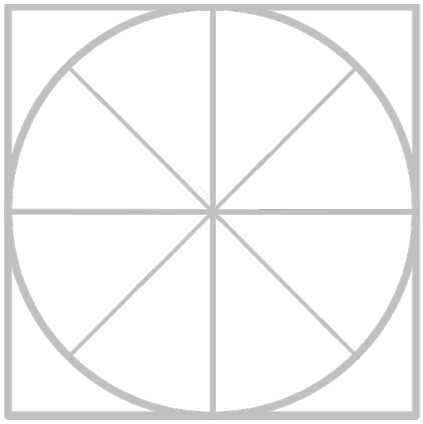
The Radicati Group, Inc.
Palo Alto, CA 94301
Phone: (650) 322-8059
www.radicati.com

THE RADICATI GROUP, INC.

Corporate Web Security - Market Quadrant 2016



An Analysis of the Market for Corporate Web Security Solutions, Revealing Top Players, Trail Blazers, Specialists and Mature Players.

May 2016

TABLE OF CONTENTS

==========

==========

RADICATI MARKET QUADRANTS EXPLAINED

Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

1. ***Top Players*** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as possess a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don't become Top Players overnight. Most of the companies in this quadrant were first Specialists or Trail Blazers (some were both). As companies reach this stage, they must fight complacency and continue to innovate.

2. ***Trail Blazers*** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don't necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for "disrupting" the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

3. ***Specialists*** – This group is made up of two types of companies:

    a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.

    b. Established vendors that offer a niche product.

4. ***Mature Players*** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered "movers and shakers" in this market as they once were.

    a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, they may choose to slow development on existing products.

b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.

c. Companies in this stage will either find new life, reviving their R&D efforts and move back into the Top Players segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market Quadrant. As a vendor continues to develop its product solutions adding features and functionality, it will move vertically along the "y" functionality axis.

The horizontal "x" strategic vision axis reflects a vendor's understanding of the market and their strategic direction plans. It is common for vendors to move in the quadrant, as their products evolve and market needs change.

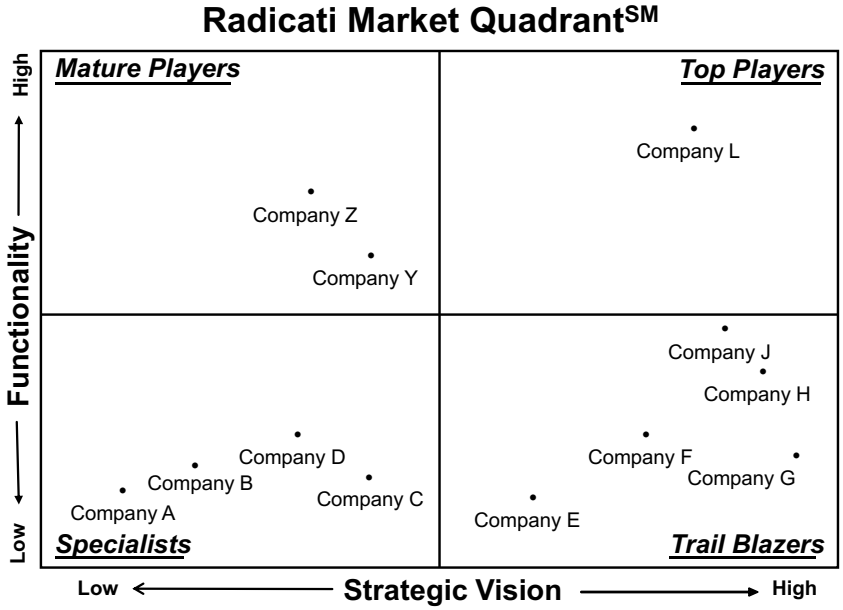


Figure 1: Sample Radicati Market Quadrant

MARKET SEGMENTATION – CORPORATE WEB SECURITY

This edition of Radicati Market Quadrants[SM] covers the "**Corporate Web Security**" segment of the Security Market, which is defined as follows:

- **Corporate Web Security –** this segment includes any software, appliance, or cloud-based service that protects corporate users and networks from Web-based malware, enables organizations to control employee behavior on the Internet, and helps prevent data loss. Some of the leading players in this market are *Barracuda Networks*, *Blue Coat Systems*, *Cisco*, *Clearswift, Forcepoint, iBoss, Intel Security*, *Sophos*, *Symantec, Trend Micro*, *Trustwave*, and *Zscaler*.

- Corporate Web Solutions, today, can be deployed in multiple form factors, including appliances, virtual appliances, cloud services and hybrid models.

- Some web security vendors target both corporate customers, as well as service providers. However, this report looks only at vendor installed base and revenue market share in the context of their corporate business.

- Cloud based and hybrid web security solutions are finding increased popularity due to the growing use of mobile devices and growing remote workforces. Nearly all vendors that previously offered appliances have now added a cloud based option to their portfolio, or are looking to do so in the very near future. Customers often opt for a hybrid model as a stepping stone to a full cloud based solution, or to accommodate different requirements of different kinds of workers (e.g. headquarters vs. roaming workforces).

- Corporate Web Security vendors are increasingly expanding the Data Loss Prevention (DLP) capabilities of their solutions. However, these are often still fairly basic compared to full scale content-aware DLP solutions and most large organizations will typically still deploy a full content-aware DLP solution for increased protection and better adherence to compliance requirements.

- The worldwide revenue for Corporate Web Security solutions is expected to grow from nearly $2.5 billion in 2016, to over $4.2 billion by 2020.

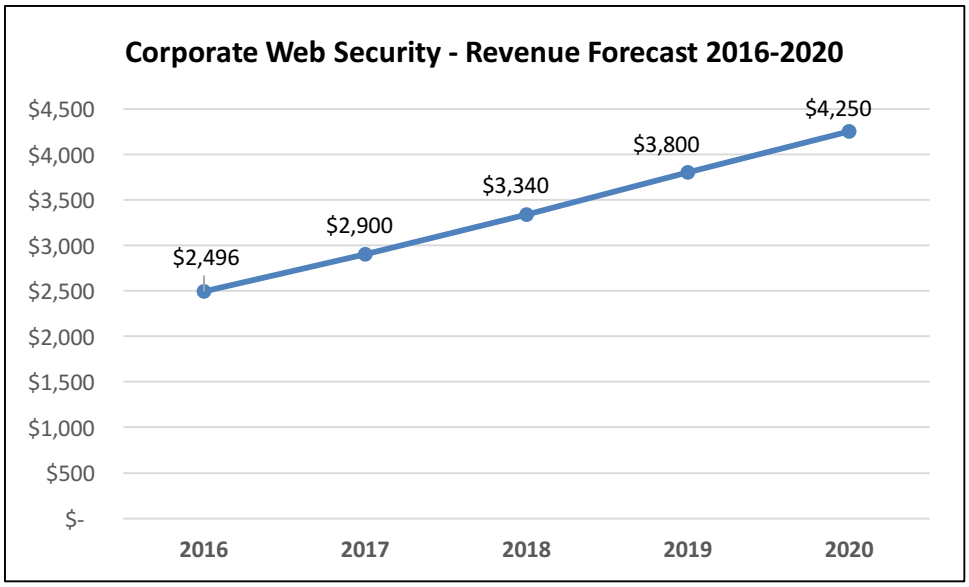


Figure 2: Corporate Web Security Market Revenue Forecast, 2016 – 2020

EVALUATION CRITERIA

Vendors are positioned in the quadrant according to two criteria: *Functionality* and *Strategic Vision*.

Functionality is assessed based on the breadth and depth of features of each vendor's solution. All features and functionality do not necessarily have to be the vendor's own original technology, but they should be integrated and available for deployment when the solution is purchased.

Strategic Vision refers to the vendor's strategic direction, which comprises: a thorough understanding of customer needs, ability to deliver through attractive pricing and channel models, solid customer support, and strong on-going innovation.

Vendors in the *Corporate Web Security* space are evaluated according to the following key features and capabilities:

- ***Deployment Options*** – availability of the solution in different form factors, such as on-premises, appliance and/or virtual appliance, cloud-based services, or hybrid.

- ***Malware detection*** is usually based on signature files, reputation filtering (proactive blocking of malware based on its behavior, and a subsequent assigned reputation score), and proprietary heuristics. The typical set up usually includes multiple filters, one or more best-of-breed signature-based engines as well as the vendor's own proprietary technology. Malware engines are typically updated multiple times a day. Malware can include spyware, viruses, worms, rootkits, and much more.

- ***URL filtering*** helps promote productivity and a malware-free environment by filtering out unwanted websites based on URL. It enables organizations to manage and control the types of websites their employees are allowed to visit. Organizations can block unique websites, or select from pre-screened categories of websites. There are usually multiple categories, ranging from around 10 to 100, that make it easier to manage which types of websites are appropriate for the workplace. Categories often include millions of pre-screened sites, which are updated daily.

- ***Web application controls*** enable organizations to automatically block potentially malicious applications, and/or limit the use of non-work related applications, such as social networks and instant messaging. The granularity of Web application controls can vary from vendor to vendor. The available policies range from binary block/allow to intricate policies that can block/allow specific actions in a given Web application.

- ***Reporting*** lets administrators view activity that happens on the network. Corporate Web Security solutions should offer real-time interactive reports on user activity. Summary views to give an overall view of the state of the network should also be available. Most solutions allow organizations to run reports for events that occurred over the past 12 months, as well as to archive event logs for longer-term access. As many organizations are deploying hybrid solutions that combine on-premises (i.e. appliance based) web security as well as cloud-based web security, it is increasingly important that vendors provide integrated reporting for hybrid environments.

- ***SSL scanning*** was not usually offered as a feature since websites with SSL security were viewed as safe. Now that malware frequently appears on legitimate websites, Web traffic over an SSL connection is also commonly monitored to enforce Web policies.

- ***Directory integration*** can be obtained via Active Directory or a variety of other protocols, such as LDAP. By integrating Web security tools with a corporate directory, organizations can use employees' directory roles to assign and manage Web policies based on a user's function and role in the organization. For example, the marketing staff can be granted full access to social media.

- ***Data Loss Prevention (DLP)*** allows organizations to define policies to prevent loss of sensitive electronic information. There is a range of DLP capabilities that vendors offer in their Corporate Web Security solutions, such as DLP-Lite or Content-Aware DLP. The inclusion of any DLP technology, however, is viewed as an advanced feature.

- ***Mobile device protection*** is increasingly important as workforces become increasingly mobile. Some vendors can protect mobile devices only while they are physically located on-premises. This approach, however, is flawed since mobile devices will inevitably be used on-the-go, away from the office. The protection of mobile devices needs to be addressed in full, preferably with no visible latency and without requiring the mobile traffic to be backhauled

through the corporate VPN.

- ***Bandwidth controls*** allow administrators to completely block bandwidth-hungry sites like YouTube, or they can impose quotas that limit time spent or data consumed. This preserves bandwidth for legitimate traffic and application use. Some vendors also include traffic shaping in their bandwidth control solutions.

- ***Administration*** through an easy-to-use interface is offered by most vendors. The advanced component of a management interface occurs when there is a unified management interface for hybrid deployments. Many vendors still keep cloud-based and on-premises management interfaces separate. As more organizations choose a hybrid deployment model, a unified management experience is a key differentiator.

- ***Granular Web application controls*** can offer intricate controls that go beyond block or allow options. We consider Web application controls to be advanced when the granularity goes beyond binary options for setting policy. It is important to have these detailed policy options for Web applications that are widely used in the enterprise, such as Facebook, YouTube and other social networks.

In addition, for all vendors we consider the following aspects:

- *Pricing* – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a "good value".

- *Customer Support* – is customer support adequate and in line with customer needs and response requirements.

- *Professional Services* – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

Note*: On occasion, we may place a vendor in the Top Player or Trail Blazer category even if they are missing one or more features listed above, if we feel that some other aspect(s) of their solution is particularly unique and innovative.*

MARKET QUADRANT – CORPORATE WEB SECURITY

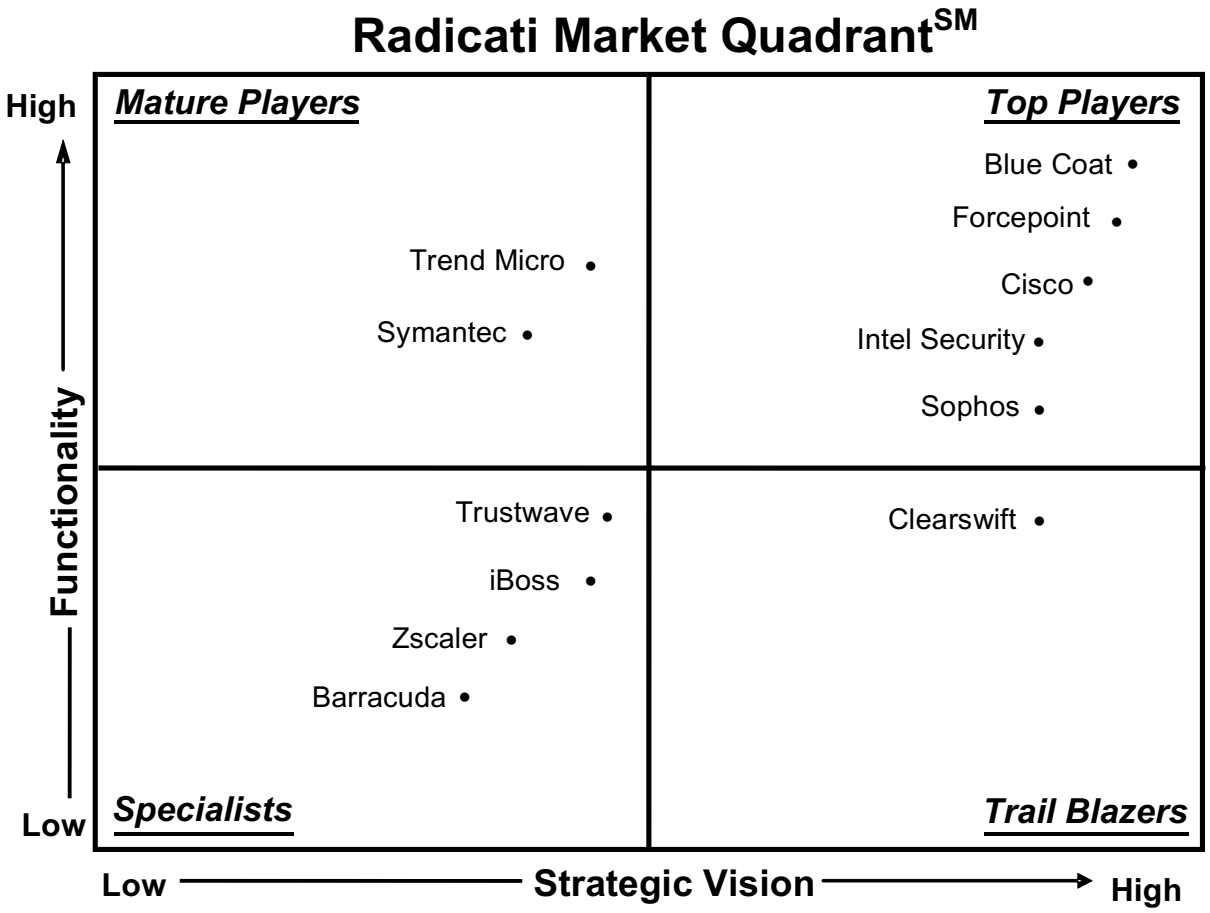


Figure 3: Corporate Web Security Market Quadrant, 2016

· Radicati Market Quadrant℠ is copyrighted May 2016 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT HIGHLIGHTS

- The **Top Players** in the market are *Blue Coat Systems, Forcepoint, Cisco, Intel Security,* and *Sophos***.**
- The **Trail Blazers** quadrant includes *Clearswift*.
- The **Specialists** quadrant includes *Trustwave, iBoss, Zscaler,* and *Barracuda Networks*.
- The **Mature Players** in this market at this time are *Trend Micro* and *Symantec*.

CORPORATE WEB SECURITY - VENDOR ANALYSIS

TOP PLAYERS

BLUE COAT

384 Santa Trinita Ave
Sunnyvale, CA 94085
www.bluecoat.com

SOLUTIONS

Blue Coat is a provider of network security and threat detection technology, including Web Security, Cloud Access Security Brokerage (CASB) and Advance Threat Protection (ATP) solutions. In early 2012, Blue Coat, was acquired by the private equity firm Thoma Bravo. In 2015, Bain Capital acquired Blue Coat from Thoma Brava.

In July of 2015, Blue Coat acquired Perspecsys and in November of 2015 acquired Elastica. Both companies provide solutions in the CASB space, which help round out Blue Coat's offerings in Cloud Data Protection and Cloud Application Security and Control.

Blue Coat's Web Security is powered by the vendor's Global Intelligence Network (GIN) technology that utilizes a combination of traffic pattern, behavioral, server and site DNA,

content, and reputation analysis to build a comprehensive view of the web-based malware ecosystem. In the Web Security space Blue Coat provides:

- **Blue Coat ProxySG and Advanced SG (ASG)** – which are available as an appliance or virtual appliances. ProxySG provides a modular Web security solution that allows components to be added as needed. ASG is an integrated solution, combining ProxySG and Content Analysis System functionality in a single appliance. ProxySG and ASG utilize the Internet Content Adaptation Protocol (ICAP) to relay certain requests to other appliances built for a specific task, such as DLP. With the ProxySG and ASG, customers can analyze their SSL encrypted web traffic. The following components can also be added to a ProxySG and ASG appliances:

    - **Blue Coat WebFilter and Intelligence Services** - blocks malware, protects user productivity, and enables compliance by filtering out suspicious and compromised URLs. URL categorization is done in real-time for new and unknown URLs. The WebFilter solution is continuously updated by the Global Intelligence Network to provide better protection from malware. Blue Coat Intelligence Services is a new offering from Blue Coat which provides additional levels of detail on web risk levels and web applications.

    - **Encrypted Tap** - is a licensable feature for the ProxySG and ASG that provides complete visibility into HTTPS or SSL-encrypted web traffic. This extension can selectively decrypt SSL traffic according to policies, and send decrypted feeds to other security devices, as well as logging servers for analysis, archiving, and forensics.

    - **Reporter -** provides in-depth views of user activity, Web traffic, application access, blocked sites, and much more. Reporter supports up to 50 concurrent administrators to manage the reporting activity. It can also generate reports on social networking usage. Reporter is available as *Standard*, *Enterprise*, *Premium*, (software or appliance) or *Hosted Reporting* versions that have similar functionality but varying capacity options.

    - **DLP -** policies can be created that analyze content, source, destination, and more traveling through email, Webmail, social networking, and other Web channels. Administrators can “fingerprint” data that lets the solution watch certain data more closely. Blue Coat offers three different DLP appliances that enterprises can choose from, the *DLP700*, the *DLP1700*, and the *DLP2700*.

- **Management Center and Director** - allows administrators to centrally synchronize and configure ProxySG and ASG appliances. Updates, reports, configuration changes, and more can all be scheduled during off-peak hours to conserve bandwidth during normal business hours. Delegated administrators within workgroups and departments can set and manage policies for their own groups.

- **Proxy Client** - is included with all ProxySG/ASG deployments. It delivers security and acceleration services (e.g. retaining a cache of company logos to keep it from using bandwidth) to remote users.

- **Blue Coat Cloud Service** - lets customers deploy a Web security solution in the cloud or as a hybrid solution when combined with the vendor's on-premises solutions. The Blue Coat Cloud Service is available as follows:

  - **Web Security Service** - provides a secure Web browsing experience for all users with the same Global Intelligence Network technology that is used throughout Blue Coat's solutions. Web application controls are available to give administrators more granular control of their network. Web Security Service also has dual anti-malware engines as part of the standard offering. Remote users are protected with WebFilter via ProxyClient, another add-on to ProxySG that is included with WebFilter.

  - **Mobile Device Security -** adds network-based application controls, Web filtering, usage reports, and more for Apple iOS and Android devices in the network.

  - **Hosted Reporting Service -** is also available and offers the same features as its on-premises counterpart.

In addition, Blue Coat offers Cloud Access Security Brokerage **(**CASB), Cloud Data Protection (CDP) and Advanced Threat Protection (ATP) solutions, which combined with its Web security solutions make up Blue Coat Lifecycle defense product portfolio. Products in Blue Coat's Advanced Threat Protection solution set include: Content Analysis System, Malware Analysis Appliance, SSL Visibility Appliance, and a Security Analytics Platform.

STRENGHTS

- Blue Coat's Web security solutions can be deployed as appliances, services, or hybrid offerings.

- Blue Coat's own Global Intelligence technology that combines traffic pattern, behavioral, server and site DNA, content and reputation analysis.

- Blue Coat's Proxy SG and ASG Secure Web Gateway and SSL Visibility Appliance provide customers the ability to inspect SSL encrypted traffic.

- Blue Coat's hybrid and SaaS solutions offer one place to centrally manage policy and reporting for all users, including remote users. Many competing solutions still require separate management interfaces for hybrid deployments.

- Blue Coat's hardware appliances come standard with hardware-assisted encryption/decryption functionality that few other vendors have available.

WEAKNESSES

- Due to their cost and management complexity, Blue Coat's solutions are generally a best fit for larger enterprise organizations with significant IT resources. However, the Blue Coat Cloud Service is aimed at building traction with smaller customers.

- Blue Coat offers an appliance based network DLP solution, but does not currently offer an endpoint DLP solution.

- Blue Coat offers the capability to secure mobile devices with and without the use of VPN through the use of global proxy settings and on-device VPN client/profiles, however, its mobile device protection is currently focused only on Android and iOS devices.

FORCEPOINT

10900 Stonelake Blvd
3rd Floor
Austin, TX 78759
www.forcepoint.com

Forcepoint is a joint venture of Raytheon Company and Vista Equity Partners that was formed in 2015 out of a combination of Websense, Raytheon Cyber Products, and the Stonesoft and Sidewinder firewall assets it acquired from Intel Security in early 2016. Forcepoint offers Web, data, and email content security, user behavior analysis, and threat protection solutions to organizations of all sizes.

SOLUTIONS

Forcepoint's **TRITON APX** offers comprehensive data theft prevention for web, email, data and endpoint security to stop advanced persistent threats, targeted attacks and evolving malware. All Forcepoint TRITON products use the proprietary **ACE (Advanced Classification Engine)** technology to identify zero day, advanced threats, and data theft attempts with composite risk scoring technology that combines multiple security analytics, such as real-time browser code scanning, content classification, data classification, Web reputation, in-house signatures and heuristics, URL filtering, anti-phishing, anti-spam, and two traditional antivirus engines.

- **Forcepoint TRITON AP-WEB** is the core on-premise web gateway proxy, offering real-time protection against advanced threats and data theft, with a range of deployment options and modules to help organizations customize a Web protection package to best fit their needs. Several advanced protection modules can be added to the core TRITON AP-WEB solution:

    - *Threat Protection Cloud Module* – analyzes suspicious files in a virtual sandbox environment to identify malicious behavior of Zero-day and other advanced malware. Detailed forensic reporting is automatically provided when malicious files are detected.

    - *Web DLP Module* – a fully integrated DLP engine provides containment defenses against data theft, and enables regulatory compliance with over 1,700 pre-defined policies and templates.

- *Web Cloud Module* – provides the benefits of a web gateway proxy without the need for on-premises appliances.

- *Web Hybrid Module* – Centrally-managed hybrid on-premises/in-the-cloud architecture for protection of roaming users.

- *TRITON AP-MOBILE* – extends policies and security settings to Android or iOS devices. Protects against mobile malware, malicious apps, SMS spoofing, phishing, Web threats and data loss. MDM features are provided through integration with AirWatch.

- **Websense Web Filter & Security** is an easily deployed non-proxy product with over 120 security and web categories, plus advanced web application and protocol controls on all ports.

- **TRITON APX Enterprise Core** – extends protection from TRITON AP-WEB to TRITON AP-EMAIL, TRITON AP-DATA and TRITON AP-ENDPOINT for unified protection across all channels of attack.

STRENGTHS

- Forcepoint offers a powerful web security solution that addresses all key web security concerns and integrates well with additional modules for full cyberattack protection.

- The TRITON APX suite gives organizations the ability to deploy additional IT security elements from Forcepoint, such as email security, while maintaining a single management interface.

- Forcepoint offers a redesigned cloud portal and reporting interface, which includes a highly intuitive drag-and-drop user interface.

- Forcepoint has some of the most complete and secure application controls in the Web security space. The granularity for Web application controls available in Forcepoint's solution is leading edge.

WEAKNESSES

- The Web security solutions from Forcepoint are somewhat more expensive when compared to others in the space. However, Forcepoint introduced new modular pricing and packaging in 2015 which makes it easier for customers to buy only the protection they currently need, and expand the solution as their needs evolve.

- Though cloud and appliance based, Forcepoint TRITON solutions are aimed mainly at the complex needs of mid-size and large customers, and may not be a good fit for small businesses and SMBs.

- Forcepoint does not yet offer AP WEB as a virtual appliance, however the vendor is working to add this in the near future.

CISCO

170 West Tasman Dr.
San Jose, CA 95134
www.cisco.com

Cisco is a leading vendor of Internet communication and security technology. Cisco's original web security solutions come from its 2007 acquisition of IronPort. In 2009, Cisco added to its web security portfolio by acquiring ScanSafe, a SaaS security company. In October 2013, Cisco completed its acquisition of Sourcefire, and in June 2014, it completed the acquisition of ThreatGRID, which offers a cloud-based malware analysis and on-premise sandboxing appliance. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos) which is made up of leading threat researchers.

SOLUTIONS

Cisco Web Security combines comprehensive URL filtering, Malware detection, Web application control, and other advanced threat detection and protection services. Cisco's Corporate Web Security solutions can be deployed as appliances, cloud-based, network integrated, or hybrid solutions.

Cisco Web Security Appliances are available in the S-Series lineup, which comes in various versions: **S680** for large enterprises (> 10,000 users), **S380** (for mid-size companies with < 10,000 users), **S170** (for small companies with < 1,000 users), and **x90** appliance model which is built on Cisco UCS hardware. All appliances have the same security features, which include:

- *Malware protection is provided through Advanced Malware Protection (AMP)* and other malware engines. Cisco's malware protection and detection capabilities are based on its acquisitions of Cognitive, Sourcefire, OpenDNS, and ThreatGrid. AMP's File Reputation blocks files through reputation verdicts delivered by AMP cloud. File Sandbox allows behavioral analysis of files and feeds intelligence back to the AMP cloud. File Retrospection enables continuous analysis of files that have traversed the gateway and provides retrospective alerting after an attack when file is determined to be malicious. Additional malware protection is available through third party signature databases from McAfee, Sophos, and Webroot. These are fully integrated with the Cisco solution both in the appliance and the cloud version.

- *Web application controls* - granular policies for thousands of different Web applications can be set, enabling users to safely use social media websites and other Web applications. In addition, safe search functionality for search engines is available for popular media portals like YouTube, Flickr and others, allowing organizations greater control in filtering objectionable content for their users.

- *DLP* - is addressed with the combination of integrated on-box Data Security Policies and the choice of advanced DLP content scanning through ICAP interoperability with third-party DLP solutions.

- *Reporting* - of user activity and insights into network usage are available, customers can store years' worth of Web activity for reporting, legal, or forensic needs.

- *Advanced Threat Detection* – Cisco has also added its Cognitive Threat Analytics (CTA) capabilities to its appliance based solutions.

Cisco Cloud Web Security (CWS) is a cloud-based solution that comes with high availability SLAs. The solution offers feature parity with Cisco's Web Security Appliances for malware protection, URL filtering, and Web application controls. In addition, Cisco Cloud Web Security

offers the following features:

- *Advanced Threat Detection* - through the anomaly detection capabilities of Cognitive Threat Analytics (CTA). CTA provides the ability to create a baseline view of network activity and then detect persistent threats, including command and control connections, through anomalies from that baseline.

- *Management* - for policy configuration is provided in the cloud through Cisco's ScanCenter. The management portal allows customers to view all aspects of the service, such as virus scanning, Web filtering, and reporting. Changes made in the ScanCenter are propagated in near real-time.

Mobile users connect to the CWS proxy service through a connector available with **AnyConnect Secure Mobility Solution** (ACSM). Mobile protection is offered for Apple iOS, Google Android, Microsoft Windows and Apple Mac OS X operating systems. Policies can vary by location, such as whether they are inside or outside of the office. Remote laptop users can connect directly to CWS using AnyConnect.

STRENGTHS

- Cisco's Web Security solutions can be deployed as appliances, cloud-based, network integrated, or hybrid solutions.

- Cisco provides strong support for mobile device Web usage via its AnyConnect Secure Mobility Client. The cloud service supports Windows, Mac OS X, Apple iOS, Android, Windows Phone 8 and BlackBerry.

- The Web security solutions at Cisco have adaptive malware scanning that sends suspicious content to an anti-malware engine that is optimized for that type of content.

- Cisco's Web security solutions offer DLP policies that administrators can enable. Furthermore, Cisco's Web Security Appliances can integrate with Content-Aware DLP solutions via ICAP

- Cisco has integrated a traffic redirection feature into some of its on-premises equipment, including: the ASA firewall, Integrated Services Router (ISR) Generation 2, ISR 4k, and WSA. All support Cisco's "connector" software, which directs traffic to the CWS service.

WEAKNESSES

- Cisco Cloud Web Security could be improved through the ability to set more in-depth bandwidth control policies.

- Cisco offers only virtualization support for VMware, KVM and other platforms that support its UCS hypervisor and meet its hardware requirements.

- Cisco offers bandwidth controls, but does not offer dynamic traffic shaping.

- Cisco currently only supports unified reporting across WSA and CWS through an on-premises SMA application. A unified reporting cloud capability is under development which will allow the CWS ScanCenter UI to also be utilized for WSA appliances as part of hybrid solutions.

INTEL SECURITY

2821 Mission College Blvd.
Santa Clara, CA 95054
www.mcafee.com

McAfee, now part of Intel Security, delivers security solutions and services for business organizations and consumers. The company provides security solutions that protect businesses of all sizes from the latest malware and emerging online threats, through threat intelligence and services that protect endpoints, networks, servers, and more.

SOLUTIONS

McAfee Web Protection is Intel Security's flagship Web security solution that protects users from inbound and outbound threats. The solution is available in two different versions: **McAfee Web Gateway**, an on-premises appliance, and **McAfee SaaS Web Protection**, a cloud-based

option. The two solutions can also be deployed as a hybrid solution. The security suite includes the following features:

- *Threat protection* – contains a proactive anti-malware scanning engine that uses emulation and behavioral analysis to filter malicious Web content without a signature. The solution is backed by Intel Security's own signature-based anti-virus technology. The solution is also fed information by McAfee Global Threat Intelligence, a cloud-based threat data source that aggregates information from multiple sources to identify the latest threats. A third-party signature-based anti-virus engine is also used in addition to all proprietary Intel Security technology used.

- *URL filtering* - uses category and reputation filtering powered by Intel Security's proprietary Global Threat Intelligence system. For uncategorized URLs, McAfee Web Gateway offers local, dynamic content classification to assign a category.

- *Off-network protection* – a proprietary client agent (McAfee Client Proxy) can be deployed to endpoint devices which automatically enables routing and authentication to the web security cloud service once users leave the corporate network.

- *Web application controls* - allow for granular policies of more than 1,500 Web applications and application sub-functionalities. Customers can also input custom application signatures for broader Web application controls.

- *Reporting* - is accessed in the McAfee ePolicy Orchestrator (ePO) via the McAfee Content Security Reporter extension, which uses its own server to handle report generation in an effort to increase scalability. Once reports have been generated, policy can be immediately updated from the reports created.

- *DLP* - control comes bundled with the solution to prevent content in the enterprise from leaving via social networking sites, blogs, wikis, applications, and more. Deployments can also upgrade to the McAfee Data Loss Prevention solution for deeper, content-aware DLP capabilities.

STRENGTHS

- The McAfee Web Protection solution has its own management solution that can manage both the on-premises software and cloud service from one interface, and allows the same policies to be set on-premises as well as pushed out to the cloud. This provides equal protection for all users, regardless of whether they route through the appliance or cloud. It can also integrate with McAfee ePO for central reporting for all McAfee solutions across the enterprise.

- Intel Security offers a host of other security solutions that can be deployed alongside its Web Protection solution, such as in-line prevention of zero-day malware, endpoint protection, malware sandboxing, data loss prevention (DLP), and more.

- Intel Security uses a shared reputation network for all its solutions, including network and Web, in order to gain a better real-time insight into malware threats and protect users from blended attacks.

- McAfee Web Protection integrates extensively with the Intel Security product portfolio including its Advanced Threat Defense appliance for centralized malware scanning, Threat Intelligence Exchange for threat information sharing, ePO for centralized reporting, and Enterprise Security Manager (SIEM) for data analytics.

WEAKNESSES

- Intel Security's web protection offers application bandwidth controls but does not offer traffic shaping for improved network bandwidth utilization.

- Reporting granularity could be improved.

- Intel does not provide its own mobile device protection, but partners with leading EMM vendors AirWatch and MobileIron to enforce protection on mobile devices.

- Intel has announced announced the end of life of its McAfee SaaS email protection solution and recommending that customers transition to Proofpoint, which may disappoint customers looking to acquire their email and web protection solutions from a single vendor.

SOPHOS

The Pentagon Abingdon Science Park
Abingdon
OX14 3YP
United Kingdom
www.sophos.com

Sophos offers a variety of mid-market security solutions, including encryption, endpoint, email, Web, UTM, and more. The company is headquartered in Abingdon, UK. Sophos acquired Mojave Networks in late 2014, adding to its cloud capabilities.

SOLUTIONS

Sophos currently offers two dedicated Web Security solutions, the **Sophos Web Appliance** and the **Sophos Web Gateway**, which comes from the integration of the Mojave Networks acquisition into Sophos Cloud. The two solutions are set to converge in 2017 with the launch of a hybrid solution combining the cloud and on-premises deployment options.

The **Sophos Web Appliance** is available as a hardware or virtual appliance. It can integrate via the cloud with Sophos' endpoint security solution. This combination provides web security, policy, and reporting for off-site users without the need for routing Web traffic through a cloud gateway. The solution also comes with the *Sophos Management Appliance* capabilities that give Sophos some remote management over customers' deployments, such as updates and troubleshooting.

The **Sophos Web Gateway** delivers an enterprise-grade Secure Web Gateway, which provides cloud management, reporting, enforcement and advanced protection. Optimized for the cloud, it offers high performance, instant visibility and granular policy control. All solutions include:

- *Threat protection* - provided by Sophos' own proprietary technology that originates from SophosLabs. The proprietary threat technology at Sophos uses reputation, anti-virus signatures, behavioral analysis, and more to find malware being accessed via the Web.

- *URL filtering* - available for 56 pre-defined categories. Custom categories can also be set-up if necessary.

- *Web application controls* - are available for multiple Web applications, such as webmail, forums, blogs, and more. Granular controls for social media sites let administrators control individual elements within the applications, such as posting updates. The solution can also block downloads of applications from the Web that may violate policy controls, such as Skype. Application control has been extended to mobile devices.

- *DLP controls* - are provided via the Web application controls that can prevent outbound data flows.

- *Management and reporting* - is built-in to the Sophos Web Appliance. Real-time reporting is available in the management dashboard. The solution can also integrate via syslog with SIEM and other third-party reporting solutions for additional reporting features that are beyond the scope of a Web security solution. Consolidated reporting and policy management across multiple appliances is done with a Sophos Management Appliance that can be deployed as either a physical or a virtual appliance.

STRENGTHS

- Sophos has an easy to use, intuitive management interface. Navigation follows a 'three clicks' rule which makes it quick and easy to learn.

- Sophos offers flexible deployment options including cloud and on-premises, as well as hybrid on the roadmap for 2017 .

- The Sophos Web Appliance solution comes with the vendor's Managed Appliance Service that allows Sophos to monitor and help troubleshoot each deployed Sophos Web Appliance.

- Sophos offers straightforward per user pricing, which in most cases works out to be more cost-effective than many other vendors in the Corporate Web Security market.

- Sophos offers Sophos Sandstorm, an advanced persistent threat (APT) and zero-day malware defense solution that complements Sophos all security products. It detects, blocks, and responds to evasive threats through cloud-based, next-generation sandbox technology.

WEAKNESSES

- Sophos solutions are aimed at the needs of small to mid-market customers, and focus on ease of use and reliability, rather than delivering extensive customization features.

- DLP capabilities are currently still fairly basic, however, more advanced features are on the roadmap for the 2017 timeframe.

- Currently, Sophos Web Gateway and Sophos Web Appliance solutions have separate management interfaces when deployed together as a hybrid solution. However, integrated management of hybrid deployments through a Next Generation Secure Web Gateway is on the roadmap for early 2017.

TRAIL BLAZERS

CLEARSWIFT

1310 Waterside, Arlington Business Park
Theale
Reading
Berkshire, RG7 4SA
UK
www.clearswift.com

Clearswift is a UK-based security company that offers threat protection through its Clearswift's Aneesya platform. As part of this platform, the **Clearswift SECURE Web Gateway** is powered by the awarded Clearswift's Deep Content Inspection engine, which shares policies across email, web and endpoint solutions.

SOLUTIONS

The Clearswift SECURE Web Gateway can be deployed as a physical or virtual appliance on-premises, in the cloud (including AWS), or in hybrid environments. A fully hosted solution is on the roadmap for 2016. The solution offers the following features:

Filtering and Content Inspection - policy-based filtering and content aware inspection extends beyond limiting browsing to view inside encrypted traffic to prevent phishing, malware and sensitive data leaks.

Advanced Threat Protection - Clearswift's SECURE Web Gateway removes malicious active content from web traffic in real time in a fully transparent, automated way.

Phishing Targeting and Information Harvesting Prevention - prevents phishing expeditions from harvesting easily accessed information hidden in document metadata (author, login, department, system names, etc.) by automatically cleansing that information from published files.

Adaptive Data Loss Prevention - Clearswift includes Adaptive Data Loss Prevention technology that detects and redacts sensitive or inappropriate information, while allowing other web, social or cloud activity to continue unhindered.

Cloud Security - bi-directional inspection allows visibility of what information is being stored or downloaded from cloud collaboration tools and storage (e.g. Office 365, Box, Dropbox, Google Drive, and others). It also helps detect the use of any cloud apps and tools adopted by users through "Shadow IT."

Securing Social Media - Clearswift enables risk-free social media communications by monitoring Twitter, YouTube content and channels, and others, while turning off granular Facebook features.

Mobile and Remote User Protection - protection that extends enforcing of an organization's sanitization policies to remote and mobile users.

STRENGTHS

- Clearswift appliances can be deployed as hardware, virtual appliances on VMware, or on cloud platforms.

- Clearswift is part of a comprehensive security platform called Aneesya, which includes internal and external email protection, and an endpoint solution which shares much of the same threat technology as the SECURE Web Gateway. This allows for easier enforcement of

unified corporate security policies.

- Clearswift Adaptive Data Loss Prevention features provide protection for incoming threats, as well as for organizations' critical information.

- Active directory integration allows enforcement of granular security policies based on user information such as group or location. SIEM and monitoring can also be easily configured through the web UI.

- Adaptive Redaction technology allows the modification of offending traffic in a safe, transparent and automated way.

WEAKNESSES

- Clearswift provides policies for bandwidth control but does not provide traffic shaping or other similar features, which help streamline large amounts of traffic.
- Web application controls, while adequate could be rendered more granular, particularly as it relates to social media sites.
- Clearswift does not provide its own mobile device protection, but relies on a partnership with AirWatch.
- Clearswift's reporting features are adequate but could be enhanced. The company is working on this and offers a Gateway Reporter appliance. Transaction information can also be exported in a standard format to be integrated with third parties reporting solutions.
- Clearswift needs to invest to raise its market visibility.

SPECIALISTS

TRUSTWAVE

70 West Madison St, Suite 1050
Chicago, IL 60602
www.trustwave.com

Founded in 1995, Trustwave is a global cybersecurity and managed security services provider (MSSP) that helps businesses defend from cybercrime, protect data and reduce risk. Trustwave is one of the largest MSSPs worldwide. In August 2015, Trustwave was acquired by Singtel, Asia's leading communications group. Trustwave is now a standalone business unit and core cybersecurity platform and brand of Singtel Group Enterprise.

SOLUTIONS

The SpiderLabs team at Trustwave provides threat intelligence, incident response, security scanning and testing, as well as anti-malware and other security research that is integrated into the company's security solutions, including its secure web gateway and managed security services. **Trustwave Secure Web Gateway (SWG)** is Trustwave's flagship Web security product that provides data-aware detection of emerging, advanced malware threats using a combination of real-time analysis, detection and policy control enforcement technologies. Trustwave SWG is available as a traditional appliance, virtual appliance, or as a hybrid on-premises and cloud solution. The Trustwave Secure Web Gateway includes the following features:

- *Threat Protection* is delivered in a multi-layered fashion that uses proprietary Real-Time Code Analysis and Malware Entrapment engine technologies to block malware that attempts to infiltrate an enterprise network. The Real-Time Code Analysis technology uses multiple malware engines to examine inbound and outbound Web traffic, including HTTP and HTTPs traffic. It analyzes incoming and outgoing Web content in real-time and understands its intent. Frequently scanned content is also cached by the solution to save bandwidth whenever the content is accessed again. The Malware Entrapment engine also provides dynamic page analysis that runs as users are accessing Web content, rendering the page as it would be in a browser and uncovering any malicious intent of the Web code. In SWG v11.7, Trustwave added a forensics capture and reporting capability that captures the files and resources

associated with web pages that trigger the Malware Entrapment engine. Customers are given a report of the incident as well as access to all of the files and can then have their security team investigate the malware.

- *Web application controls* enable administrators to set and enforce policies for social media and Web 2.0 sites and applications usage. Granular access is available to allow, block, or restrict posts or uploads and related traffic to social networking sites, such as Facebook, Twitter, LinkedIn, Google+ or YouTube. Trustwave has added granular controls for cloud drives including Dropbox, Google Drive, Box, MS OneDrive, and Apple iCloud Drive. This allows control over downloading, uploading, sharing, and working in the file system.

- *Management* is unified for all deployment scenarios. Out-of-the-box reporting gives administrators access to various reporting options, including for security and productivity analysis purposes, with various scheduling options. Advanced reporting features, such as automatic report generation, a real-time dashboard, and more, is available with the **Trustwave Security Reporter**. The advanced reporting module also supports archiving and integration with other reporting tools using syslog and other standard output formats.

- *URL Filtering* is provided with Trustwave's proprietary Web filtering technology that gives administrators access to more than 100 categories to filter. Based on classification, reputation, and content, Trustwave blocks access to malicious URLs and IP addresses. SWG also includes dynamic categorization for any URL that is not already in the URL database.

- *DLP* is included with the integrated Trustwave DLP technology. It provides easy basic data loss prevention capabilities, such as preventing users from spreading confidential data on social media sites. It also allows administrators to add custom data types and content. Customers can expand the scope of DLP controls to include enterprise DLP via the integration of Trustwave's DLP through Trustwave SWG support of the standard ICAP protocol.

The Trustwave **Managed Anti-Malware service**, powered by the company's Secure Web Gateway (SWG) product, provides advanced content, network and application security without the need for an organization to install and manage the technologies themselves. It offers the same features as SWG. With Trustwave Managed Anti-Malware service, organizations receive around-the-clock support from the global network of Trustwave Security Operations Centers

(SOCs). All Trustwave Managed Security Services are available through the Trustwave TrustKeeper cloud and managed security services platform.

The Trustwave Managed Anti-Malware service also includes integrated threat intelligence from SpiderLabs, the Trustwave advanced threat research team. As part of the service customers automatically receive a "Zero-Malware Guarantee" – if a customer demonstrates any malware missed by the solution, Trustwave will add a free month to their subscription, up to once per quarter. Trustwave is the only vendor in the Web Security Market to offer a guarantee against malware.

The Trustwave Managed Anti-Malware service also provides a highly customizable, real-time dashboard. The dashboard is backed by a big data back-end that allows users to drill-down to every individual web transaction. The big data back-end also allows Trustwave security experts to monitor and alert about security risks and anomalous behavior.

In 2016, Trustwave plans to launch a Security-as-a-Service (SaaS), or all cloud, version of the Managed Anti-Malware service. This service is expected to include all of the same security engines as the on-premises based product, as well as its other functionality including URL filtering, DLP, and application control. This will be a multi-tenant cloud offering that will better serve distributed customers and offer better policy coverage for mobile devices off the corporate network.

Trustwave Web Filtering And Reporting (WFR) are targeted at organizations focused on safe Web surfing enforcement and user productivity. Trustwave WFR is an appliance-based solution that includes the following features:

- *URL filtering* is one of the key features of this solution. All Web traffic is filtered to scan for spyware, botnets, anonymous Web proxies, and other threatening technologies. Furthermore, the solution can filter Web traffic by Web application, such as social networking, instant messaging, P2P, and more; file type; and protocol, such as HTTP or HTTPS. The URLs are also filtered based on the enterprise policy for optimized productivity. The URL Categorization database is kept up-to-date, and its updates are distributed on a daily basis to the URL filtering system.

- *Reporting* tools give administrators a real-time look at the status of their network, bandwidth use, user intent, and more. Reports can be automatically scheduled based on templates.

Trustwave WebMarshal scans incoming and outgoing traffic to protect against threats on the Web. The solution can be deployed in a variety of ways, including as a standalone proxy server, a Microsoft ISA Server plug-in, or as an array of servers for load-balancing in large scale deployments. It includes the following features:

- *Threat Protection* is aided by Trustwave's proprietary TRACENet technology that utilizes heuristic filters, and reputation-based blacklists to protect against Web threats.

- *URL filtering* can block access to sites based on more than a hundred different categories. Content, reputation, and other aspects are used to filter these URLs.

- *Web application controls* are included that can be set based on bandwidth and quotas (by time and volume, per user/user group, per day, week, month, year), time of day, or type of application, such as social media, streaming media, or instant messaging.

- *DLP* capabilities are included that can be enforced by unique user or user group. Trustwave WebMarshal can provide DLP based on keyword or phrases written in a browser or uploaded in a file, such as a .doc file. Restrictions can also be placed on what file types can be uploaded. Enforcement is also available on HTTPS.

- *Reporting* features allow to identify the most frequently visited websites, blocked content, top Web users, and more. Summary reports can also be generated for simplicity.

STRENGTHS

- Trustwave's Secure Web Gateway offers strong proprietary anti-malware technology. Their technologies for Real-Time Code Analysis and Malware Entrapment engines include advanced heuristics, reputation network analysis, and more.

- Trustwave offers a variety of security solutions that protect multi-vector data and offer malware security, such as Web, email, social media malware protection, data loss prevention and encryption across web, email and social media attack vectors.

- Trustwave offers integrated DLP in its Web security solution, as well as the ability to integrate with full enterprise DLP through its own or a third-party solution.

- Trustwave SWG is available in various form factors, including as a managed service, traditional appliance, virtual appliance, or as a hybrid (i.e. on-premises and cloud) solution.

WEAKNESSES

- Trustwave does not currently offer a multi-tenant cloud platform. However, the vendor is working to address this in the coming year.

- Although remote and mobile workers can be protected with Trustwave's Web security solutions, the vendor has limited native protection for mobile devices. This is being addressed in the soon to be released multi-tenant cloud offering.

- While Trustwave offers comprehensive application control for social media and cloud storage, some of its other application controls could offer deeper and more granular functionality.

IBOSS

4110 Campus Point Court
San Diego, CA 92121
www.iboss.com

iboss delivers Internet security through the cloud by leveraging a Containerized Cloud architecture of its own design. iboss targets mid to large organizations as well as state and local government organizations. iboss is a privately held company, headquartered in San Diego, California.

SOLUTIONS

iboss offers a stream based cloud web security platform, which allows it to secure all ports and protocols including evasive protocols. In addition, iboss leverages cloud behavioral sandboxing, cloud behavioral DLP, integrated IPS and blended AV signatures Key capabilies include:

*CISO Command Cent*er - is designed as a single dashboard which correlates threat information into actionable intelligence. It allows administrators to identify data loss, high risk activity and

mitigate threats. The CISO dashboard helps reduce dwell time of active infections on the network.

Threat Intelligence Cloudsourcing - The CISO Command Center provides the dynamic ability to research any event including malware, URL, file type in the cloud from within the CISO dashboard, for instant research and forensics. This allows administrators to further research threat events and identify the potential exposure to the network without having to manually research it. *Expanded Single Pane of Gl*ass - architecture to include FireSphere for Mobile Ether - provides full APT capabilities in conjunction with secure web gateway and MDM application control capabilities.

Flexible cloud integration options – iboss's Containerized Cloud architecture provides the flexibility to integrate into any organization including those who may be cloud adverse or who are restricted from leveraging the public cloud due to regulatory or corporate compliances. The design allows organizations to manage a single policy console regardless of local or public cloud hosting.

Behavioral (DLP) via Data Anomaly Monitoring Technology - iboss integrates Baselining and Network Traffic Anomaly Monitoring, to continuously monitor network traffic to detect anomalous behavior and contain traffic being exfiltrated from the network resulting in reduced data loss during an attack.

Active and Passive Sandboxing in the cloud - iboss provides auto deposit and on-demand behavioral cloud-based Sandboxing which quarantines high risk files before they hit the device reducing the potential for compromise. This ensures all devices, including mobile workers are consistently receiving the advanced behavioral threat defenses while roaming.

STRENGTHS

iboss deployment options include on-premises, private cloud and/or public cloud and can support any network of any size, with a flexibility that meets a wide-range of customer requirements.

iboss integrates Baselining and Network Traffic Anomaly Monitoring, which serves to continuously monitor network traffic to detect anomalous behavior and contain traffic being exfiltrated from the network resulting in reduced data loss during an attack.

iboss provides auto deposit and on-demand behavioral Sandboxing through the cloud, which dynamically Sandboxes and quarantines high risk files before they hit the device reducing the potential for compromise.

The iboss Incident Response Dashboard provides a single-pane-of-glass where events are correlated into incidents, which reduces the meantime to detect active infections on the network, thereby resulting in a reduction of noisy event logs, heightened visibility of the threat landscape and lower administrative overhead.

WEAKNESSES

- The iboss cloud-based service lacks support for SAML.
- iboss currently lacks market visibility, a recent investment from Goldman Sachs, is meant to help the vendor raise awareness of the product and company globally.
- iboss has regional offices in APAC and EMEA, however, the vendor is still developing its market presence in these regions.

ZSCALER

110 Baytech Drive, Suite 100
San Jose, CA 95134
www.zscaler.com

Founded in 2008, Zscaler's Security-as-a-Service platform delivers unified, carrier-grade Internet security, advanced persistent threat (APT) protection, data loss prevention, SSL decryption, traffic shaping, policy management and threat intelligence.

SOLUTIONS

Zscaler offers an entirely cloud based security platform, which acts as a proxy for incoming and outgoing Internet traffic. Traffic can be routed to Zscaler via a GRE tunnel, firewall port forwarding, proxy chaining, proxy auto-configuration (PAC) files, or IPSec/SSL VPN. Zscaler

cloud based security is available as an integrated suite of security products available in three different packages. Key capabilities include:

- *Inline Threat Protection* **-** Zscaler bi-directionally inspects Internet traffic, blocking malware and cyber-attacks with multiple layers of security, including MD5 signature blocking, anti-virus, intrusion detection, content inspection, machine learning, threat assessment, SSL decryption, cloud mining, risk profiling, sandboxing, advanced persistent threat (APT) protection and more.

- *Sandboxing/Behavioral Analysis* **-** Zscaler protects against zero-day malware and Advanced Persistent Threats (APTs) by identifying suspicious objects, and executing them in virtual sandboxes. Any malicious behaviors are recorded and analyzed, and malicious objects are automatically blocked across all of Zscaler's user installed base in near real-time.

- *DLP Inspection* - Zscaler provides full inspection of all Internet traffic, including SSL, ensuring that confidential information and intellectual property does not leak to the Internet.

- *URL Filtering* - allows organizations to limit exposure by managing access to web content for users, groups and locations. URLs are filtered by global reputation, against across a wide number of categories.

- *Cloud Application Visibility & Control* - allows monitoring, protection and cloud application usage control across the organization. Policies can be set to ensure the safe use of business critical cloud applications, and restrict the use of non-sanctioned applications across users, groups and locations.

- *Bandwidth Control* – allows organizations to easily and efficiently allocate bandwidth to prioritize business critical web applications, over personal usage.

- *Unified Policy and Reporting* - a unified console allows the creation of web policies across security, Internet access management and data loss prevention. Administrators manage their own policy, with changes instantly reflected across the entire cloud. The administrative portal provides a single pane of glass to view and analyze all traffic across all devices and locations in real time.

- *SIEM Integration* - Zscaler Nanolog Streaming Service (NSS) transmits web logs from the Zscaler Cloud to the organization's enterprise SIEM in real time. Administrators can choose to send all the logs, or only specific fields based on interest or the EPS capacity. NSS enables companies to meet compliance mandates on local log archival, correlate web logs to other logs in the SIEM, and receive real-time alerts of security incidents from the SIEM.

STRENGTHS

- Zscaler's cloud-based security model provides effective protection across all traffic, users, and devices, including cloud applications, remote locations, and mobile employees.

- Zscaler's integrated security suite offers in-depth defense, with all traffic going through multiple layers of security and SSL inspection.

- Zscaler's cloud-based security approach helps reduce total cost of ownership, as it does not need customers to purchase and manage hardware appliances.

WEAKNESSES

- DLP, bandwidth control, Web 2.0 controls, and other advanced features are only available on higher-priced packages of the Zscaler Web Security Suite.

- Zscaler no longer offers email security as part of its service portfolio.

- Zscaler offers a cloud-based firewall service as an add-on to its SWG service. The firewall service, however, is not intended as a replacement for enterprise firewalls or UTM appliances in the near term. It is primarily suitable for small businesses, branch offices, roaming laptops or kiosks.

- Zscaler customers have reported instances of performance degradation which have affected user satisfaction with the solution.

BARRACUDA NETWORKS

3175 S. Winchester Blvd
Campbell, CA 95008
www.barracuda.COM

Founded in 2003, Barracuda Networks is a provider of content and network security, application delivery, storage and data protection solutions. Barracuda Networks is a publicly traded company.

SOLUTIONS

Barracuda Networks' security solutions are backed by Barracuda Central, a 24/7 security center that tracks the latest web threats. Data collected at Barracuda Central is used to create signatures against malware. Barracuda Central also handles website categorization updates. Updates are sent automatically via Energize Updates to Barracuda Networks' security solutions. Barracuda Central was significantly enhanced through a partnership with LastLine, where Barracuda hosts LastLine's sandbox engine in the Barracuda Central Cloud.

The Barracuda Web Filter is sold as an appliance that monitors real-time inbound and outbound traffic. Virtual appliances are also available for VMware ESXi, Microsoft Hyper-V, KVM, and Citrix Xen platforms. These solutions include the following features:

- *Threat Protection* combines both proprietary and open-source anti-virus technologies that protect users from viruses, exploit kits, bot networks, and other malware. Infected clients can be isolated from the network while providing access to remediation software.

- *URL Filtering* is available for content, domain name, URL pattern, or file type. The solution also performs dynamic classification of real-time threats. Warnings can be used for potentially malicious or policy violating websites.

- *Web 2.0 and Improved Application Control* allows the regulation of popular Web and client applications, such as apps on Facebook, IM, streaming media, and more. It filters these applications based on IP addresses, port numbers, and other patterns to build signatures while utilizing real-time deep packet inspection. The technology also employs a local cache for frequently used safe sites to preserve bandwidth and reduce latency.

- *Policy Management* is accessed from a single pane with options for policies by unique user, group of users, IP address, and more. Exception rules can also be created to supersede these policies when necessary.

- *Reporting* is available to generate more than 70 pre-defined reports to analyze data for the past 6 months, including a new performance summary report. The Barracuda Web Filter can forward all Web traffic as syslog messages that can be further analyzed or stored longer on a separate log storage or SIEM solution.

- *Customizable Dashboards* allow admins to create multiple dashboards that represent their own priorities. These dashboards are easy to create with the built in reports and drag & drop functionality. The feature is available on models 610 and above.

- *Remote Protection* is provided via the **Barracuda Web Security Agent** for Microsoft Windows and Apple Mac OS X workstations. The agent is tamperproof to ensure the most secure protection and prevent user circumvention. Apple iOS devices are also protected when outside of the network with the **Barracuda Safe Browser** solution that acts a replacement for the Safari Web browsing application.

- *Mobile Device Management* is included with all Web Security offerings, featuring support for iOS and Android devices.

- *Wireless Access Point Integration* was added with several WLAN AP providers including, Ruckus, Aerohive and Meru. The integration enables a single-sign onto to both the WLAN AP and the Barracuda Web Filter improving the overall end user experience. Additionally, administrators can also have deep visibility into user behavior and network activity. This enables customers to better shape their wireless policies based on meaningful data about their network traffic.

- *Chromebook Support* was added to enforce user-based policies outside of the network perimeter through the use of proxy authentication and LDAP.

Barracuda Web Security Service is a cloud-based content filtering and malware protection solution that offers similar features to the Barracuda Web Filter solution. The Barracuda Web Security Service can be combined with the Barracuda Web Filter, to create a hybrid solution.

STRENGHTS

- Barracuda Networks offers a single management interface, Barracuda Cloud Control (BCC) for all of its deployments that can manage users and consolidate report data across different geographies.

- Barracuda Networks is one of the lower priced Web security solutions in the market today.

- Barracuda Networks is able to provide social media archiving, enabling organizations to archive and store social media interactions for compliance, DLP and eDiscovery.

WEAKNESSES

- Barracuda Network's web security solutions are a best fit for small to midsize customers, with basic web protection needs. Larger customers with finer grained control needs may find the solutions lacking.

- DLP features are minimal in the solutions offered by Barracuda. However, the Barracuda Web Filter provides ICAP integration which allows for easy integration with third party DLP solutions.

- Barracuda bandwidth controls are not as developed as other vendors, however, Barracuda offers extensive bandwidth management controls as part of its firewall solutions which are typically deployed along its web proxy solutions.

MATURE PLAYERS

TREND MICRO

Shinjuku MAYNDS Tower, 1-1,
Yoyogi 2-Chome, Shibuya-ku
Tokyo, 151-0053, Japan
www.trendmicro.com

Founded in 1988, Trend Micro provides multi-layered network and endpoint security solutions for businesses and consumers worldwide. Trend Micro's security solutions are powered by its Trend Micro Smart Protection Network.

SOLUTIONS

Trend Micro Interscan Web Security (IWS) is part of Trend Micro's Smart Protection Suites, which combine endpoint and mobile threat protection with multiple layers of email, collaboration, and gateway security. Trend Micro's IWS includes:

- **InterScan Web Security Virtual Appliance** – an on-premises web gateway security appliance.

- **InterScan Web Security as a Service** – a cloud-based web security solution.

- **Trend Micro Control Manager** – a centralized, user-based security management console.

Trend Micro IWS includes the following capabilities:

- *Threat Protection* – offers real-time protection against blended threats, viruses, worms, spyware, bots, keyloggers, phishing attempts, rootkits, and other malware. Threat protection is powered by the company's proprietary Smart Protection Network, which pushes updates to the IWS for provide zero-hour protection.

- *URL Filtering* provides administrators with access to over 80 categories for filtering. Granular control of URL filtering policies can be applied to select users or groups of users. Policy actions include allow, monitor, block, block with password override, warn, and

enforce with time quota.

Trend Micro Advanced Reporting and Management is an optional add-on for IWS to expand reporting capabilities. It offers real-time data and analytics for individual user behavior. The Trend Micro Advanced Reporting and Management is commonly deployed as an aid in policy creation and refinement. IWS can also integrate with **Trend Micro Damage Cleanup Service** to remove viruses, worms, rootkits, and other malware from an infected machine.

STRENGTHS

- Trend Micro offers both on-premises and cloud based options with an integrated management console for ease of administration of hybrid environments.
- Trend Micro supports VMware and Microsoft Hyper-V as virtual platforms for its appliance based solutions.
- Trend Micro includes gateway-based, out-of-the-box DLP based on pattern matching.
- Comprehensive, drill-down reports that enable real-time, detailed tracking of individual user actions are available.

WEAKNESSES

- Trend Micro does not provide an integrated management interface across its appliance and cloud based InterScan solutions, which would ease administration of hybrid deployments.
- Trend Micro offers only basic DLP support.
- Trend Micro offers application controls and monitoring, but does not support traffic shaping.
- Trend Micro has been slow to update IWS viewing it more as an add-on for its existing customer base.

SYMANTEC
350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Symantec offers a wide range of security solutions for the enterprise. Symantec's Web Security solutions are available as cloud services, appliances, and virtual appliances.

SOLUTIONS

Symantec's Web security solutions are backed by the Symantec Global Intelligence Network that offers real-time protection from malware, and Symantec Insight, a real time reputation based malware filtering technology which helps detect new, targeted attacks.

Symantec Web Gateway 5.2.x provides protection for Web users with optional URL filtering functionality that can be added to deployments. The solution is available as a physical appliance or virtual appliance.

- *Threat protection* - is provided by Symantec's proprietary malware-scanning technology, which offers bi-directional scanning of all ports, including activity over SSL. Behavioral analysis and other technologies to detect suspicious activity, such as programs attempting to phone-home, is also used to protect from threats. Symantec Web Gateway can provide specific information about which machines are infected with malware or part of a botnet network, allowing customers to easily clean up infected machines.

- *Application controls* - provide granular control over more than 100 applications and protocols, such as instant messaging, remote access, streaming media, P2P, and more.

- *DLP* - is available via integration with Symantec's Data Loss Prevention Network Prevent for Web solution. The integration is available via ICAP and scans SSL content.

- *URL filtering* is provided by the Symantec RuleSpace engine, which is an add-on to the core offering of the Symantec Web Gateway. The URL filtering policy engine allows administrators to create custom rules for select users, groups, specific blocks of time, or by bandwidth consumption.

- *Centralized management* is available for multiple appliances, regardless of form factor. The reporting component is also available with prebuilt reports that can be automatically generated or accessed on-demand.

Symantec Web Security.cloud is a cloud-based solution that offers many of the same features of the Symantec Web Gateway. The cloud-based solution also utilizes the same threat technology that is delivered by Symantec's Global Intelligence Network, and its Skeptic™ proprietary technology. Threat protection, application control, URL filtering, centralized management, and more are included. Similarly, Symantec has a host of other cloud-based security solutions that integrate with the Symantec Web Security.cloud solution. Remote users are protected by Web Security.cloud's Smart Connect agent that enforces Web policies for each user.

STRENGTHS

- Symantec offers a broad range of security solutions, including email security, endpoint protection, data loss prevention, and more to complement its Web security solutions.

- Symantec invests heavily in malware research to protect users from new and advanced threats.

- Symantec Web Security's data protection feature picks up all the dictionaries, standard policies and templates of the greater Symantec DLP solution and applies them to the service. As these elements are updated, Symantec's Web Security Solution Data Protection feature is inherently updated so it delivers the latest data protection in Web.cloud.

WEAKNESSES

- There is considerable feature disparity between Symantec's on-premises and cloud based Web Security solutions, and the management of the two solutions is not unified. Customers considering a hybrid approach should investigate closely what is provided in both offerings.

- Symantec has announced it is retiring its Web Gateway 5.2.x appliance solution, with end of engineering support in 2017, and end of life support in 2019. A replacement strategy has not yet been announced.

- The setting and ease of administration of bandwidth controls included in the Web security solutions from Symantec could be improved.

- DLP is provided through integration with Symantec Data Loss Prevention for Web, however, this is a separate solution.

- The recent split of Symantec into two companies (Symantec focused on security and Veritas dedicated to information management) has caused some transition pain and slowed down innovation. It remains to be seen how quickly the new, recently re-organized Symantec can regain focus on R&D and new technology development.

THE RADICATI GROUP, INC.
http://www.radicati.com

The Radicati Group, Inc. is a leading Market Research Firm specializing in emerging IT technologies. The company provides detailed market size, installed base and forecast information on a worldwide basis, as well as detailed country breakouts, in all areas of:

- **Email**
- **Security**
- **Instant Messaging**
- **Unified Communications**
- **Identity Management**
- **Web Technologies**

The company assists vendors to define their strategic product and business direction. It also assists corporate organizations in selecting the right products and technologies to support their business needs.

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim.

The Radicati Group, Inc. was founded in 1993, and is headquartered in Palo Alto, CA, with offices in London, UK.

Consulting Services:

The Radicati Group, Inc. provides the following Consulting Services:

- Management Consulting
- Whitepapers
- Strategic Business Planning
- Product Selection Advice
- TCO/ROI Analysis

Multi-Client Studies

To learn more about our reports and services, please visit our website at www.radicati.com.

MARKET RESEARCH PUBLICATIONS

The Radicati Group, Inc. develops in-depth market analysis studies covering market size, installed base, industry trends and competition. Current and upcoming publications include:

Currently Released:

Title	Released	Price*
Advanced Threat Protection Market, 2016-2020	Mar. 2016	$3,000.00
Enterprise Mobility Management Market, 2016-2020	Mar. 2016	$3,000.00
Information Archiving Market, 2016-2020	Mar. 2016	$3,000.00
US Email Statistics Report, 2016-2020	Mar. 2016	$3,000.00
Email Statistics Report, 2016-2020	Mar. 2016	$3,000.00
Instant Messaging Market, 2016-2020	Feb. 2016	$3,000.00
Instant Messaging Growth Forecast, 2016-2020	Feb. 2016	$3,000.00
Social Networking Growth Forecast, 2016-2020	Feb. 2016	$3,000.00
Mobile Growth Forecast, 2016-2020	Jan. 2016	$3,000.00
Endpoint Security Market, 2015-2020	Dec. 2015	$3,000.00
eDiscovery Market, 2015-2020	Dec. 2015	$3,000.00
Microsoft SharePoint Market Analysis, 2015-2019	Aug. 2015	$3,000.00
Email Market, 2015-2019	Jul. 2015	$3,000.00
Cloud Business Email Market, 2015-2019	Jul. 2015	$3,000.00
Corporate Web Security Market, 2015-2019	Jul. 2015	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2015-2019	Jun. 2015	$3,000.00

*** Discounted by $500 if purchased by credit card.**

Upcoming Publications:

Title	To Be Released	Price*
Email Market, 2016-2020	June 2016	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2016-2020	July 2016	$3,000.00

*** Discounted by $500 if purchased by credit card.**

All Radicati Group reports are available online at http://www.radicati.com**.**