The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Corporate Web Security - Market Quadrant 2019 *

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

March 2019

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 very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.

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.

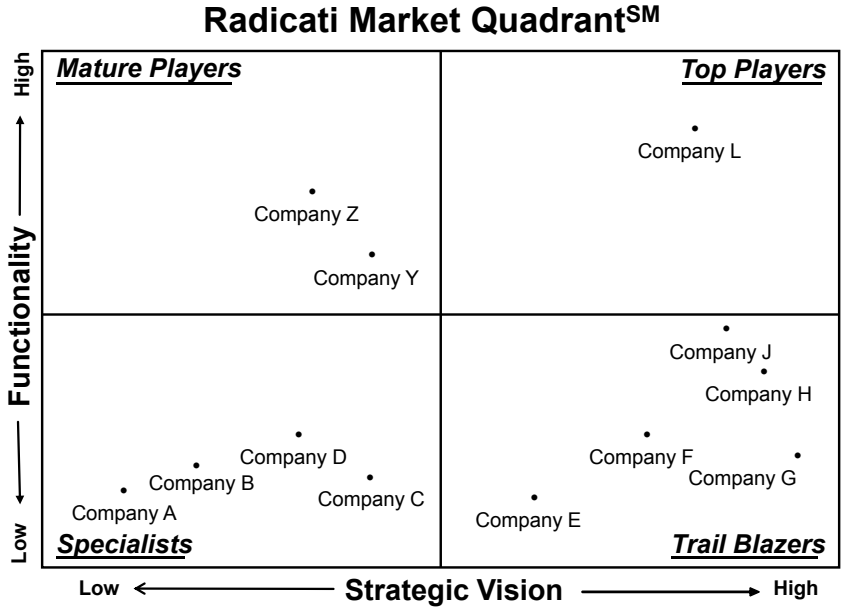

Figure 1: Sample Radicati Market Quadrant

INCLUSION CRITERIA

We include vendors based on the number of customer inquiries we receive throughout the year. We normally try to cap the number of vendors we include to about 10-12 vendors. Sometimes, however, in highly crowded markets we need to include a larger number of vendors.

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*, *Cisco*, *Clearswift, Forcepoint, iboss, Kaspersky Lab, McAfee*, *Sophos*, *Symantec, Trend Micro*, *Trustwave*, and *Zscaler*.

- 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.

- Corporate Web Solutions are available in multiple form factors, including appliances, virtual appliances, cloud services and hybrid models.

- Cloud and hybrid web security solutions are seeing strong adoption. Nearly all vendors that previously offered appliances have added a cloud based option to their portfolio. Customers often opt for a hybrid deployment as a stepping stone to a full cloud based solution, or to accommodate different requirements from various parts of their organization (e.g. headquarters vs. roaming workforces).

- Corporate Web Security vendors are also expanding the Data Loss Prevention (DLP) capabilities of their solutions. However, these tend to still be fairly basic compared to full scale content-aware DLP solutions and most large organizations will typically also 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 $3.7 billion in 2019, to an estimated $6.1 billion by 2023.

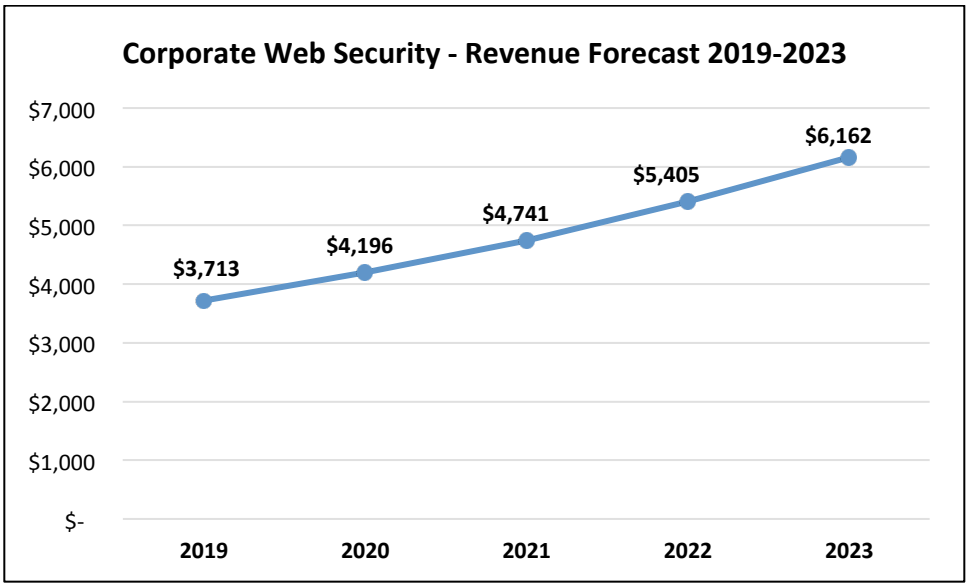

Figure 2: Corporate Web Security Market Revenue Forecast, 2019 – 2023

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.

- ***Sandboxing*** – is increasingly finding its way into web security solutions as part of advanced malware analysis aimed at detecting complex threats. Sandboxing refers to a set of techniques which allow suspect files or code to execute in a protected environment in order to detect any unwanted behavior. Sandboxing needs to be performed quickly, in near-real time, so as not to affect network performance and user productivity. Web security solutions that include some form of sandboxing will typically allow customers to set limits on its use in order to ensure it does not excessively affect employee web activity.

- ***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.

- ***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.

- ***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.

- ***Social Networking Controls*** – allow administrators to easily define, monitor and enforce policies for constructive employee access to consumer and business social networks.

- ***Cloud Access Security Broker (CASB)*** – are on-premises or cloud-based solutions that sit between users and cloud applications to monitor all cloud activity and enforce security policies. CASB solutions can monitor user activity, enforce security policies and detect hazardous behavior, thus extending an organization's security policies to cloud services. Integration with a CASB solution is becoming an increasingly important aspect of a well designed web security posture.

- ***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.

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

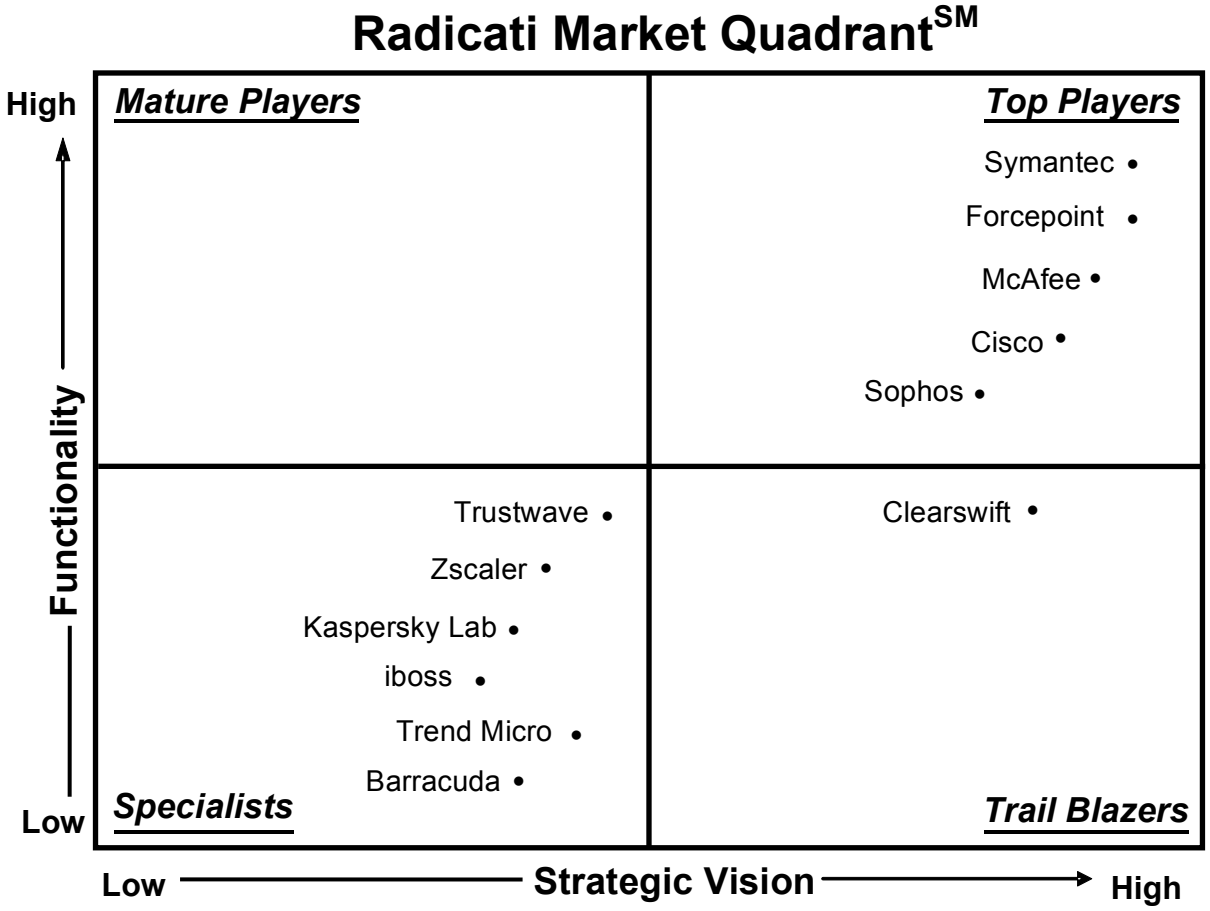

Figure 3: Corporate Web Security Market Quadrant, 2019·

· Radicati Market Quadrant℠ is copyrighted March 2019 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 *Symantec, Forcepoint, McAfee, Cisco,* and *Sophos***.**
- The **Trail Blazers** quadrant includes *Clearswift.*
- The **Specialists** quadrant includes *Trustwave*, *Zscaler*, *Kaspersky Lab, iBoss, Trend Micro,* and *Barracuda Networks*.
- There are no **Mature Players** in this market at this time.

CORPORATE WEB SECURITY - VENDOR ANALYSIS

TOP PLAYERS

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. Symantec is publicly traded.

SOLUTIONS

Symantec's Web security portfolio includes solutions from its acquisition of Blue Coat, legacy Symantec solutions, and the 2018 acquisition of Fire Glass. All Symantec web security solutions are backed by the Symantec Global Intelligence Network, that offers real-time protection from malware and real-time URL filtering. The solutions also offer real-time reputation based malware filtering which helps detect new, targeted attacks. In addition to web security options, available adjacent integrations include integration with Web Isolation, Symantec Mail Gateway, Symantec DLP, and Symantec CASB (CloudSOC), and Symantec Endpoint Protection solutions.

Symantec has also introduced the Integrated Cyber Defense eXchange (ICDX), as a platform to integrate Symantec and partner security solutions.

In the Web Security space Symantec provides the following solutions:

- **Symantec Web Security Service (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 cloud solution 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 Symantec'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 by the Web Security Service via a Unified Agent, or, if using Symantec Endpoint Protection, can simply configure Internet traffic to redirect to the Web Security Service. WSS also includes Intelligence Services feeds, including the CASB cloud application identifiers and attribute data (for Shadow IT risk protection) and web application controls.

    - *DLP* – WSS is available with Symantec's cloud DLP offering, or can be directly integrated with an organization's on-premises DLP deployment.

    - *Web Isolation* – adds a browser isolation service, allowing web site browsing to occur on a remote web browser, so the end-user is isolated from any malicious activity. Web Isolation can be used on unknown or risky sites, as well as for privileged users, and used in a read-only mode to protect against URLs from phishing emails.

    - *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.

    - *Malware Analysis Service* – offers cloud-based sandboxing, available in standard and advanced service levels.

- **Blue Coat ProxySG and Advanced SG (ASG)** – are available as an appliance or separate 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:

  - *Symantec 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 Intelligence Services solution is continuously updated by the Global Intelligence Network to provide better protection from malware. Symantec Intelligence Services also provides additional levels of detail on web risk levels, geo-location, CASB cloud application identifiers and attribute data (for Shadow IT risk protection) and web application controls.

  - *Web Isolation* – is an add-on product which enables browser isolation, allowing web site browsing to occur on a remote web browser, so the end-user is isolated from any malicious activity. Web Isolation can be used on unknown or risky sites, as well as for privileged users, and used in a read-only mode to protect against URLs from phishing emails.

  - *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 (as needed for data privacy and compliance), 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 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 (cloud based) 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.

- *Management Center* – allows administrators to centrally synchronize and configure ProxySG, ASG and associated 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.

In addition, Symantec plans to add Fortinet's NGFW (Next Generation Firewall) solution to its Web Security Service as a cloud firewall service in the 2019 timeframe.

Symantec also offers **Cloud Access Security Brokerage (CASB) - CloudSOC**, **Cloud Data Protection (CDP)** and **Advanced Threat Protection (ATP)** solutions, which augment its web security product portfolio. Products in Symantec's Advanced Threat Protection solution set include: **Content Analysis System**, **Malware Analysis Appliance**, **SSL Visibility Appliance**, and a **Security Analytics Platform**.

STRENGTHS

- Symantec's Web Security Solutions can be deployed as appliances, services or hybrid offerings.

- Symantec offers a broad range of security solutions, including email security, endpoint protection, Data Loss Prevention, security analytics, CASB, CDP, SSL visibility and more to complement its Web Security Solutions.

- Symantec integrated data protection features pick up all the dictionaries, standard policies and templates of the greater Symantec DLP solution and applies them to the web security.

- Symantec's Global Intelligence technology combines traffic pattern, behavioral, server and site DNA, content and reputation analysis.

- Symantec'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.

WEAKNESSES

- Symantec on-premises Web security solutions are somewhat complex and are a good fit for medium and large customers with experienced security and IT teams. However, Symantec's cloud solutions are increasingly a good fit for customers of all sizes.

- Symantec Web Security solutions, while highly feature rich, are priced somewhat higher than many competing solutions.

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

FORCEPOINT

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

Forcepoint is a Raytheon Company and Vista Equity Partners joint venture formed in 2015 out of a combination of Websense and Raytheon Cyber Products. Forcepoint offers a systems-oriented approach to insider threat detection and analytics, cloud-based user and application protection, next-generation network protection, data security and systems visibility.

SOLUTIONS

Forcepoint's solutions rely on its 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 Web Security** – can be deployed in the cloud, on-premises or as hybrid appliance with a cloud deployment. Forcepoint Web Security includes native CASB functionality, with cloud application discovery and risk reporting of shadow IT with access to a cloud application catalog with over 10,000 applications. It can be enhanced through several advanced protection modules which include:

    - *Forcepoint Cloud Application Module* – provides an inline (proxy) CASB functionality integrated with Web Security to control up to 15 sanctioned cloud applications. This module offers granular proxy-based cloud application controls, user behavior analytics, anomaly detection , and detailed device control for cloud applications.

    - *Forcepoint Advanced Malware Detection* – provides malware and threat activity defense through dynamic behavioral analysis of advanced, targeted zero-day threats and advanced persistent threats (APTs) that may attack through various channels.

    - *Forcepoint DLP for Web* – prevents data loss of intellectual property due to external threats or accidental/inadvertent employee behavior, through integrated enterprise-class DLP with Incident Risk Ranking to automatically identify incidents posing the greatest risks. The fully integrated DLP engine enables regulatory compliance with over 2,000 pre-defined policies and templates in a single console.

    - *Forcepoint Mobile Security* – extends policies and security settings to Android and iOS devices. Protects against mobile malware, malicious apps, SMS spoofing, phishing, and Web threats and data loss. MDM features are currently provided through an integration with VMware (AirWatch).

- **Forcepoint CASB** – provides visibility and control for cloud applications such as Office 365, Google G Suite, Salesforce and others. It enforces security policies for all endpoint devices including BYOD and access points (mobile apps and browsers). It helps protect data stored in cloud storage services through DLP and Forcepoint Advanced Malware Detection.

STRENGTHS

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

- Forcepoint Web Security integrates with additional IT security elements from Forcepoint, such as email security, while maintaining a single management interface. Forcepoint Web Security Cloud can be added to Forcepoint Next Generation Firewall (NGFW) for advanced protection.

- Forcepoint offers strong CASB functionality, through its Cloud Application Module, which integrates with Forcepoint Web Security within the same console and using the same proxy at no additional charge, as well as its full CASB offering at an additional cost.

- 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

- Forcepoint solutions are a best fit for mid-size and large enterprises with advanced needs.

- Forcepoint solutions tend to be more expensive than competing web security solutions but do include greater functionality, such as basic DLP and CASB capabilities, at no extra cost.

- Forcepoint does not offer its own sandboxing technology, but delivers sandboxing through a partnership with Lastline, for best-in-class sandboxing technology.

MCAFEE

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

McAfee delivers security solutions and services for business organizations and consumers. The company provides security solutions, threat intelligence and services that protect endpoints, networks, servers, the Cloud and more.

SOLUTIONS

McAfee Web Protection is the company's flagship hybrid Web security solution that protects users from inbound and outbound threats. It is also available in different versions: **McAfee Web Gateway**, available as an on-premise hardware appliance, virtual appliance, or an AWS based appliance; and **McAfee Web Gateway Cloud Service**, a cloud-based option. The different solutions may be deployed together 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 emulation engine is accompanied by McAfee'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 McAfee technology.

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

- *Off-network protection* – as an alternative to PAC files, which can be used, 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 administrators to set granular policies of more than 6,000 Web applications and application sub-functionalities. Customers can also input custom application signatures for broader Web application controls.

- *Reporting* – is accessed in 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, policies can be immediately updated from the reports created. The standalone SaaS option includes its own standalone reporting in ePO cloud.

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

In 2018, McAfee acquired Skyhigh Networks, a CASB solution provider, and has been rebranded it as MVISION Cloud. McAfee has provided the first integrations of its DLP and Web capabilities with MVISION Cloud. Currently, McAfee Web Gateway can send web logs to McAfee MVISION Cloud for a comprehensive Shadow IT report. From these reports, customers can create lists of cloud services (referred to as Service Groups) that can be utilized on either the web gateway appliances or the cloud service. Policy decisions include blocking, allowing access or creating specific policies.

STRENGTHS

- McAfee Web Protection has its own management solution that can manage both the on-premises software and cloud service from a single interface. It 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, which allows for central reporting for all McAfee solutions across the enterprise.

- McAfee offers a broad range of security solutions that can be deployed alongside its Web Protection solution, such as endpoint protection, malware sandboxing, data loss prevention (DLP), and more.

- McAfee 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 McAfee 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.

- McAfee is in the process of integrating its Web capabilities with its CASB, McAfee MVISION Cloud solution, to provide its customers with added cloud visibility and protection.

WEAKNESSES

- Reporting granularity could be improved.

- McAfee's management interface, while highly sophisticated, could be improved with a better graphical user interface and easier rule creation.

- McAfee does not offer an email gateway solution, which may disappoint customers looking to acquire their email and web protection solutions from a single vendor.

CISCO

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

Cisco is a leading vendor of Internet communication and security technology. Cisco has invested in a number of acquisitions over the last six years, including Duo, Viptela, OpenDNS, Cloudlock, Sourcefire, and ThreatGrid, that have come together to form its overall security portfolio. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), made up of leading threat researchers. Cisco is publicly traded.

SOLUTIONS

Cisco offers a suite of corporate web security solutions, which comprise: **Cisco Web Security Appliances (WSA)**, a set of on-premises appliance based solutions; and **Cisco Cloud Web Security (CWS)**, a cloud based solution which is transitioning to **Cisco Umbrella**, a cloud-delivered secure internet gateway. Umbrella and WSA both leverage Cisco Advanced Malware Protection (AMP) and Talos threat intelligence. AMP is Cisco's cloud-delivered file reputation as well as static and dynamic file analysis service that powers the entire Cisco Security portfolio. Talos is Cisco's expansive threat intelligence engine and research team, which scans and blocks billions of web activities every day. Other threat protections, such as Cisco web reputation and

Umbrella statistical & machine learning models, are also cloud-delivered and shared across all platforms.

Cloud-based Web Security Solutions

- **Cisco Umbrella (DNS and web level security)** – is a cloud security solution that provides the first line of defense against Internet threats. It delivers visibility into Internet activity across all locations, devices, and users (on and off network), even when not connected to a VPN. By analyzing and learning from Internet activity patterns, Umbrella can automatically uncover attacker infrastructure staged for current and emerging threats, and proactively block requests to malicious destinations before a connection is established. It provides the following key features:

  - *Visibility and protection everywhere* – ensures there are no gaps off the network, over non-web ports and protocols, and for all locations where appliances, tunnels or PAC files are too complex to set up.

  - *Machine learning* – uncovers known and emergent threats, and blocks connections to malicious destinations at the DNS and IP layers. Using Umbrella machine learning and statistical models, Cisco Talos web reputation, and other third party feeds, Umbrella blocks malicious URLs at the HTTP/S layer, as well as blocks the downloading of files from risky sites.

  - *Open platform built for integration* – open APIs help integrate across Cisco's entire security portfolio, as well as with third parties like FireEye, Checkpoint, Splunk, Alienvault, and Phishme.

  - *Anycast routing* – data centers announce the same IP address, so requests can be sent transparently sent to the fastest available with automated failover. Umbrella has peering partnerships with a large number of ISPs and CDNs that provide shortcuts between networks, allowing faster request resolution.

  - *No hardware to install or software to manually update* – Umbrella uses DNS as the main mechanism to get traffic to its platform for inspection. Additionally, customers can leverage their existing Cisco footprint, Cisco AnyConnect, Cisco routers (ISR 4K series),

Meraki, SD-WAN (Viptela) and Cisco Wireless LAN controllers, to quickly provision thousands of network devices and laptops. It represents a modern (micro-services) platform-based approach, which makes it easier for organizations to acquire, deploy, and manage a broad set of web security protection from a single vendor.

- *Migration to the cloud* – Cisco offers Cisco Defense Orchestrator, to help existing customers of Cisco WSA migrate to the cloud.

- *Roaming* – extends protection to roaming employees, including when they are off the VPN. The Umbrella roaming client provides visibility and enforcement at the DNS-layer. It is also integrated into Cisco's AnyConnect VPN client, making it a simple deployment for existing AnyConnect users.
- Cisco is aggressively expanding the capabilities of Umbrella to include Secure Web Gateway (full proxy), cloud-delivered firewall and CASB capabilities in one management console.

- **Cisco Cloud Web Security (CWS)** – is a traditional cloud-based solution that offers a broad set of malware protection, URL filtering, and Web application controls. Cisco began the end of life process for CWS in 2019, and customers are being offered incentives to migrate to the Umbrella Secure Internet Gateway.

Appliance-based Solutions

- **Cisco Web Security Appliances (WSA)** – are available in the S-Series lineup, which comes in various versions: **S690** for large enterprises (> 10,000 users), **S390** (for mid-size companies with < 10,000 users), **S190** (for small companies with < 1,000 users). All **x90** appliance models are built on Cisco UCS hardware. Cisco also offers virtual appliance models that run the same software as physical appliances. Currently, Cisco offers four VM models – S00v, S100v, S300v and S600v. These VM models are supported on VMware, Hyper-V and KVM hypervisors. For customers who wish to deploy WSAs in the public cloud, the WSA image is also offered in AWS.

STRENGTHS

- Cisco offers a broad portfolio of Web Security solutions can be deployed as appliances, cloud-based, network integrated, or hybrid solutions.

- Cisco Umbrella delivers a broad set of web security capabilities in one platform, that normally require separate solutions (typically from different vendors).

- Cisco provides strong support for mobile device web use via its AnyConnect Secure Mobility Client.

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

- Cisco has integrated a traffic redirection feature into many 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 offers bandwidth controls but does not offer dynamic traffic shaping.

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

- While Cisco has delivered CASB, Meraki and Viptela integrations over the past year, there is still room for further integrations across Cisco products to strengthen its overall web security portfolio.

- Cisco does not currently support common policy deployment across its WSA and Umbrella portfolio. The vendor needs to address this to help ease administration of hybrid deployments.

- Cisco is evolving its cloud Umbrella portfolio at a rapid pace, and driving customers of CWS to the Umbrella platform. Customers should check carefully on feature availability and bundling of the different solutions.

SOPHOS

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

Sophos offers IT security solutions for businesses, which include encryption, endpoint, email, Web, next-generation firewall (NGFW), and more. All solutions are connected with Sophos Central, Sophos's cloud-based management platform, and backed by SophosLabs, its global network of threat intelligence centers. The company is headquartered in Oxford, U.K., and is publicly traded on the London Stock Exchange.

SOLUTIONS

Sophos currently offers web security through several products including: Sophos Web Appliance, cloud-based Central Web Gateway, the Sophos UTM product line, and next-gen XG Firewall. All share the same security capabilities and have similar ranges of other web filtering functions appropriate to the product and deployment method.

- **Sophos Web Appliance** – is available as a hardware or virtual appliance. It can integrate via the cloud with Sophos's endpoint security solution. This combination provides web security, policy, and reporting for off-site users without the need to route web traffic through a cloud gateway. The solution also comes with Sophos's Managed Appliance capabilities, that lets Sophos provide direct support to customers' deployments, such as updates and troubleshooting. Sophos Management Appliance provides centralized management and load-balancing for multiple gateways and is included in the gateway subscription.

- **Sophos Central Web Gateway** – provides cloud management, reporting, enforcement and advanced protection for computers and mobile devices both on and off the corporate network. It offers high performance, instant visibility and granular policy control.

- **Sophos XG Firewall** and **Sophos SG UTM –** provide comprehensive Web Gateway functionality. XG Firewall also offers cloud app visibility and shadow IT detection functionality, and a solution that leverages a heartbeat connection between gateway and

endpoint to identify unrecognized application traffic.

Sophos also integrated web protection into the Sophos Endpoint solution, with full web control and protection capabilities, as well as the ability to share a common policy definition with the gateway products.

All Sophos Web Gateway solutions include:

- *Threat protection* – provided by Sophos's own proprietary technology that originates from SophosLabs. The proprietary threat technology uses reputation, anti-virus signatures, behavioral analysis, and more to identify malicious downloads and web content. Sandboxing is also available.

- *URL filtering* – based on comprehensive built-in URL categories, or custom categories, which can be defined as required. The products can display warnings or apply usage quotas in addition to simply blocking unwanted content.

- *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 solutions 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. XG Firewall also provides extensive content scanning for sensitive terms.

- *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. 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. Sophos is also developing a new approach which will provide a single point for managing web policies and usage reporting for on-premises and roaming network users, with enforcement coordinated across firewall, gateway, endpoint and network devices, thus making it easier to apply one policy consistently everywhere.

STRENGTHS

- Sophos offers flexible deployment options including cloud and on-premises, with comprehensive Web Gateway functionality also available in next-generation Firewall, UTM and Endpoint products.

- Sophos XG Firewall features Synchronized App Control, a solution that leverages a heartbeat connection between gateway and endpoint to identify unrecognized application traffic based on the endpoint process that generated it. This feature provides deep visibility into traffic that other solutions might just group as generic HTTP or HTTPS.

- Sophos XG Firewall offers cloud app visibility and shadow IT detection functionality, which allows customers to monitor the use of cloud apps and quickly identify new or unsanctioned app usage.

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

- In addition to detecting malware and other unwanted applications, Sophos's threat detection inspects Javascript and active web content to detect early-stage and in-browser attacks, including in-browser crypto-mining code.

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

- Sophos offers both network and endpoint security solutions, with Sophos Synchronized Security offering adding value to customers that use multiple products.

WEAKNESSES

- Sophos solutions are aimed at organizations that value simplicity, ease of use and reliability, rather than delivering extensive customization features.

- Sophos's cloud-based and appliance-based Web Gateway solutions offer different levels of functionality, customers should check carefully to determine which solution best fits their protection needs.

- Sophos web security DLP capabilities are currently limited to preventing users from posting data to a range of sites including webmail and blogs, and the detection of sensitive content in files uploaded and downloaded to the Internet.

- Currently, Central Web Gateway and Sophos Web Appliance solutions have separate management interfaces when deployed together as a hybrid solution. However, integrated cloud-based management of hybrid deployments, including on-premises gateway, endpoint, mobile and cloud protection, is on the vendor's roadmap.

TRAIL BLAZERS

CLEARSWIFT

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

Founded in 1982, Clearswift is a UK-based security company that offers cyber-security solutions to protect business's data from internal and external threats.

SOLUTIONS

Clearswift offers threat protection through its Clearswift's Aneesya platform. As part of this platform, the **Clearswift SECURE Web Gateway** is powered by the Clearswift's Deep Content Inspection engine, which shares policies across email, web and endpoint solutions. The Clearswift SECURE Web Gateway can be deployed as a physical or virtual appliance on-premises, in the cloud (including AWS and Azure), or in hybrid environments, a hosted solution or a managed service is also available.

The solution offers the following features:

- *Anti-virus and URL classification* – downloads can be check for viruses by up to three anti-virus engines, while URL classification enables granular filtering by topics.

- *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. This includes web pages, as well as downloaded files.

- *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.

- *ICAP Integration* – A modified version of the SECURE Web Gateway, the SECURE ICAP Gateway is available for use with ICAP enabled proxies. This can be used in both forward and reverse proxy configurations, providing the Clearswift advanced features without having to rip and replace existing hardware.

- *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. Granular policies based on time and quota access are also available.

- *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 as a cloud solution.

- 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 simpler and consistent enforcement of unified corporate security policies.

- Clearswift Adaptive Data Loss Prevention features provide advanced 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 integration and monitoring can also be easily configured through the web UI.

- Adaptive Redaction technology allows the modification of traffic to comply with corporate policies 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 offer sandboxing functionality. However, the vendor has this on its roadmap for 2019.

- Clearswift does not provide its own CASB functionality, but offers this in partnership with 3rd party vendors.

- 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 help 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 2015, Trustwave was acquired by Singtel, Asia's leading communications group. Trustwave is now a standalone business unit and core cyber-security 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. **Trustwave Secure Web Gateway (SWG)** is Trustwave's flagship Web security product that provides 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, or as a multi-tenant 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. 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. SWG also has 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 also has granular controls for cloud drives including Dropbox, Google Drive, Box, Amazon Drive, Microsoft 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 through 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. Trustwave 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 further expand the scope of DLP controls to include third party best of breed DLP via ICAP integration.

The Trustwave **Managed Secure Web Gateway (SWG) Cloud service** offers the same features as Trustwave SWG in a cloud form factor. 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 SWG Cloud 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", where if a customer demonstrates any known or unknown malware missed by the solution, Trustwave will add a free month to their subscription, up to once per quarter.

Trustwave offers an inline Malware Analysis Sandbox option, which blocks malicious files with minimal impact on user experience. Together with the Malware Entrapment Engine, it combines to provide real-time protection against unknown and dynamic malware delivered through web pages and files.

The Trustwave Managed SWG Cloud service 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.

Trustwave also offers a Security-as-a-Service (SaaS), or all cloud, version of the Managed SWG service. The service includes 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. The multi-tenant cloud offering better serves distributed customers and offers better policy coverage for roaming laptops off the corporate network.

Trustwave WebMarshal scans incoming and outgoing traffic to protect against threats on the Web. The solution can be deployed 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 (e.g. 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 SWG is available in various form factors, including as a managed service, traditional appliance, virtual appliance, a hybrid (i.e. on-premises and cloud), and as a multi-tenant cloud managed solution.

- Trustwave provides managed SWG customers with a Zero Malware Guarantee, where if any malware is shown to get past Trustwave's SWG, the customer gets a free extra month of service (up to once/quarter).

- 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 recently introduced a new, VPN-based, SWG Cloud Mobile Security Service.

- 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.

WEAKNESSES

- Although remote and mobile workers can be protected with Trustwave's Web security solutions, the vendor has limited native protection for mobile OS devices. This is being addressed in a future offering.

- Trustwave does not provide its own CASB functionality, but offers CASB through a partnership with Netskope.

- 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.

- Trustwave lacks market visibility.

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. In 2018, Zscaler acquired the machine learning technology and development team of TrustPath. Zscaler is publicly traded.

SOLUTIONS

Zscaler Web Security, part of the Zscaler Cloud Security Platform, offers a 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 and 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 Zscaler's user installed base in near real-time.

- *DLP* – 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* – Zscaler offers closed loop integration with Microsoft's Cloud Application Security (CASB) functionality, Microsoft Cloud App Security, to help monitor, protect and control cloud application usage 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.

Zscaler also operates Zscaler Internet Access-Government (ZIA-Government) which is FedRAMP certified for deployment by US federal agencies.

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 totally SaaS based security approach helps reduce total cost of ownership, as customers do not need to purchase and manage software or hardware appliances.

- Zscaler's SaaS approach dovetails well with organizations fully vested in the deployment of a fully cloud based IT infrastructure and cloud applications.

WEAKNESSES

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

- Zscaler no longer offers email security as part of its service portfolio, which may disappoint customers looking to source both web and email security from a single vendor.

- 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, 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.

- Zscaler customers reported scaling issues and faulty functioning of VPN functionality as affecting their deployments.

KASPERSKY LAB

39A/3 Leningradskoe Shosse
Moscow 125212
Russian Federation
www.kaspersky.com

Kaspersky Lab is an international group, which provides a wide range of security products and solutions for consumers and enterprise business customers worldwide. The company's business solutions are aimed at a broad range of customers including large enterprises, small and medium-sized businesses. Kaspersky Lab is privately owned.

SOLUTIONS

In the web security space, Kaspersky Lab offers **Kaspersky Security for Web Gateways,** a solution which currently contains a single on-premises application, **Kaspersky Antivirus for Proxy**, which is in the process of being replaced by the new **Kaspersky Security for Proxy,** which can be used in cloud deployments to deliver broader functionality. Kaspersky Security for Proxy is an application that integrates proxy servers using ICAP.

The solution comprises the following functionality:

- *Malware detection* – Kaspersky Security for Proxy uses multiple security layers to identify malware, including precise detection, machine learning-powered structure heuristics, reputation based filtering, and more.

- *Sandboxing* – Kaspersky Web Traffic Security uses emulative sandbox allowing analyzing the behavior of any object as it executes in a safe virtual environment to protect against even sophisticated, heavily obfuscated malware. It integrates with the Kaspersky Anti Targeted Attack (KATA) platform through an external ICAP-protocol sensor.

- *URL Filtering* – Kaspersky Web Traffic Security organizes URL filtering by categories and user dictionary to restrict certain categories of web resources to reduce risk, and ensure

uninterrupted work without unwanted distractions. Access to a cloud-based URL reputation database (updated in real time) is also available via the Kaspersky Security Network (KSN) and the Kaspersky Private Security Network (KPSN).

- *Web application controls* – Kaspersky Web Traffic Security can be used in combination with Kaspersky Endpoint Security agents on any platform (Windows, Linux, Android) to provide capabilities to block web applications according to defined policies.

- *SSL scanning* – Kaspersky Security for Proxy scans SSL traffic based on surveillance characteristics set up by administrators through the use of system tools. Ready-to-use settings for SSL traffic surveillance are available in an all-in-one appliance version.

- *Reporting* – centralized events management, log management, dashboard, and integration with SIEM solutions give system administrators flexible options to investigate problems and create reports on-site.

- *Administration* – Kaspersky Web Traffic Security offers a flexible easy-to-use management console to control all ICAP-capable systems' security, including proxies and storage, via a single-point web interface, which provides visibility and manageability for security administrators.

STRENGTHS

- Kaspersky Security for Proxy offers multi-layered threat protection with high expandability, where additional security layers can be added as needed.

- Kaspersky Web Traffic Security integrates with a powerful threat detection and response platform consisting of Kaspersky Anti-Targeted Attack (KATA) and Kaspersky Endpoint Detection and Response (KEDR).

- Kaspersky Security for Proxy is available as a multi-tenant solution making it a good fit for organizations that want to outsource their IT needs.

- Kaspersky Security for Proxy leverages an architecture specifically developed for cloud deployment, with access to Kaspersky's own powerful threat intelligence, including constantly updated black- and whitelisting databases, a reputation database and targeted

attack-related hosts database.

- Kaspersky Web Traffic Security offers full integration with Active Directory (AD) allowing for powerful role-based access control (RBAC) and rules management through a centralized interface.

WEAKNESSES

- Kaspersky Security for Proxy needs to add complete unified management along with protection for other infrastructure elements (e.g. endpoints, servers, storage, and others).

- Kaspersky Security for Proxy needs to improve the granularity of its web application management controls.

- Kaspersky Security for Proxy needs to add more advanced reporting functionality.

- Kaspersky does not offer a CASB solution, however, it provides APIs for integration with third party CASB solutions.

- Kaspersky offers limited DLP capabilities, however, it supports ICAP for integration with full-scale third party DLP solutions.

IBOSS
101 Federal Street, 23rd Floor
Boston, MA 02110
www.iboss.com

iboss, founded in 2003, delivers cloud-based cyber-security by leveraging an elastic, node-based architecture of its own design. iboss targets mid to large organizations, education, and local government organizations. iboss is a privately held company.

SOLUTIONS

The iboss **distributed gateway platform** is an elastic, distributed, non-shared web gateway architecture that enables the transition from legacy appliances to the cloud. It provides feature

and function parity across all devices, users, and locations, all managed in the cloud by a single pane of glass.

The iboss Distributed Gateway Platform includes a broad range of content filtering, malware detection, advanced threat protection, and management features, including:

- *Web content filtering* – effectively blocks access to harmful, objectionable, or otherwise unwanted online content. It includes the following capabilities: stream-based protection covering all ports and protocols, granular category and user based filtering, alerts on user-defined keywords and events, port access management, and a dynamic, real-time URL database.

- *Malware Prevention* – a set of malware detection and prevention capabilities that protect against viruses, worms, Trojans, ransomware, and attacks that use evasive applications (e.g. TOR). Key features include: signature-based malware prevention and breach detection, command and control callback monitoring across all ports and protocols, automated locking of infected devices, crowd-sourced threat intelligence, and rapid response capabilities.

- *SSL traffic management* – monitors and manages the growing amounts of SSL traffic on organizations' networks, enabling them to detect, block and respond to SSL-based threats faster and more effectively. Capabilities include: fast, scalable SSL decryption, and micro-segmentation for selective decryption based and content, device, user, group, or other user-defined parameters.

- *Bandwidth monitoring and shaping* – gives organizations complete visibility into their bandwidth utilization, ensuring availability by spotting problems and curbing misuse. Key capabilities include: centralized policy and threshold setting, monitoring, and controls for ensuring bandwidth availability at critical times and locations.

- *BYOD and Guest Wi-Fi management* – reduces the risks presented by BYOD devices and guest Wi-Fi users with integrated BYOD management. Capabilities include: identification of BYOD users not using a NAC and automated binding to the network directory or LDAP, advanced application controls, and automatic high-risk quarantine.

- *Single Platform Orchestration* – provides single-pane-of-glass management with real-time visibility across all locations and devices. Capabilities include: cloud-based administrative

console with responsive web UI, bi-directional policy management, seamless directory integration and group management, and system delegated administrators.

- *Customized, real-time reporting* – streamlines the production of timely, accurate reports for a range of compliance and internal management purposes. Automated reporting capabilities include: comprehensive drill-down reports; live, historical, and statistical reports; and easy report scheduling and customization. Also includes native Splunk integration and SIEM integration for forensic-level reporting.

- *Network anomaly detection and data hijacking prevention* – monitors packets, bytes and connections across all data channels to establish baselines of normal network traffic. Automatically detects anomalous behavior, contains malware that causes it, and stops the activity before data loss occurs. Includes data flow restrictions by country, organization, or subnet, with fully configurable thresholds. Delivers full-stream protection, including TCP and UDP ports, and provides real-time alerts and drill-down forensics for anomalous traffic.

- *Intrusion detection & prevention (IDPS)* – delivers effective, real-time detection and prevention of network breaches by viruses, worms and other categories of malware. Includes an automated data feed of threat signatures with frequent updates. Provides instantaneous views of event details, including source and destination IP addresses, and easy rules creation and editing.

- *Incident response center* – analyzes and prioritizes security incidents to enable faster and more effective responses. Automatically translates and correlates data from security event logs in real-time to identify the most serious incidents that require prioritized and expedited remediation.

- *Sandboxing* – leverages file detonation in a controlled sandbox environment for signature-less malware detection.

- *Cloud Application Security Broker (CASB)* – offers controls and visibility into cloud application use. It provides extensive controls for Spotify, Pinterest, Facebook, Twitter, LinkedIn, and Search Engines. As well as controls for the suite of Google Apps, including Google Drive. It integrates natively with Office 365, Microsoft Azure, and Microsoft Cloud App Security (CAS).

- *Cyber risk scoring* – powered by industry-leading analytics technology from FICO, it automatically identifies and scores the cyber risks posed by specific users and devices. It leverages proprietary algorithms to quickly spot breaches that other systems may miss, including attacks using TOR.

- *Mobile device management* – provides the ability to monitor, manage, and secure mobile devices anywhere, any time. Includes granular application management, application locking or pushing, and live device location Geo-Mapping.

STRENGTHS

- iboss offers a flexible entirely SaaS cloud-based model, available in easy to understand and competitively priced packaging options.

- iboss integrates Baselining and Network Traffic Anomaly Monitoring, which serves to continuously monitor network traffic to detect anomalous behavior and contain traffic being ex-filtrated 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 mean time 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

- iboss's administrative interface, while delivering a comprehensive set of capabilities, could be improved through a more intuitive graphical interface and streamlined policy creation.

- iBoss CASB functionality is based on integration with Microsoft Cloud App Security (CAS), rather than its own technology.

- While iboss has regional offices in APAC and EMEA, the vendor still needs to develop its market presence in these regions.

- iboss has a strong presence in the Education K-12 sector, however the company needs to raise its visibility in other market sectors.

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 is publicly traded.

SOLUTIONS

Trend Micro solutions are powered by its cloud-based Trend Micro Smart Protection Network, which brings together threat reporting and analysis based on a worldwide threat assessment infrastructure. Trend Micro XGen security provides automatic sharing of threat intelligence across endpoints, network components, data centers and cloud services.

Trend Micro Secure Web Gateway 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 Secure Web Gateway includes:

- **InterScan Web Security Virtual Appliance** – an on-premises web gateway security virtual appliance. It offers web filtering, app control, cloud-based reputation filtering, and gateway antivirus scanning.

- **InterScan Web Security as a Service** – a cloud-based web security solution. It also features web filtering, app control, cloud-based reputation filtering, and gateway antivirus scanning.

- **Trend Micro Control Manager** – a centralized, user-based security management console to manage across both on-premises appliance and cloud deployment models.

Trend Micro Secure Web Gateway solutions include 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 Smart Protection Network, which pushes updates to provide zero hour protection. Sandboxing is also provided as an option through the **Trend Micro Deep Discovery Analyzer**.

- *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.

- *Application control* – monitors a wide range of protocols and applications, including instant messaging, peer-to-peer, social networking applications, and streaming media.

- *DLP* – is available through an add-on module. It offers over 200 out-of-the-box DLP templates to satisfy major compliance requirements and protect sensitive data.

Trend Micro Advanced Reporting and Management is an optional add-on for Secure Web Gateway solutions to expand reporting capabilities. It offers real-time data and analytics for individual user behavior. Trend Micro Advanced Reporting and Management is commonly deployed as an aid in policy creation and refinement. Secure Web Gateway solutions 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 its on-premises and cloud-based web security solutions 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.

- Trend Micro offers comprehensive, drill-down reports that enable real-time, detailed tracking of individual user actions.

WEAKNESSES

- Trend Micro provides separate management interfaces for its appliance and cloud based web security solutions, as well as a third console for hybrid deployments. This is somewhat cumbersome for organizations that are evolving their deployment from on-premises to cloud.

- Trend Micro offers only basic DLP support.

- Trend Micro offers limited CASB functionality through Cloud App Security solution for Office 365 and file sharing services, however, this is a separate solution that does not integrate with its web security solutions.

- Trend Micro offers application controls and monitoring, but does not support traffic shaping.

- Trend Micro has been slow to update its web security solutions, viewing it more as an add-on for customers of its endpoint security offerings.

BARRACUDA NETWORKS

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

Barracuda Networks, founded in 2003, provides security, archiving and storage solutions. Barracuda Networks was acquired in February 2018 by private equity firm Thoma Bravo in a move that took the company private.

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 is also enhanced through partnerships with Lastline for sandbox functionality, and Avira for heuristic and behavioral analysis of endpoint collected data.

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 proprietary, open-source and licensed anti-virus technologies that protect users from viruses, exploit kits, bot networks, and other malware. Infected clients can be isolated from the network, and administrators are alerted to initiate remediation efforts. Cloud based sandboxing for analysis of unknown or zero hour threats is available as an-add on subscription.

- *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. It also handles typo-squatted domains and common misspellings in popular urls.

- *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. For especially heavy reporting jobs there is also integration with Barracuda Report Server (BRS), an appliance specifically designed for ingesting and manipulating report data.

- *Customizable Dashboards* – allow administrators 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. Barracuda also offers **Chromebook Security Extension**, which protects Chromebook devices both on and off network without requiring traffic backhaul.

- *Wireless Access Point Integration* – is available in partnership with several WLAN AP providers including, Ruckus, Aerohive, Meru, Aruba, Clear pass and Cisco. The integration enables a single-sign onto to both the WLAN AP and the Barracuda Web Filter. Additionally, administrators can have deep visibility into user behavior and network activity. This enables organizations to better shape their wireless policies based on data about their network traffic.

- *Google Directory Services* – integrates with Google Directory Services to define policies and provide reporting.

STRENGTHS

- 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 as well as aggregate data from multiple appliances.

- Barracuda Networks is one of the more competitively priced Web security solutions on the market today.

- Barracuda Networks web security solutions can provide social media alerts based on the content of social media posts. These alerts can be archived and stored for compliance, DLP and eDiscovery.

- Barracuda offers efficient, low-cost delivery models for its Web Security appliance solutions with next-day shipping of replacement units, and a free appliance replacement every four years.

WEAKNESSES

- Barracuda Network's web security solutions are a best fit for customers with basic web protection needs. Customers with more fine-grained control needs may find the solutions somewhat basic.

- 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.

- Mobile device protection requires backhauling traffic back through the Web Security Gateway for content control and malware protection.

- Barracuda bandwidth controls are not as developed as those available from other vendors. However, Barracuda does offer extensive bandwidth management controls as part of its next generation firewall solutions, which are typically deployed along its web proxy solutions.

- Barracuda does not provide a CASB solution, or integrate with 3rd party solutions.

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.

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*
Email Statistics Report, 2019-2023	Mar. 2019	$3,000.00
Social Networking Statistics Report, 2019-2023	Feb. 2019	$3,000.00
Instant Messaging Statistics Report, 2019-2023	Jan. 2019	$3,000.00
Mobile Statistics Report, 2019-2023	Jan. 2019	$3,000.00
Endpoint Security Market, 2018-2022	Nov. 2018	$3,000.00
Secure Email Gateway Market, 2018-2022	Nov. 2018	$3,000.00
Cloud Access Security Broker (CASB) Market, 2018-2022	Nov. 2018	$3,000.00
Enterprise DLP Market, 2018-2022	Nov. 2018	$3,000.00
Microsoft SharePoint Market Analysis, 2018-2022	Jun. 2018	$3,000.00
Corporate Web Security Market, 2018-2022	Jun. 2018	$3,000.00
Email Market, 2018-2022	Jun. 2018	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2018-2022	Jun. 2018	$3,000.00
Cloud Business Email Market, 2018-2022	Jun. 2018	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Information Archiving Market, 2019-2023	Mar. 2019	$3,000.00
Unified Endpoint Management Market, 2019-2023	Apr. 2019	$3,000.00
Advanced Threat Protection Market, 2019-2023	Apr. 2019	$3,000.00

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

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