The Radicati Group, Inc.
www.radicati.com

# THE RADICATI GROUP, INC.

# Corporate Web Security - Market Quadrant 2021 *

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

***March 2021***

## 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.

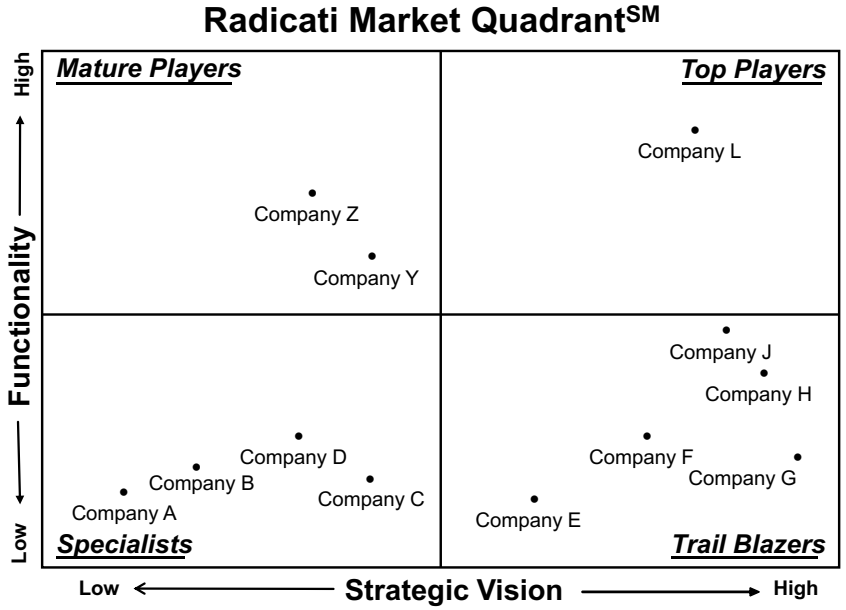


**Figure 1: Sample Radicati Market Quadrant**

## 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, McAfee*, *Mimecast*, *Sophos*, *Symantec, Trend Micro*, 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. However, customers in some highly-regulated verticals still require on-premise solutions. 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 increasingly integrating Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), Remote Browser Isolation (RBI), sandboxing technology and more, into their solutions in an effort to deliver next-generation web security solutions that better address the security needs of cloud computing environments.

- The worldwide revenue for Corporate Web Security solutions is expected to grow from over $4.6 billion in 2021, to an estimated $7.9 billion by 2025.

 

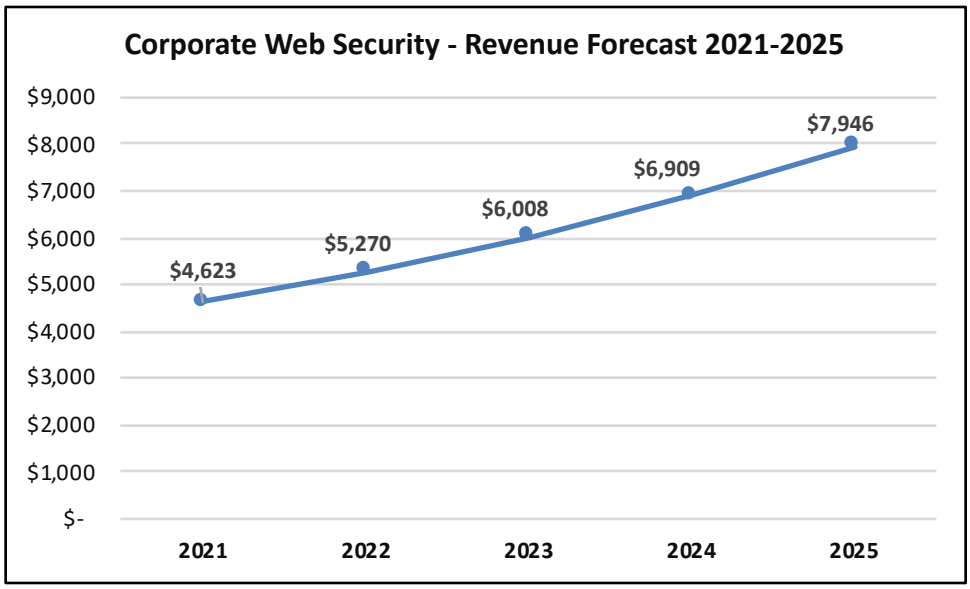


**Figure 2: Corporate Web Security Market Revenue Forecast, 2021 – 2025**

## 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, 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*** – 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.

- ***Threat Intelligence Networks*** — does the solution integrate with Threat Intelligence Networks, and is it the vendor's own intelligence network or is it based on third party Threat Intelligence feeds.

- ***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

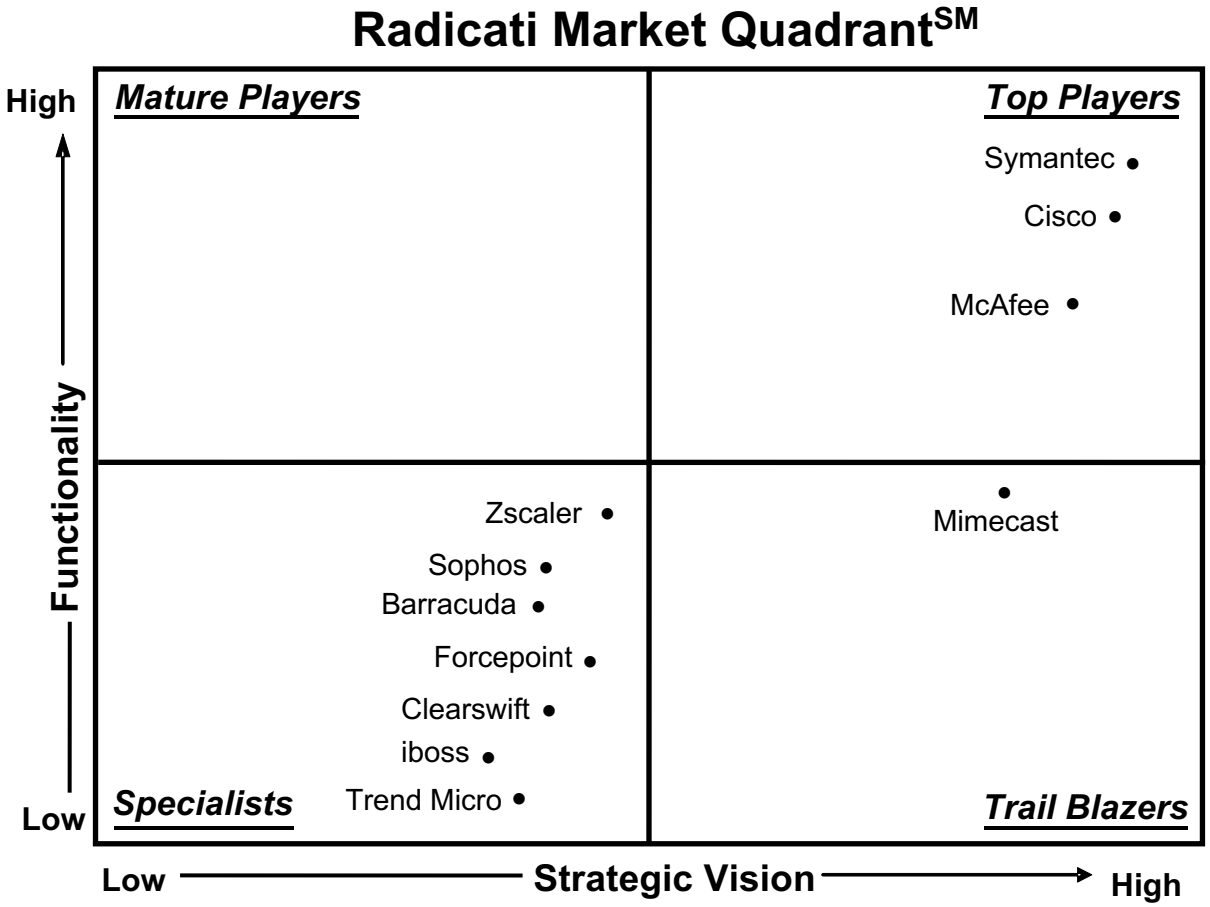


**Figure 3: Corporate Web Security Market Quadrant, 2021***

* Radicati Market Quadrant℠ is copyrighted March 2021 by The Radicati Group, Inc. This report has been licensed for distribution. Only licensee may post/distribute. 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, Cisco,* and *McAfee.*
- The **Trail Blazers** quadrant includes *Mimecast.*
- The **Specialists** quadrant includes *Zscaler, Sophos, Barracuda Networks, Forcepoint, Clearswift, iBoss,* and *Trend Micro*.
- There are no **Mature Players** in this market at this time.

## CORPORATE WEB SECURITY - VENDOR ANALYSIS

## TOP PLAYERS

### SYMANTEC, A DIVISION OF BROADCOM

1320 Ridder Park Drive
San Jose, CA 95131
www.symantec.com

Founded in 1982, Symantec has grown to be one of the largest providers of enterprise security technology. Symantec's security solutions are powered by its Global Intelligence Network, which offers real-time threat intelligence. Symantec is a division of Broadcom, a publicly traded company.

#### SOLUTIONS

Symantec's Web security portfolio is built upon a proxy-based Secure Web Gateway architecture with numerous advanced security components available in a single purchase. The Symantec SWG solution is available as cloud service, appliances, and virtual appliances. All Symantec web security solutions are backed by the Symantec Global Intelligence Network, which 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. Symantec SWG solution comprises Web Isolation, Cloud Application Visibility and Control, Content Analysis,

 

Sandboxing, Cloud Firewall Service, Zero Trust Network Access, Reporting, Centralized Management and more. In addition, adjacent integrations are available with Symantec Email Security Solutions, Symantec DLP, and Symantec Endpoint Security solutions. Symantec also offers 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 Protection Suite** – lets customers deploy a Web security solution in the cloud, at the edge, or as a hybrid solution. It is available as follows:

    - *Symantec Secure Web Gateway (Proxy)* – Symantec SWG software extends the security capabilities of Edge Proxies to support web security and enforcement of corporate and regulatory compliance. Users are also entitled to Web Security Service (WSS), which delivers the same capabilities as Symantec's on-premises Proxy solution, in a cloud service format.

    - *Intelligence Services - Advanced* – offers real-time web content protection, security categorization and web application control. The web filtering service automatically filters and categorizes billions of URLs into over 80 predefined categories, including 12 security categories that can be easily managed by IT administrators.

    - *Web Application Firewall (WAF)* – Web Protection Suite customers get WAF licenses to conduct advanced threat analysis on both inbound and outbound content to detect and protect infrastructure from attacks. Protection is provided through signature-based engines capable of blocking known attack patterns, as well as advanced signature-less engines designed to uncover unknown and zero-day attacks in the web traffic.

    - *Web Isolation* – allows 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 by privileged users, and used in a read-only mode to protect against malicious URLs within phishing emails. A *Malware Analysis Service* offers cloud-based sandboxing, which is available in standard and advanced service levels.

    - *Centralized Management & Reporting* – offers Cloud and Edge software for centralized management and reporting capabilities of the SWG infrastructure to enhance web

 

security, mitigate cloud access risks and reduce operational costs. Users can host logs in the cloud, providing visibility of all user traffic from any location.

Symantec offers the following optional add-on capabilities:

- *DLP* – Web Protection Suite can be added to the Symantec Cloud DLP offering, or can be directly integrated with an organization's on-premises DLP deployment.

- *CASB (CloudSOC)* – Web Protection Suite can be integrated with Symantec's CASB solution to protect data in motion and at rest for SaaS, IaaS and PaaS applications. Full CASB controls with ATP and DLP capabilities serve to ensure compliant and safe use of sanctioned applications.

- *ZTNA (Secure Access Cloud)* – is an agentless Software Defined Perimeter that enables Layer 7 access to corporate resources in IaaS, PaaS, and Privacy Data Center environments, including granular controls and contextual monitoring.

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

- *Cloud Firewall Service* – is an add-on capability which offers firewall protection (through a partnership with Fortinet) to all ports and protocols.

- **Symantec Proxy and Content Analysis Software** – is included as part of Web Protection Suite, as well as available independently through subscription licensing. It can be deployed on Symantec's dedicated, high-performance appliances, as separate virtual appliances or in the cloud. Content Analysis can be deployed next to Proxy on the same appliance or next to Proxy as a VM to add deep content inspection. Proxy and Content Analysis utilize the Internet Content Adaptation Protocol (ICAP) to relay requests to other appliances or cloud solutions built for a specific task, such as DLP.

  The following additional capabilities are also supported:

  - *Reporter* – provides in-depth views of user activity, Web traffic, application access, blocked sites, and more.

 

- *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 all instances of Proxy and Content Analysis, physical or virtual appliances.

Symantec also offers **Cloud Access Security Brokerage (CASB) - CloudSOC** 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** with **Malware Analysis**, **SSL Visibility Appliance**, and a **Security Analytics Platform**.

**STRENGTHS**

- Symantec 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, SSL visibility, remote browser isolation, 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 apply them to the web security offering.

- 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's 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 offer a good fit for customers of all sizes.

- Symantec Web Protection Suite is a flexible, feature-rich and attractively priced web security solution for enterprise customers. However, it is currently not available for smaller customers.

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

- Symantec offers its own, strong CASB capabilities, however, the full CASB feature set is not included in the Web Protection Suite but available as a separate solution.

## 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 security portfolio has been augmented over the last ten years through a number of acquisitions, including Duo, Viptela, OpenDNS, Cloudlock, Sourcefire, and ThreatGrid. Cisco's security solutions benefit from its threat intelligence team, Cisco Talos Intelligence Group, which relies on a broad telemetry of data that spans across networks, endpoints, cloud environments, virtual systems, and daily web and email traffic. Cisco is publicly traded.

### SOLUTIONS

Cisco offers a suite of corporate web security solutions, which comprise: **Cisco Umbrella**, a multi-function, cloud-delivered security service which is part of Cisco's SASE architecture and **Cisco Secure Web** formerly Web Security Appliance (WSA), a set of on-premises appliances or virtual solutions. Umbrella and Secure Web appliances both leverage Cisco Secure Endpoint

 

(formerly Advanced Malware Protection - AMP) and Talos threat intelligence. Secure Endpoint is Cisco's cloud-delivered file reputation, as well as static and dynamic file analysis service that powers the entire Cisco Security portfolio. Talos' statistical and machine learning models are shared across all platforms and utilized by Cisco SecureX, an XDR cloud-native platform that is provided free with all web security solutions. SecureX compiles security data from across the Cisco portfolio and a wide range of third-party security solutions to provide context, accelerate investigations, and automate remediation steps.

Cisco offers the following Cloud-based Web Security Solutions:

- **Cisco Umbrella (Secure Internet Gateway - SIG)** – is a multi-function, cloud security solution that combines DNS security, secure web gateway, cloud-delivered firewall, CASB functionality, interactive threat intelligence, and the SecureX XDR platform. It delivers visibility into cloud applications and Internet activity across all locations, devices, and users (on and off network), even when not connected to a VPN. 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. The secure web gateway inspects all web traffic (including selective or full SSL decryption) for greater transparency, control, and protection. The cloud-delivered firewall inspects all non-web internet traffic, and logs and blocks traffic using IP, port, and protocol rules for consistent enforcement throughout the customer environment.

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

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

 

- *Anycast routing* – intelligently routes traffic to the closest Umbrella data center circumventing degraded or unavailable links automatically. It provides customers with availability, reliability, and quality without the need to manage load balancers, configuration files, or routing policies.

- *Fast and flexible deployment* – PAC files, proxy chaining, Secure Client (formerly AnyConnect) or IPsec tunnels can be used to forward Internet traffic to Umbrella. A wide variety of edge devices can be used to direct traffic via a IPsec tunnel to Cisco data centers. Integrations have been built for Cisco Secure SD-WAN (Viptella) and Meraki. Cisco leverages a patent pending failover process to quickly redirect traffic in the event of a problem.

- *No hardware to install or software to manually update* – Umbrella is a cloud native service. Additionally, customers can leverage their existing Cisco footprint, Cisco Secure Client (formerly AnyConnect), Cisco routers (ISR 4K series), Meraki, SD-WAN (Viptela) and Cisco Wireless LAN controllers, to quickly provision network devices and laptops or redirect traffic to the Umbrella cloud.

- *Migration to the cloud* – Cisco offers license portability and Cisco Defense Orchestrator, to help existing customers of Cisco Secure Web appliances 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. Cisco's Secure Client (AnyConnect) client, can be used to route DNS traffic and can send all web traffic to the Umbrella secure web gateway and firewall.

- *Management* – the Cisco Umbrella dashboard includes Secure Web Gateway (full proxy), DNS security, cloud-delivered firewall and CASB capabilities and interactive threat intelligence in a single management console.

Cisco offers the following Appliance-based Solutions:

- **Cisco Secure Web** – appliances are available in the S-Series lineup, which comes in various versions: **S695** for large enterprises (> 10,000 users), **S395** (for mid-size companies with < 10,000 users), **S195** (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 ESXi, Microsoft Hyper-V, KVM hypervisors, and Cisco Unified Computing System (Cisco UCS) servers. The image is also offered in AWS, for customers who wish to deploy Secure Web in the public cloud.

**STRENGTHS**

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

- License flexibility between Umbrella and Secure Web Appliances enables customers to easily transition to the cloud. Hybrid scenarios are also supported.

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

- Cisco provides strong support for mobile devices (i.e. iOS/Android) web use, via its Secure Client (formerly AnyConnect) Mobility Client.

- Cisco's Web security solutions offer DLP policies that administrators can enable and customize. Cisco's Secure Web appliances can also integrate with third party 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 can direct traffic to the cloud services.

**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.

- Administration and reporting across Cisco's hybrid deployments of Umbrella and Secure Web could be improved. The vendor has this on its roadmap.

- Cisco is still developing a common identity framework across its Secure Web and Umbrella solutions.

## MCAFEE

6220 America Center Drive
San Jose, CA 95002
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. In late 2020, McAfee filed an initial public offering.

### SOLUTIONS

**McAfee Unified Cloud Edge (UCE)** converges three core technologies, Web, CASB, and DLP into a single solution to provide consistent data and threat protection controls from device to cloud. **McAfee Next-gen Secure Web Gateway** is the web security components of UCE, which includes the following features:

- *Unified management & reporting* – available via MVISION Cloud. McAfee has converged its cloud-based Web Gateway technology with its MVISION Cloud solution, giving customers one location to protect data and defend against threats in the cloud.

- *CASB* – integration with McAfee's MVISION Cloud offers closed-loop remediation, shared risk databases, advanced shadow IT (proxy-based) use cases, and mobile McAfee Client Proxy (MCP). Advanced Shadow IT reporting and risk mitigation can be achieved by moving a part of the control for Internet Access from the web gateway into automated policy decisions based on the automated analysis of Internet traffic in MVISION Cloud. The CASB features on the web gateway include tenant restriction to avoid usage of cloud services other than the corporate account.

 

- *Threat protection* – contains a proactive and unique anti-malware scanning engine that uses emulation and behavioral analysis to filter malicious Web content in real-time without a signature or impacting browsing experience. The emulation engine is complimented 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.

- *URL filtering* – uses category and reputation filtering powered by McAfee's proprietary Global Threat Intelligence network. For uncategorized URLs, McAfee web security 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 26,000 Web applications and application sub-functionalities.

- *DLP* – control comes bundled with the solution to prevent content in the enterprise from leaving via email, 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. McAfee also includes unified DLP across end endpoints, cloud and web as part of the McAfee Unified Cloud Edge offering.

- *Remote Browser Isolation (RBI)* – is based on McAfee's Light Point Security acquisition. It provides user protection against advanced web based threats, such as ransomware and credential phishing. McAfee offers free remote browser isolation in-line with MVISION UCE for risky web sites for all users, which helps support consistent policies, data protection and visibility across isolated and non-isolated traffic. A separate add-on is also available for isolating all traffic.

**STRENGTHS**

- McAfee Unified Cloud Edge converges Web, CASB, DLP, and RBI technologies into a single product with common workflows and reporting.

 

- McAfee Next-gen Secure Web Gateway tightly integrates with MVISION Cloud for unified management, advanced Shadow IT, shared risk database and more, offering organizations a single pane of glass to protect against threats from device to cloud.

- McAfee Unified Cloud Edge 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. It can also integrate with both cloud and on-premises versions of McAfee ePO, which allows for central reporting across hybrid enterprise deployments.

- McAfee Next-gen Secure Web Gateway integrates extensively with the McAfee product portfolio including: MVISION eXtended Detection and Response (XDR); 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's Unified Cloud Edge's CASB offering is FedRAMP High certified.

**WEAKNESSES**

- McAfee Advanced Threat Defense, while highly powerful, does not currently support Apple macOS, or Linux platforms.

- While McAfee is striving for tight integration across a rich portfolio of Web, DLP, CASB and RBI technologies, ease of policy setting and reporting granularity could still be improved.

- McAfee's Next-gen Secure Web Gateway does not currently FedRAMP authorized. The vendor has this on its near term roadmap.

- 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.

- McAfee has announced the sale of its Enterprise business to a consortium led by Symphony Technology Group (STG). At the time of this writing, it is too soon to know what impact this will have on product direction.

 

## TRAIL BLAZERS

### MIMECAST

1 Finsbury Avenue
London
EC2M 2PF
www.mimecast.com

Founded in 2003, Mimecast is a provider of cloud-based business services which comprise email, collaboration and web security, archive and data protection, to awareness training, uptime assurance and more. Mimecast is headquartered in London, UK, with North American headquarters in Lexington, MA and offices globally. Mimecast is a publicly traded company.

#### SOLUTIONS

Mimecast's **Web Security** solution is built on the same multi-tenant cloud platform as its Email Security service. The two solutions are tightly integrated providing a single solution and console to protect the two leading attack vectors.

Mimecast Web Security offers the following functionality:

*Web Threat Protection* – blocks websites that deliver malware or are part of phishing attacks. Inspects content and file downloads from suspicious sites using a dynamic proxy that applies anti-virus, SSL inspection, URL categorization and static file analysis. Detects and prevents data exfiltration. It leverages the latest threat intelligence from multiple sources, and offers extended proxy for inspecting riskier sites like webmail, social media and file sharing. It also offers Browser isolation for safe web use within an isolated container.

*Web Filtering/Acceptable Web Use Enforcement* – applies granular web category selections to ensure policies meet specific requirements. Provides the ability to selectively apply policies to all users, entire networks, groups, or only to specific users.

*Remote User Protection* – delivers consistent security and controls to all employees and devices both on and off the network. Targets policies to specific users regardless of their location or device. It currently supports Windows, Mac, iOS platforms.

 

*Shadow IT Discovery and Management* – identifies which cloud apps are being used, by whom and how often. It applies policies to block specific apps, and monitors apps before taking action. Provides consistent controls and protection regardless of how apps are accessed, including through mobile devices. Selectively manages app usage with options for everyone, groups and individuals.

*Integration with User Awareness Training* – block pages can be customized to deliver just in time coaching in context when a user hits a blocked category or scenario.

*Visibility and Reporting* – Dashboard projects key metrics including top accessed and blocked domains, site categories, and requests leading to malicious sites. Generates detailed user-level activity and security reports, as well as scheduled reports. It also supports selective log data retention (e.g. no data, or no personally identifiable information, PII).

Mimecast also offers **Mimecast Web Security for Guest Wi-Fi** which protects guest Wi-Fi users and helps meet organizational security and governance needs by applying consistent web security and usage controls to guest Wi-Fi networks. It stops guest network users from accessing malicious sites, controls what site categories can be accessed to prevent inappropriate web use, and manages what cloud apps can be accessed.

**STRENGTHS**

- Mimecast offers tight integration of Web and Email security on the same cloud-native platform, which delivers key benefits to both organizations and end-users, including: a consistent set of policy and application controls, shared intelligence, a consistent user experience, reduced cost and complexity, and simplified setup and management.

- Mimecast web security delivers robust user-level reporting, including data on DNS record types, policy applied, identity (user, device ID, IP, location), and authentication methods used for each web request.

- Mimecast makes use of proprietary static file analysis technology to rapidly and accurately analyze file downloads without impacting user experience or productivity.

- Mimecast offers a lightweight agent for Windows, Mac and iOS with transparent user identification to make rollout simple for administrators and end-users.

 

- Mimecast offers an extended proxy feature that allows customers to selectively apply proxy inspection to additional threat vectors like Social Media Messaging, Personal Web Mail and Cloud File Sharing applications.

**WEAKNESSES**

- Mimecast currently offers a set of Application Visibility and Control capabilities but does not offer full CASB functionality. This is on the vendor's roadmap.

- The Mimecast web service does not currently offer DLP functionality. This is on the vendor's roadmap.

- Mimecast currently offers its Mimecast Security Agent (MSA) for iOS, Mac and Windows devices to ensure protection for roaming devices. Agents for Android and Chromebook are on the roadmap.

- While Mimecast offers browser isolation functionality, this is a separate add-on.

## SPECIALISTS

### ZSCALER

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

Zscaler, founded in 2007, offers a Security-as-a-Service platform distributed over a global network of data centers that deliver Internet security, advanced persistent threat (APT) protection, data loss prevention, SSL decryption, traffic shaping, policy management and threat intelligence. Zscaler is publicly traded.

 

**SOLUTIONS**

**Zscaler Web Security**, part of the Zscaler Cloud Security Platform, is 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 Control* – is Zscaler's CASB functionality which serves to monitor, protect and control cloud application usage across the organization. It also offers closed loop integration with Microsoft's Cloud Application Security (CASB) functionality. 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.

- *Remote Browser Isolation* – Zscaler supports fully integrated web browser isolation based on its Appsulate acquisition.

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

**STRENGTHS**

- Zscaler's SaaS is a good fit for organizations fully vested in the deployment of a fully cloud based IT infrastructure and cloud applications.

- 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 model delivers effective protection across all traffic, users, and devices, including cloud applications, remote locations, and mobile employees.

- Zscaler's global footprint makes it a good choice for customers with distributed worldwide operations.

 

### WEAKNESSES

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

- Zscaler does not offer 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.

## 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' cloud-based management platform, and backed by SophosLabs, its global network of threat intelligence centers. The company is headquartered in Oxford, U.K. In 2020, the company was acquired by private equity firm Thoma Bravo, and is now a private company.

 

**SOLUTIONS**

Sophos currently offers web security through several products including the next-gen **XG Firewall** and the legacy **Sophos SG UTM** product line. All are built around the same core security capabilities and offer similar ranges of other web filtering functions appropriate to the product and deployment method. Sophos Endpoint and Sophos Mobile also provide web filtering and reporting capabilities managed by Sophos Central.

- **Sophos XG Firewall** – is Sophos's flagship next-generation firewall which provides comprehensive Web Gateway functionality. The version 18 (v18) release introduces a new high-performance SSL/TLS decryption engine and inline web filter that inspects encrypted and non-encrypted web traffic on any port. It integrates with Sophos's cloud-based Intelix platform to protect against emerging threats with sandboxing and deep learning analysis. It also offers cloud app visibility and shadow IT detection, leveraging a heartbeat connection between gateway and endpoint to identify unrecognized application traffic.

- **Sophos SG UTM –** provides comprehensive Web Gateway functionality as part of a unified threat management (UTM) solution.

- **Sophos endpoint protection –** Intercept X, Sophos's flagship Endpoint Protection products, provide in-depth web protection for devices wherever they are deployed. With built-in scanning of web traffic in transit as well as inspection of network traffic for signs of malicious behaviour.

During 2020, Sophos announced a planned end-of-life for its **Sophos Web Appliance** product in mid-2023. The company is recommending that customers replace the old Web Appliance infrastructure with XG Firewall.

All Sophos Web Gateway solutions include:

- *Threat protection* – provided by Sophos's own proprietary technology that originates from SophosLabs. The proprietary threat technology uses machine learning, reputation, anti-virus signatures, behavioral analysis, and more to identify malicious downloads and web content. Products also integrate with Sophos's Intelix platform for cloud-based analysis with deep learning AI models and sandboxing to unmask a wider range of potential threats.

 

- *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* – Sophos Central provides a cloud-based solution for management and reporting with XG Firewall. With its EDR and upcoming XDR solution, built on a highly-scalable cloud-based data lake, Central combines visibility into endpoint and network devices to suspicious incidents and provides greater insight into real and suspected threat activity within an organization.

**STRENGTHS**

- Sophos offers flexible deployment options 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.

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

 

including in-browser crypto-mining code.

- Sophos' web gateway products integrate with Intelix, an advanced persistent threat (APT) and zero-day malware analysis and defense, which detects, blocks, and responds to evasive threats through cloud-based, next-generation sandbox technology and deep learning.

- 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' 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.

- Sophos does not currently offer browser isolation technology, which is becoming prevalent with many competing solutions.

- Currently, Endpoint and Network solutions have separate management interfaces when deployed together as a hybrid solution. However, integrated cloud-based management of hybrid deployments is on the vendor's roadmap.

## 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 is owned by private equity firm Thoma Bravo.

 

**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 relies on partnerships with multiple vendors for sandbox functionality, and Avira for Static Analysis, heuristic and behavioral analysis of endpoint data.

Barracuda Networks offers the following web security solutions:

- **Barracuda Web Security Gateway (WSG)** – is sold as a set of on-premises and virtual appliances of different throughput and user capacity, that monitor real-time inbound and outbound traffic. These appliances 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 identified, 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.

- *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. 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.

- *Management* – is provided through a single management interface, **Barracuda Cloud Control (BCC)**, that can manage users and consolidate report data across different geographies as well as aggregate data from multiple appliances.

- **Barracuda Content Shield (BCS)** – is Barracuda's SaaS Cloud web security solution, which delivers content filtering, file-based protection, policy enforcement and reporting, centralized management and real-time threat intelligence. It is a proxy-free architecture that provides both DNS and advanced URL filtering, using agent installed on the device to protect users on and off the network. It is available in two flavors: *content shield*, and *content shield plus*. The plus version adds endpoint malware protection, SSL inspection, heuristic file analysis, powerful domain or category or URL filtering policy based on Per-User or Group,

 

and reporting based on individual Users or Groups, remote user support, LDAP, Google Directory Services/Azure AD integration. BCS supports Chromebook devices using the *Barracuda Chromebook Security for BCS* extension available via the Chrome Web Store.

**STRENGTHS**

- Barracuda Networks Web security solutions are among the more competitively priced solutions on the market today.

- Barracuda Networks supports a broad range of form factors that fulfill the needs of customers of all sizes, and different deployment requirements (e.g. on-premises, virtual appliance, cloud-based).

- 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, 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.

- The Cloud Web Filtering Solution is integrated with the Web Security Gateway Appliance or virtual instance to present single interface for the customers to create and apply policies uniformly across all devices, users and groups.

**WEAKNESSES**

- Barracuda Network's web security solutions are a good fit for customers looking for solid web protection at competitive pricing. Customers with fine-grained, complex protection requirements needs may find the solutions somewhat basic.

- DLP features are minimal in the solutions offered by Barracuda Networks. However, ICAP integration is supported, to allow integration with third party DLP solutions.

- Mobile device protection requires backhauling traffic back through the Web Security Gateway for content control and malware protection. However, customers can link the Web

 

Security Gateway appliance with the Barracuda Content Shied cloud service so Web Security policies are applied locally on the remote devices without overhauling traffic to Web Security Gateway appliances.

- 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 currently provide a CASB solution or integrate with 3rd party solutions. The vendor has this on its roadmap.

## FORCEPOINT

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

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. Forcepoint, a Raytheon Company and Vista Equity Partners joint venture, was acquired by Francisco Partners in early 2021.

### 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 as an appliance, as a cloud service, or as a hybrid deployment. Forcepoint Web Security includes native CASB functionality, with cloud application discovery and risk reporting of shadow IT with access to a large cloud application

 

catalog. It can be enhanced through several advanced protection modules which include:

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

- *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.

- *Web DLP* – 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 pre-defined policies and templates in a single console.

- *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 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 basic CASB functionality, through a 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 offers a broad and highly granular set of Web application controls.

**WEAKNESSES**

- Forcepoint solutions tend to be more expensive than competing solutions, and are a best fit for mid-size and large enterprises with advanced needs.

- Forcepoint does not offer its own sandboxing technology, but delivers sandboxing through a partnership with Lastline, a best-of-breed sandboxing vendor.

- Forcepoint does not offer its own remote browser isolation technology, but OEMs its solution from Ericom Software, a best-of-breed zero trust browser isolation and secure access vendor.

- Forcepoint has lost market visibility, and is primarily focused on the North American government market.

## 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 data from internal and external threats. In 2019, Clearswift was acquired by HelpSystems, a provider of IT management software and services.

 

**SOLUTIONS**

Clearswift offers threat protection through its DLP 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 checked 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. It also supports the redaction of text in images, which can be applied to inbound or outbound traffic.

- *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 forward proxy mode to provide security for users, or in reverse proxy mode to secure website access. ICAP

 

integration also allows tight integration with the HelpSystems' GoAnywhere MFT product line.

- *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's SWG is part of a comprehensive DLP security platform which includes internal and external email protection, and an endpoint solution, which shares much of the same threat technology. 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.
- Clearswift does not provide its own CASB functionality, but offers this in partnership with third party vendors.
- Clearswift's reporting features are adequate but could be enhanced. The company 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 continue to invest to help raise its market visibility, particularly in North America.

## 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 based on a distributed containerized architecture which scales easily and offers a highly secure 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 offers 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 also 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.

iboss partners with FireEye to offer iboss + FireEye Cloud Network Security, which provides advanced threat protection and data breach prevention through the cloud regardless of the end user's location, or form factor (e.g. desktop, laptop, tablet, server, IoT, and other mobile devices).

**STRENGTHS**

- iboss offers a flexible 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.

- iboss's partnership with FireEye offers customers a robust, combined web gateway and advanced threat detection capability.

**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 cloud CASB functionality is still fairly basic compared to other vendors in this space.

- iboss does not offer DLP functionality.

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

- While iboss has regional offices in APAC and EMEA, the vendor can further improve its market presence in these regions.

## 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 security solutions for organizations, service providers, and consumers. Its solutions are powered by the cloud-based Trend Micro Smart Protection Network, which brings together threat reporting and analysis based on a worldwide threat assessment infrastructure. Trend Micro is publicly traded.

### SOLUTIONS

Trend Micro **Smart Protection Suites** offers an integrated defense solution for desktops, laptops, servers and virtualized deployments, with a central management interface. The vendor's XGen Endpoint Security functionality, combines machine learning and other techniques, in order to protect against ransomware and advanced attacks.

**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 is available in two flavors, standard and advanced, and includes:

 

- **InterScan Web Security Virtual Appliance** – is 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** – is 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** – is 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* – 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 and Categorization* – 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.

- *Cloud DLP* – offers over 200 out-of-the-box DLP templates to satisfy major compliance requirements and protect sensitive data. It is included in the advanced version of Trend Micro Secure Web Gateway.

- *Cloud App access* – is Trend Micro's CASB functionality which provides cloud app control and visibility, allowing administrators to identify unsanctioned apps and control user access to sanctioned apps. It is included in the advanced version of Trend Micro Secure Web Gateway.

 

**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 supports VMware and Microsoft Hyper-V as virtual platforms for its appliance based solutions.

- Trend Micro Secure Web Gateway Advanced 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.

- Trend Micro offers a cloud-based management console which supports single pane of glass management of both cloud and on-premises deployments.

### WEAKNESSES

- Trend Micro offers only basic DLP and CASB functionality, both of which are available only in the higher priced Secure Web Gateway Advanced version.

- 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.

 

## 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, 2021-2025 | Feb. 2021 | $3,000.00 |
| Instant Messaging Statistics Report, 2021-2025 | Feb. 2021 | $3,000.00 |
| Social Networking Statistics Report, 2021-2025 | Jan. 2021 | $3,000.00 |
| Mobile Statistics Report, 2021-2025 | Jan. 2021 | $3,000.00 |
| Endpoint Security Market, 2020-2024 | Nov. 2020 | $3,000.00 |
| Secure Email Gateway Market, 2020-2024 | Nov. 2020 | $3,000.00 |
| Microsoft SharePoint Market Analysis, 2020-2024 | May 2020 | $3,000.00 |
| Email Market, 2020-2024 | Apr. 2020 | $3,000.00 |
| Office 365, Exchange Server and Outlook Market Analysis, 2019-2023 | Apr. 2020 | $3,000.00 |
| Cloud Business Email Market, 2020-2024 | Apr. 2020 | $3,000.00 |
| Corporate Web Security Market, 2020-2024 | Apr. 2020 | $3,000.00 |
| Unified Endpoint Management Market, 2020-2024 | Apr. 2020 | $3,000.00 |
| Advanced Threat Protection Market, 2020-2024 | Apr. 2020 | $3,000.00 |

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

### Upcoming Publications:

| Title | To Be Released | Price* |
|---|---|---|
| Information Archiving Market, 2021-2025 | Apr. 2021 | $3,000.00 |
| Advanced Threat Protection Market, 2021-2025 | Apr. 2021 | $3,000.00 |
| Corporate Web Security Market, 2021-2025 | Apr. 2021 | $3,000.00 |

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

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

 