellow" alt="Feature partially present/ pending" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
</tr>
<tr>
<td>McAfee</td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="red" alt="Feature absent" /></td>
<td><img src="yellow" alt="Feature partially present/ pending" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="red" alt="Feature absent" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
</tr>
<tr>
<td>iboss</td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
<td><img src="green" alt="Feature fully present" /></td>
</tr>
</tbody>
</table>

**Legend**
- ![Feature fully present](green) = Feature fully present
- ![Feature partially present/ pending](yellow) = Feature partially present/pending
- ![Feature absent](red) = 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)

|--------------------|-----------------------------|------------------------|-----------------------|----------------------|------------------------|------------------|-------------|-----------------------|--------------------------|----------|

For an explanation of how Advanced Features are determined, see Information Presentation – Feature Ranks (Stoplights) in the Appendix.
Complete detection, control, and applicability of your web usage complemented by granular visibility is needed today.

The broadest feature functionality is required for total risk management of web usage.

1 Total Risk Management

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.

Exemplary Performers

iboss provides complete malware detection using behavioral data anomaly detection, file sandboxing, and Kaspersky supported scanning all based on a 65K port awareness. Leveraged partnerships allow MDM and web security in one platform.

ContentKeeper offers a high speed, fault tolerant transparent bridge that is scalable. Mobile/BYOD, application/social media, and browser controls supported by Streaming Antivirus, behavioral analysis, browser and window sandboxing mitigate total web risks.

Barracuda offers an integrated solution through ICAP support. Features like SSL inspection, sandboxing, and URL manipulation, in addition to robust social media and application controls, all work to provide overall strong detection and web risk management.

For an explanation of how Scenarios are determined, see Information Presentation – Scenarios in the Appendix.
Securing web usage for most organizations is aimed at maintaining privacy and protecting data.

SSL inspection, advanced malware detection, and DLP capabilities are needed to maintain privacy and protection from web-based threats.

**Exemplary Performers**

iboss provides DLP by blending techniques, including integrated IDPS technology, sandboxing, and Kaspersky AV. Behavioral anomaly technology allows profiling of infrastructure and a heuristic data focus that protect against persistent threats.

ContentKeeper appliances support the ability to decode and analyze SSL traffic, allowing built-in DLP functionality to detect keywords embedded in documents or files. Bypassing capabilities of banking and other highly sensitive sites allows additional privacy protection.

Websense ported its DLP product’s functionality into the WSGA and specifically adapted it to address data theft and leakage at the web gateway. 1,700 pre-defined data classifiers and compliance templates allow quick data protection to customers.

**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.
Organizations that have a public-facing physical presence must secure web usage for their guests

Major mobile operating system support and a robust guest user login portal with credential authentication is needed for guest Wi-Fi support.

**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.

*Public Wi-Fi capable (Café, airport, university, etc.)*

*Known guest environments suitable*

*Closed network applicable (little to no guests)*

For an explanation of how Scenarios are determined, see Information Presentation – Scenarios in the Appendix.
This content security specialist vendor went public in November 2013

Champion

Product: Barracuda Web Filter
Employees: 1,200
Headquarters: Campbell, CA
Website: www.barracuda.com
Founded: 2003
Presence: NYSE: CUDA

Overview

• Barracuda is a strong security software vendor focusing on the mid-market and constrained IT resource organizations. The Barracuda Web Filter can be deployed as a physical or virtual appliance and provides strong web protection.

Strengths

• Barracuda has unique business relationships with technology partners for AV (Avira), advanced malware (Lastline), WLAN (Meru, Ruckus), and URL filtering (DeSvio, Malwarebytes).
• The Web Filter is supported by Barracuda Central: a threat intelligence for real-time protection of the latest threats.
• SSL inspection can be customized for specific blocking.
• Barracuda works closely with wireless access point vendors in order to support web filtering integration and the seamless passing of authentication information to the Web Filter.

Challenges

• Although having strong threat protection, Barracuda only allows the use of open source ClamAV or newly added Avira as an antivirus engine. Internal development of signatures does occur but with relatively less dedicated resources from Barracuda when compared to other vendors in this VL.
• The Barracuda Web Filter does not support dynamic URL categorization.

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

Pricing provided by vendor
Barracuda had worked hard to gain trusted vendor status through strong products with quick time to value.

**Vendor Landscape**

**Value Index**

100
1st out of 12

**Silo Solution**

The solution does not integrate with other security solutions.

**Integration**

The solution can integrate with either/or NAC, SIEM, DLP, and authentication server.

**On-Premise Appliance**

- NAC, SIEM, DLP, AD, and other LDAP servers

**Cloud-Based Deployment**

- NAC, SIEM, DLP, AD, and other LDAP servers

**Hybrid Deployment**

- NAC, SIEM, DLP, AD, and other LDAP servers

**Features**

- Dynamic URL Categorization
- Advanced URL Filtering
- Advanced Malware Det.
- Applications Control
- Advanced Appl. Control
- DLP Functionality
- Integration
- Mobile Device Support
- Rule-Based Policy Engine
- Reporting

**Info-Tech Recommends:**

With a strong feature offering, Barracuda is a good candidate for SMBs and enterprise clients. Historical performance in education and government industries are the main customers that should be shortlisting Barracuda. Recent business partnerships and integrations to increase value should cause existing clients of these vendors to take notice. Price conscious customers should shortlist Barracuda.
Trend Micro is moving to provide complete user protection across devices, applications, or the network.

**Champion**

- **Product:** InterScan Web Security (IWS)
- **Employees:** 5,217
- **Headquarters:** Tokyo, Japan
- **Website:** [www.trendmicro.com](http://www.trendmicro.com)
- **Founded:** 1988
- **Presence:** TYO: 4704

**Overview**

- Trend Micro offers on-premise, in the cloud, or hybrid deployment models with a single management console to manage and report. Trend Micro is a mature content security vendor with primary focuses of email and web security protection.

**Strengths**

- A highly connected gateway, the IWS malware detection is supported by Trend Micro’s reputation database (cloud-based Smart Protection Network) and remote user remediation is supported by Trend Micro’s Damage Cleanup Services.
- HTTP manipulation and support for over 1,000 protocols and applications including IM, P2P, social networking, and streaming media provide advanced application controls.
- Heuristic-based approaches and vulnerability exploit rules detect zero day attacks.

**Challenges**

- Discrepancies exist between the cloud service and IWS around functionality such as DLP integration with threat sandboxing.
- To perform sandboxing and adaptive blacklisting, Trend Micro’s “Deep Discovery” solution must be integrated.
- IWS has native DLP capabilities but is only available as an additional license.

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

Pricing provided by vendor
Trend Micro is a well established player in the SWG market offering total risk management of web activity.

**Vendor Landscape:**
- **Trend Micro** is a well established player in the SWG market offering total risk management of web activity.

**Value Index:**
- **92**
- 2nd out of 12

**Vendor:**
- **Info-Tech Recommends:** A strong feature-rich product, Trend Micro is a good candidate for any high demand security organization. With a major focus on content security such as web and email, Trend Micro is a good candidate for organizations with data or malware concerns or for organizations that already have a strategic relationship with the company.
Cisco offers a strong on-premise SWG and cloud-based SWG service but without unified management

**Champion**

Product: Cisco Web Security Appliance (WSA)
Employees: 63,000+
Headquarters: San Jose, CA
Website: [www.cisco.com](http://www.cisco.com)
Founded: 1984
Presence: NASDAQ: CSCO

**Overview**

- Cisco’s primary web filtering capabilities came from the acquisition of IronPort in 2007. Since then, it has developed a strong secure web gateway that is backed by the vendor strength of Cisco.

**Strengths**

- Cisco provides advanced threat detection from two complementary technologies: Advanced Malware Protection (AMP) and Cognitive Threat Analytics (CTA). File reputation sandboxing and behavioral analysis of web browsing traffic are performed on-premise and in the cloud respectively by the two technologies.
- Cisco provides holistic network security through integration with Cisco security and network technologies.
- The AnyConnect client supports Windows, OS X, Apple iOS, Android, Windows Phone 8, and BlackBerry.

**Challenges**

- High risk profile organizations needing advanced reporting require a Cisco version of Splunk at extra cost.
- Lacks visibility into outbound malware detection for prioritized remediation in reporting and dashboards.
- Cisco does not offer a unified management system for on-premise WSA and Cloud Web Security Service.
Cisco is always a strong security vendor with strategic opportunities outside of security technologies.

**Vendor Landscape:**

- **Cisco:** Strong security vendor with strategic opportunities outside of security technologies.
- **Value Index:** 48 (8th out of 12)

**Product Features:**

- **Overall Features:**
  - **Interface:** 3
  - **Afford.:** 3
  - **Arch.:** 2
- **Vendor Viability:** 4
- **Vendor Focus:** 4
- **Vendor Support:** 4
- **Vendor Sales:** 4

**Silo Solution:**

- **On-Premise Appliance:**
  - The solution does not integrate with other security solutions.
- **Cloud-Based Deployment:**
  - The solution can integrate with either/or NAC, SIEM, DLP, and authentication server.
- **Hybrid Deployment:**
  - The solution can integrate with SIEM, DLP, AD, and other LDAP servers

**Integration:**

- **SIEM, DLP, AD, and other LDAP servers**
- **AD**
- **SIEM, DLP, AD, and other LDAP servers**

**Features:**

- **Dynamic URL Categorization**
- **Advanced URL Filtering**
- **Advanced Malware Det.**
- **Applications Control**
- **Advanced Appl. Control**
- **DLP Functionality**
- **Integration**
- **Mobile Device Support**
- **Rule-Based Policy Engine**
- **Reporting**

**Info-Tech Recommends:**

Cisco offers a robust and scalable enough product to be a shortlist candidate for most mid-sized to large enterprises. Cisco Cloud Web Security enhances network infrastructure by using its built-in connector capability to integrate numerous Cisco products, enabling ecosystem and strategic advantages, making it a good shortlist candidate for any sized organization.
Symantec offers a mid-range SWG suitable for average security requirements

**Market Pillar**

- **Product:** Symantec Web Gateway (SWG)
- **Employees:** 20,850
- **Headquarters:** Mountain View, CA
- **Website:** [www.symantec.com](http://www.symantec.com)
- **Founded:** 1982
- **Presence:** NASDAQ: SYMC

**Overview**

- Symantec has a strong reputation for antivirus and web filtering products. The SWG is a scalable platform that protects organizations against various threats, including Web 2.0 threats such as spyware, botnets, or malicious URLs.

**Strengths**

- Powered by Insight (Symantec’s reputation-based malware filtering technology supported by intelligence from 210 million systems), the SWG is able to perform advanced malware analysis.
- Symantec has partnered with Check Point Software, Cisco, and Palo Alto networks to share threat detection information that can be integrated into Symantec endpoint protection software.
- Symantec is able to deliver end-to-end protection through having one of the largest security product offerings of any vendor.

**Challenges**

- SWG does not support on appliance sandboxing or behavioral analysis by browser code emulation. Sandboxing is roadmap though and malware detection is supported.
- Dynamic classification for unknown URLs is not supported.
- Although web filtering is supported for the iPhone, iPad, and Macintosh mobile devices, it is not tested and can be unreliable.
- The SWG can scan HTTPS/SSL traffic only in proxy mode and when all traffic from end users is being forced through the proxy.

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

Pricing solicited from public sources
Strong vendor stability and relationship leverage are some of the biggest reasons to choose Symantec

**Vendor Landscape**

<table>
<thead>
<tr>
<th>Overall</th>
<th>Features</th>
<th>Interface</th>
<th>Afford.</th>
<th>Arch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/5</td>
<td>1/5</td>
<td>3/5</td>
<td>2/5</td>
<td>3/5</td>
</tr>
</tbody>
</table>

**Product**

<table>
<thead>
<tr>
<th>Silo Solution</th>
<th>On-Premise Appliance</th>
<th>Cloud-Based Deployment</th>
<th>Hybrid Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>The solution does not integrate with other security solutions.</td>
<td></td>
<td>DLP, AD, LDAP</td>
<td>NA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Integration</th>
<th>The solution can integrate with either/or NAC, SIEM, DLP, and authentication server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP, AD, LDAP</td>
<td></td>
</tr>
</tbody>
</table>

**Value Index**

50
7th out of 12

**Features**

- Dynamic URL Categorization
- Advanced URL Filtering
- Advanced Malware Det.
- Applications Control
- Advanced Appl. Control
- DLP Functionality
- Integration
- Mobile Device Support
- Rule-Based Policy Engine
- Reporting

**Info-Tech Recommends:**

Symantec designed its SWG to have broad applicability for most enterprise customers. Existing Symantec customers can leverage their relationship and are good shortlist candidates. Symantec offers superb detection and will be increasing this capability with the recent partnerships with Check Point Software, Cisco, and Palo Alto Networks. Organizations with basic security needs should shortlist Symantec.
McAfee excels in malware detection through full browser emulation capabilities

<table>
<thead>
<tr>
<th>Market Pillar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product: McAfee Web Gateway (MWG)</td>
</tr>
<tr>
<td>Employees: 7,000</td>
</tr>
<tr>
<td>Headquarters: Santa Clara, CA</td>
</tr>
<tr>
<td>Website: <a href="http://www.mcafee.com">www.mcafee.com</a></td>
</tr>
<tr>
<td>Founded: 1987</td>
</tr>
<tr>
<td>Presence: NASDAQ: INTC (Intel)</td>
</tr>
</tbody>
</table>

**Overview**
- McAfee, owned by Intel, is the second largest security software vendor offering a family of on-premise SWG appliances (McAfee Web Gateway [MWG]) and a cloud-based SWG service (SaaS Web Protection).

**Strengths**
- MWG scans a webpage’s active content using browser code emulation to understand its behavior and predict its intent.
- MWG combines intelligence from its malware engine and cloud-based McAfee Global Threat Intelligence to support advanced protection. Malware detection sensitivity can be adjusted.
- Integration with McAfee Data Loss Prevention enables secure outbound traffic through scanning of user generated content.
- Robust application controls through HTTP manipulation allows the removal of selected web application functions.

**Challenges**
- The cloud-based SWG service (SaaS Web Protection) does not offer the same level of policy granularity available on-premise.
- Wi-Fi support is not featured through a guest registration portal with authentication limiting use for public or guest access. This functionality is performed by McAfee’s NAC solution.
- Mac OS X is still not supported.
- McAfee has consistently received low customer satisfaction for technical support and policy integration across components.

3 year TCO for this solution falls into pricing tier 7, between $100,000 and $250,000
Intel is keen to grow McAfee and see greater cross product value with existing customers

**Value Index**

37

9th out of 12

**Info-Tech Recommends:**

McAfee commands a strong reputation and brand value within the security software market. Existing McAfee customers should shortlist MWG, especially those that are already using McAfee ePolicy Orchestrator. McAfee is able to meet high security demand scenarios but requires strong technical prowess and additional technologies to receive the full enterprise value that is offered by other vendors.
Websense started in web filtering and supports strong data protection and privacy

**Market Pillar**

- **Product:** Web Security Gateway Anywhere
- **Employees:** 1,600
- **Headquarters:** San Diego, CA
- **Website:** [www.websense.com](http://www.websense.com)
- **Founded:** 1994
- **Presence:** Privately Held

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

- Pricing provided by vendor

**Overview**

- Websense is a content-focused security software vendor with an established market position in web security. Websense’s main focus is the TRITON solution: a unified threat protection solution covering web, email, data, and mobile security.

**Strengths**

- The TRITON management console provides a dynamic solution for central policy and reporting management across security products including the WSG.
- Websense Advanced Classification Engine (ACE) is a composite scoring classification model able to perform real-time heuristics.
- The optional ThreatScope add-on to WSG provides valuable behavioral sandboxing analysis of files and objects.
- Advanced data theft defenses include OCR for detection of sensitive data contained in images, geo location awareness, custom encryption detection, and drip DLP for low profile theft.

**Challenges**

- WSG does not provide canned compliance-specific reports and lacks integration capabilities into third-party reporting engines.
- Automatic recording of session traffic and activity is not supported, limiting the ability to perform forensics into incident details or provide live granular visibility into traffic.

**Pricing**

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

- Pricing provided by vendor

- $1

- $1M+
Websense is refocusing on content security, including services that protect email and other data

**Vendor Landscape**

- **Websense**
  - Focus: Content Security
  - Value Index: 10 (12th out of 12)

**Product Features**

- **Silos Solution**
  - The solution does not integrate with other security solutions.

**Integration**

- The solution can integrate with either/or NAC, SIEM, DLP, and authentication server.

**Deployment Options**

- **On-Premise Appliance**
  - SIEM, DLP, AD, LDAP servers

- **Cloud-Based Deployment**
  - SIEM, DLP, AD, LDAP servers

- **Hybrid Deployment**
  - SIEM, DLP, AD, LDAP servers

**Features**

- Dynamic URL Categorization
- Advanced URL Filtering
- Advanced Malware Det.
- Applications Control
- Advanced Appl. Control
- DLP Functionality
- Integration
- Mobile Device Support
- Rule Based Policy Engine
- Reporting

**Value Index**

10 (12th out of 12)

**Info-Tech Recommends:**

A subscription-based pricing model may make Websense too expensive for price conscious or limited organizations. Websense focuses mainly on the TRITON management system to provide a high level of web security and threat protection in a unified architecture. Those considering integration of web, email, data, and mobile security should shortlist Websense. Existing customers should shortlist Websense.
Sophos is most commonly known for their endpoint protection platform (EPP)

**Market Pillar**
- **Product:** Sophos Web Appliance (SWA)
- **Employees:** 1,700
- **Headquarters:** Oxford, UK & Burlington, MA
- **Website:** www.sophos.com
- **Founded:** 1985
- **Presence:** Privately Held

**Overview**
- Sophos is an established and mature player in the SWG market. Sophos offers a range of gateways through in-house development and its acquisition of Astaro in 2011. It offers a dedicated appliance for web security or an integrated option with its UTM.

**Strengths**
- Sophos supports a high performance web malware engine performing inspection in real time. Browser code emulation, behavioral analysis, and non-performance hindering HTTP and HTTPS scanning provide strong protection. SophosLabs continuously updates the SWA's threat intelligence via the cloud.
- Sophos's EPP integrates with its SWA and UTM, providing strong web protection for offsite users.
- Sophos has a high level of usability due to a streamlined GUI supported by intuitive policy configuration and help functions.

**Challenges**
- The SWA offers little dynamic categorization of uncategorized URLs, primarily only for detection of anonymizer sites.
- ICAP is not supported for the SWA, limiting integration capabilities with other security technologies.
- Social media controls lack in breadth of control options. Fine grained controls are road mapped for end of 2014.
- Limited on box reporting capabilities around analytics or regulatory compliance limit use for high risk profiles without a SIEM.

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

Pricing provided by vendor
Sophos offers an easy to use product that is lacking in robust application controls

**Vendor Landscape**

<table>
<thead>
<tr>
<th>Vendor Landscape</th>
<th>Product</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>Features</td>
<td>Interface</td>
</tr>
<tr>
<td><img src="chart.png" alt="Chart" /></td>
<td><img src="chart.png" alt="Chart" /></td>
<td><img src="chart.png" alt="Chart" /></td>
</tr>
</tbody>
</table>

**Value Index**

- **31**
- 11th out of 12

**Silo Solution**

- The solution does not integrate with other security solutions.

**Integration**

- The solution can integrate with either/or NAC, SIEM, DLP, and authentication server.

<table>
<thead>
<tr>
<th>On-Premise Appliance</th>
<th>Cloud-Based Deployment</th>
<th>Hybrid Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD, LDAP, SIEM, UTM (some DLP native)</td>
<td>UTM Secure Web Gateway</td>
<td>NA</td>
</tr>
</tbody>
</table>

**Features**

- Dynamic URL Categorization
- Advanced URL Filtering
- Advanced Malware Det.
- Applications Control
- Advanced Appl. Control
- DLP Functionality
- Integration
- Mobile Device Support
- Rule-Based Policy Engine
- Reporting

**Info-Tech Recommends:**

Sophos is a strong overall security software vendor but lacks in some advanced functions required by high security demand organizations. Sophos is a good candidate for small to mid-sized organizations, especially those already using its EPP solution. Strong GUI and mobile support make Sophos a good candidate for non-technically expertise organizations.
Trustwave gained its SWG functionality through acquisition

**Innovator**

- **Product:** Trustwave Secure Web Gateway
- **Employees:** 1,100
- **Headquarters:** Chicago, IL
- **Website:** [www.trustwave.com](http://www.trustwave.com)
- **Founded:** 1996
- **Presence:** Privately Held

**Overview**

- Trustwave is a security vendor specializing in compliance and data protection. It entered the SWG market with the acquisition of M86 Security in 2012.

**Strengths**

- Mobile devices and BYOD are supported with automated responses due to integration of SWG with Trustwave’s NAC, DLP, and SIEM products.
- SWG supports an “X-Ray Mode” for testing new policies on live traffic without disruption of ongoing business.
- Real-time analysis of web objects is supported by strong browser code emulation.
- SWG enforcement of security policies and rules support various regulations.

**Challenges**

- Mobile support lacks multi-tenant cloud-based SWG service as well as any guest Wi-Fi support.
- Dynamic classification for unknown URLs is not supported.
- Anti-circumvention functionality for blocking port evasive applications, such as BitTorrent, is not supported.
- Although the reporting dashboard is customizable, it is weaker in providing strong web visibility when compared to other vendors.
- Trustwave’s compliance focus can stifle other scenario expertise.

---

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

Pricing solicited from public sources
Trustwave offers a strong SWG that can be augmented by their compliance and managed security service focuses.

**Vendor Landscape**

<table>
<thead>
<tr>
<th>Overall</th>
<th>Features</th>
<th>Interface</th>
<th>Afford.</th>
<th>Arch.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Product**

**Silo Solution**

The solution does not integrate with other security solutions.

**Integration**

The solution can integrate with either/or NAC, SIEM, DLP, and authentication server.

<table>
<thead>
<tr>
<th>On-Premise Appliance</th>
<th>Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AD, LDAP, Trustwave’s NAC, SIEM, and DLP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cloud-Based Deployment</th>
<th>Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AD, LDAP, Trustwave’s NAC, SIEM, and DLP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hybrid Deployment</th>
<th>Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AD, LDAP, Trustwave’s NAC, SIEM, and DLP</td>
</tr>
</tbody>
</table>

**Features**

- Dynamic URL Categorization
- Advanced URL Filtering
- Advanced Malware Det.
- Applications Control
- Advanced Appl. Control
- DLP Functionality
- Integration
- Mobile Device Support
- Rule-Based Policy Engine
- Reporting

**Value Index**

<table>
<thead>
<tr>
<th>76</th>
</tr>
</thead>
</table>

3rd out of 12

**Info-Tech Recommends:**

Trustwave’s main focus is compliance and managed security services. Any organizations interested in either of those should shortlist Trustwave. Major compliance with regulatory initiatives such as SOX (COBIT) DS5, PCI DSS 1.1, GLB Act, HIPAA, and FISMA is supported. An almost dedicated focus to these types of customers may deter full support or value from other use cases.
ContentKeeper is relatively new to North America but has had impressive enterprise experience in Australia

**Innovator**

- **Product:** Security Internet Gateway (CK-SIG)
- **Employees:** 50
- **Headquarters:** Canberra ACT, Australia, & Orange, CA, USA
- **Website:** [www.contentkeeper.com](http://www.contentkeeper.com)
- **Founded:** 1999
- **Presence:** Privately Held

**Overview**

- ContentKeeper is a dedicated SWG vendor from Australia with some corporate and mostly government and education customers. It offers a family of SWG scalable solutions with advanced features designed for large enterprises.

**Strengths**

- CK-SIG supports sandboxing to execute suspicious files in a virtualized Windows environment. Detailed reports can be generated for each item analyzed.
- Access policies for mobile devices and users are supported through BYOD functionality with agents available for off-network devices. Windows, OS X, iOS, Linux, Chrome OS, and Android are supported.
- ContentKeeper appliances support the ability to decode and analyze SSL traffic for full decryption and inspection.

**Challenges**

- ContentKeeper is a relatively smaller and unproven vendor without industry recognition for malware analysis and detection.
- CK-SIG’s graphical user interface (GUI) lacks in ease of use and intuitiveness when compared to other vendors in this VL.
- CK-SIG does not support ICAP limiting integration capabilities.

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

Pricing provided by vendor
ContentKeeper focuses only on web security and filtering solutions

<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>
<tr>
<td>INNOVATOR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHAMPION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMERGING PLAYER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MARKET PILLAR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Value Index**

70

5th out of 12

**Info-Tech Recommends:**

ContentKeeper has a focus on developing high speed, scalable, fault tolerant technologies specifically for large enterprise customers like government and education. Although having less experience with private companies, ContentKeeper can be a shortlist candidate for these cases. With not fully seasoned anti-malware capabilities, potential customers should evaluate these capabilities to confirm suitability.

**Features**

- Dynamic URL Categorization
- Advanced URL Filtering
- Advanced Malware Det.
- Applications Control
- Advanced Appl. Control
- DLP Functionality
- Integration
- Mobile Device Support
- Rule-Based Policy Engine
- Reporting
iboss usually deploys only 1/3 of hardware compared to competitors

**Innovator**

- **Product:** iboss Secure Web Gateway (SWG)
- **Employees:** 108
- **Headquarters:** San Diego, CA
- **Website:** [www.iboss.com](http://www.iboss.com)
- **Founded:** 2004, Entered market 2008
- **Presence:** Privately Held

---

**Overview**

- iboss, formerly Phantom Technologies, is a family of on-premise, hybrid, and cloud platforms. The SWG offers various advanced and unique features that iboss developed from spending five years in research and development before going to market.

**Strengths**

- iboss supports unique patent pending 3D security which allows policies to be dynamically applied and changed based on the user’s physical location in an organization (e.g. heavier restrictions while in an R/D lab vs. company break room).
- iboss is an Apple and Samsung Enterprise Partner, providing deep visibility into those platforms.
- iboss supports a unique video screen capture to help confirm intentional vs. unintentional user violations.
- iboss utilizes a closed loop real-time database sync with the cloud.

**Challenges**

- As a dedicated SWG vendor, iboss has limited strategic vendor value derived from getting other network security technologies from the same vendor. That said, numerous integration options are available for security products from other vendors.

---

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

Pricing provided by vendor
Through years of R&D, iboss offers one of the most advanced and forward thinking feature sets.

**Vendor Landscape**

Through years of R&D, iboss offers one of the most advanced and forward thinking feature sets.

**Vendor Landscape**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Overall</th>
<th>Features</th>
<th>Interface</th>
<th>Afford.</th>
<th>Arch.</th>
<th>Viability</th>
<th>Focus</th>
<th>Support</th>
<th>Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>iboss</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

**Value Index**

68

6th out of 12

**Silo Solution**

The solution does not integrate with other security solutions.

**Integration**

The solution can integrate with either/or NAC, SIEM, DLP, and authentication server.

**On-Premise Appliance**

- NAC, AD, eDirectory, LDAP, Google LDAP, Oracle ID, SIEM, DLP

**Cloud-Based Deployment**

- NAC, AD, eDirectory, LDAP, Google LDAP, Oracle ID, SIEM, DLP

**Hybrid Deployment**

- NAC, AD, eDirectory, LDAP, Google LDAP, Oracle ID, SIEM, DLP

**Features**

- Dynamic URL Categorization
- Advanced URL Filtering
- Advanced Malware Det.
- Applications Control
- Advanced Appl. Control
- DLP Functionality
- Integration
- Mobile Device Support
- Rule-Based Policy Engine
- Reporting

**Info-Tech Recommends:**

Historic focus on K-12 market has developed strong features with a large customer base. Unique feature offerings (3D scanning, image scrubbing, two year transaction data retention, browser based searching, full screen playback, etc.) make iboss a good shortlist candidate for organizations with unique or special security requirements. As well, iboss is a good candidate for most mid to large enterprises.
An aggressive acquisition strategy and high revenue growth poises Blue Coat for major developments

**Emerging Player**

- **Product:** ProxySG Secure Web Gateway*
- **Employees:** 1,473
- **Headquarters:** Sunnyvale, CA
- **Website:** www.bluecoat.com
- **Founded:** 1996
- **Presence:** Privately Held

**Overview**

- Blue Coat is a long time player in the web filtering and antivirus market spaces. Blue Coat is developing its Web Filter toward a more holistic lifecycle defense against advanced targeted attacks.

**Strengths**

- Blue Coat supports one of the industry’s most robust proxy supporting numerous protocols, authentication and directory integration, and Online Certificate Status Protocol (OCSP).
- Extensive reporting functionality with canned reports are supported for both on-premise and cloud-based deployments.
- ProxySG is supported by Blue Coat’s global threat intelligence WebPulse: a resource of some 75 million users.
- Blue Coat has expanded capabilities into advanced malware analysis, sandboxing, and SSL inspection through acquisition.

**Challenges**

- The ProxyAV only utilizes signature-based detection supported from four different antivirus partnered engines.

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

Pricing provided by vendor

*Blue Coat recommends their cloud-based SWG for mid-market sized enterprises. Both the on-premise and cloud options have similar functionality only differing in policy configuration. The cloud option has a significantly lower total cost of ownership than on-premise as well.
Once dedicated to web security, Blue Coat now offers a huge array of security products

### Vendor Landscape

<table>
<thead>
<tr>
<th>Vendor Landscape</th>
<th>Overall</th>
<th>Features</th>
<th>Interface</th>
<th>Afford.</th>
<th>Arch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue Coat</td>
<td>🌐</td>
<td>🌐</td>
<td>🌐</td>
<td>🌐</td>
<td>🌐</td>
</tr>
</tbody>
</table>

### Value Index

36

10th out of 12

### Product

<table>
<thead>
<tr>
<th>Silo Solution</th>
<th>Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>The solution does not integrate with other security solutions.</td>
<td>The solution can integrate with either/or NAC, SIEM, DLP, and authentication server.</td>
</tr>
</tbody>
</table>

#### On-Premise Appliance

- NAC, SIEM, DLP, AD, and other LDAP servers

#### Cloud-Based Deployment

- Transparent AD integration

#### Hybrid Deployment

- NAC, SIEM, DLP, AD, and other LDAP servers

### Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic URL Categorization</td>
<td>🌐</td>
</tr>
<tr>
<td>Advanced URL Filtering</td>
<td>🌐</td>
</tr>
<tr>
<td>Advanced Malware Det.</td>
<td>🌐</td>
</tr>
<tr>
<td>Applications Control</td>
<td>🌐</td>
</tr>
<tr>
<td>Advanced Appl. Control</td>
<td>🌐</td>
</tr>
<tr>
<td>DLP Functionality</td>
<td>🌐</td>
</tr>
<tr>
<td>Integration</td>
<td>🌐</td>
</tr>
<tr>
<td>Mobile Device Support</td>
<td>🌐</td>
</tr>
<tr>
<td>Rule-Based Policy Engine</td>
<td>🌐</td>
</tr>
<tr>
<td>Reporting</td>
<td>🌐</td>
</tr>
</tbody>
</table>

### Info-Tech Recommends:

Blue Coat is a strong candidate for large organizations, especially those with multiple locations or branch offices. Historic experience has been with large enterprises. A focus on fewer and better alarms being triggered is aimed at more resource constrained organizations. Any organization looking to take advantage of an ecosystem of security products from one vendor should shortlist Blue Coat.
Zscaler is the largest global security cloud vendor with over 100 data centers providing near zero latency

**Emerging Player**

<table>
<thead>
<tr>
<th>Product:</th>
<th>Zscaler Internet Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees:</td>
<td>400</td>
</tr>
<tr>
<td>Headquarters:</td>
<td>San Jose, CA</td>
</tr>
<tr>
<td>Website:</td>
<td><a href="http://www.zscaler.com">www.zscaler.com</a></td>
</tr>
<tr>
<td>Founded:</td>
<td>2008</td>
</tr>
<tr>
<td>Presence:</td>
<td>Privately Held</td>
</tr>
</tbody>
</table>

**Overview**

- Zscaler is a cloud-based vendor with a broad internet security platform. Zscaler leverages a Direct-to-Cloud network to provide the industry’s only 100% cloud-delivered SWG. Impressive growth and rapid product development are gaining market attention.

**Strengths**

- Zscaler offers numerous cloud-based benefits not traditionally seen in the SWG market: no appliances, software, or clients; no maintenance; flexible scalability and increased connectivity.
- Web logs can be streamed to an on-premise SIEM.
- Content aware scanning of all traffic augmented by full SSL support and cloud intelligence detects advanced security threats.
- Broad traffic redirection (including Ipsec) and authentication (including SAML) provide flexible deployment options.
- Flash cookies and Kerberos authentication enable agentless authentication for mobile.

**Challenges**

- Zscaler supports PAC files, creating the risk of having compromised PAC files redirect browser traffic to an attacker controlled server. Port evasive applications on endpoints relying on PAC files won’t be forwarded to Zscaler. Other delivery methods exist and are used.
- Zscaler only monitors ports 80 and 443 limiting visibility to non-HTTP/HTTPS protocols.

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

Pricing solicited from public sources
Zscaler’s model is to deliver web security to anyone from anywhere while reducing in-house costs like hardware or staff.

**Vendor Landscape: Secure Web Gateway**

**Value Index**

76

4th out of 12

**Info-Tech Recommends:**

As a cloud-based offering, cloud accepted customers should shortlist Zscaler to realize the benefits from a hosted deployment option. A low price point and minimal management make Zscaler a great shortlist candidate for any small, limited resource, or budget constrained organization. A relatively untested malware detection and concerns with cloud functionality limit its use for high security demand customers.
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.
• Interface: 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.
• Focus: The commitment to both the market-space, as well as to the various sized clients (small, mid-sized, and enterprise clients).
• Support: The ability of the vendor to support its products on a global scale.
• Sales: 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, Focus, Support, Sales) is 100% and the sum of the Product criteria (Features, Interface, 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 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, Focus, Support, Sales) is 100%, and the sum of the product criteria (Features, Interface, 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.

![Harvey Balls Table]

---

Vendor Landscape: Secure Web Gateway

Info-Tech Research Group 48
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.”

<table>
<thead>
<tr>
<th>Features</th>
<th>Feature 1</th>
<th>Feature 2</th>
<th>Feature 3</th>
<th>Feature 4</th>
<th>Feature 5</th>
<th>Feature 6</th>
<th>Feature 7</th>
<th>Feature 8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
<td>Red</td>
<td>Red</td>
<td>Yellow</td>
<td>Red</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

Green means a feature is fully present; red, fully absent.

Yellow shows partial availability (such as in some models in a line).
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, Interface, 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, Interface, 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, it is 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 not 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.
Pricing Scenario

A mid-level retailer with corporate offices on the US west coast, east coast, and Ireland is looking to implement a SIEM solution. The company employs 2200 people. The firm is interested in reducing the effort associated with monitoring, alerting, and responding to security events at the Endpoint, Network, and Datacenter levels. The firm also has 100 retail outlets scattered throughout the US and Europe however all stores are franchised and so out of scope.

The corporate office breakdown is as follows:

**US West Coast (Head Office)**
- Employing 1600 people (70%), the west coast office holds Sales, Finance, Strategy, Marketing, Buyers, and the majority of IT. The IT staff here consists of 45 employees, 3 of which are dedicated security professionals consisting of 1 Security Manager and 2 Security Analysts.

**US East Coast (Satellite)**
- Employing 200 people (10%), the east coast office includes only Sales and Marketing staff.

**Ireland (Satellite)**
- Employing 400 people (20%), the Ireland office employs Buyers and Manufacturing and also a DR facility. Manufacturing consists of 300 employees. The company’s remaining 5 IT staff are located here though none have dedicated security responsibilities.

In terms of the IT infrastructure of the organization, consider the following:

**General Infrastructure**
- Internal network is gigabit throughout.
  - Redundant core routers at all 3 facilities
  - Distribution switches: 80 at Head Office, 10 at East Coast, 20 in Ireland
  - US East Coast office connects to Internet through US West Coast office (H.Q.)
  - Ireland office has its own separate Internet link
- Primarily Microsoft – 70% Virtualized
  - 4 Domain servers (2 at Head Office, 1 at each of the other offices)
  - HA production virtual server cluster at Head Office + separate dev and QA virtual servers in Ireland (also used for DR purposes)
  - Oracle DB on HP-UX dual servers (non-virtual) at the US West Coast office, and a single instance in Ireland.
Pricing Scenario (continued)

° Exchange 2010 (2 servers)
° SharePoint 2010 (single server)
° 700 laptops running Windows 7; 1200 desktops also running Windows 7
• Corporate owned iOS, Android and BlackBerry mobile phones and tablets are allowed to connect to internal network.
• Running a virtualized VOIP system as opposed a traditional PBX.

Security Infrastructure
• Gateway firewalls at each site
• Endpoint & Gateway anti-malware
• Endpoint encryption is implemented on all laptops
• No IDPS
• No holistic DLP solution

Web Content Filtering Expectation
• All employees should be protected by SWG
• URLs which are classified as inappropriate sites by policies should be disallowed
• Employees should be protected from malware infection
• For some social media sites (i.e. Facebook), employees are allowed to visit but not allowed to publish certain sensitive content defined by policies
• Employees are not allowed to send out corporate defined sensitive information (e.g. PII, Credit Card Information, Intellectual Property, etc.)
• SWG should have bandwidth management capability

Support Services
• Gold level support services should include the following:
  ° Technical documentation and guides
• 24/7 Technical support by phone or online