IDC MarketScape

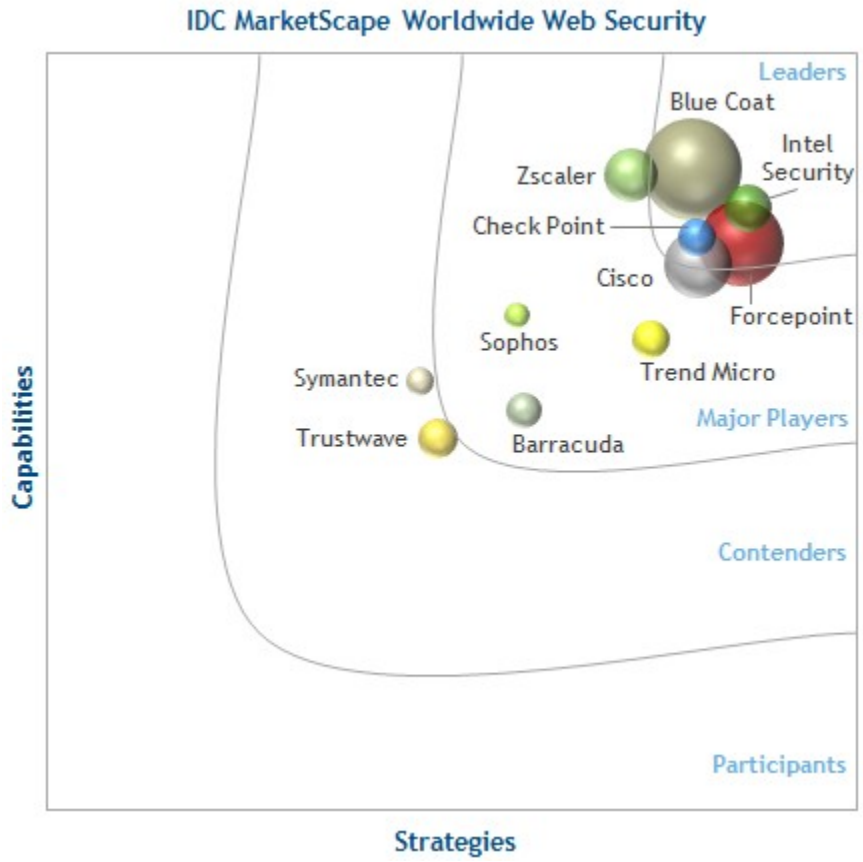
IDC MarketScape: Worldwide Web Security 2016 Vendor Assessment

Robert Westervelt Elizabeth Corr

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Web Security Vendor Assessment



Source: IDC, 2016

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

March 2016, IDC #US41000015

IDC OPINION

The Web security market is in a state of transition as organizations race to identify and extend control and visibility to a significantly growing mobile workforce. Web security vendors are also adapting to extend visibility and control over software-as-a-service (SaaS)-based services, which can be easily adopted by employees through their mobile devices to support file sharing and collaboration. The rapidly evolving threat landscape is also forcing Web security gateway makers to catch up with more powerful offerings. Criminal attack campaigns target users through Web site drive-by attacks, often from legitimate Web sites, where malicious code scans Web browsers and browser components to exploit Flash and Java vulnerabilities. These risks have led to highly visible threats, including a continued barrage of banking malware. Attacks are increasingly being delivered via hijacked advertising networks, weaponizing legitimate sites where the ads are hosted. Ransomware is also being detected in greater amounts and can spread through a drive-by attack, links shared on social media sites, or through malicious files hosted on popular SaaS services. Organizations are seeking more robust Web security capabilities. Web security deployment models are rapidly changing as organizations address how to enforce security policies on remote workers, branch offices, and mobile devices. The standard on-premises approach is one of three main deployment options available to customers, but SaaS and hybrid deployment models are increasingly being adopted. The standard on-premises approach is one of three main deployment options available to customers, but SaaS and hybrid deployment models are increasingly being adopted. In detail:

- **Web security gateway:** This on-premises offering is offered as a software or hardware appliance and has been the traditional way organizations address Web security threats and exert control and visibility over worker Internet activity. Features include URL filtering and categorization, inbound/outbound threat detection (malware, botnet traffic, data loss prevention [DLP]), and controls for social media and Web applications. The protection is designed to address a variety of threats, including drive-by attacks, phishing attempts, and malicious file downloads. Security vendors are increasingly adding integration with advanced threat detection products, such as SaaS-based and on-premises sandboxes for suspicious file analysis, network traffic inspection, and security analytics platforms that support incident response.
- **SaaS Web security:** Adoption of SaaS Web security services includes midmarket and larger enterprises extending on-premises Web security gateways to address branch offices, remote workers, and mobile threats. SaaS Web security solutions are typically proxy based and generally not configured in line for blocking. Main features include URL and content filtering, including detection of malicious code in Web sites or attempts to redirect users to an attack Web site. Customers also gain control and visibility of social media and popular SaaS services. Management capabilities have improved and in some cases are synonymous with on-premises capabilities. Subscribers of these services enjoy little to no maintenance requirements and can add or remove licenses for additional security capabilities as they become available.
- **Hybrid Web security architectures:** IDC is seeing a significant interest in customers seeking to bolster the effectiveness of traditional on-premises gateways with SaaS components in a hybrid deployment to protect users in remote branch offices where an on-premises device, or backhauling traffic via the WAN for filtering by a home office Web appliance, is impractical or expensive. The hybrid approach is typically proxy based to extend visibility and control over remote worker laptops and their mobile devices, regardless of their location and connectivity.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

This IDC MarketScape includes vendors offering Web security technologies under the traditional secure Web gateway product category, which includes features such as URL filtering and categorization, inbound/outbound threat detection (malware, botnet traffic, DLP), and controls for social media and Web applications. Vendors were also evaluated across three delivery platforms for Web security: on-premises hardware appliances, virtual appliances (software), and software as a service. Other inclusion criteria were: vendors with offerings sold on a worldwide scale (i.e., not primarily focused on certain countries or geographies) and vendors listed with at least $10 million in worldwide product revenue. Further:

- **Full secure Web gateway capabilities.** Each Web security gateway vendor is required to possess full Web security capabilities and support either full SaaS, hybrid, or on-premises deployment models.
- **Revenue.** Each Web security gateway vendor is required to have total global Web security revenue in excess of $10 million that was attained in 2014.
- **SSL decryption.** All vendors in this IDC MarketScape meet the requirement of supporting full SSL decryption with management capabilities.
- **Geographic presence.** Each SWG vendor is required to have a global presence.

Vendors included in this IDC MarketScape are Barracuda, Blue Coat Systems, Cisco Systems, Check Point Software Technologies, Forcepoint Security (previously known as Websense), Intel Security, Sophos, Symantec, Trend Micro, Trustwave, and Zscaler.

ESSENTIAL BUYER GUIDANCE

Web security vendors continue to adapt their mature offerings to the rapid changes experienced at the corporate network as a result of mobile, social, SaaS adoption, and other external influences that make up the 3rd Platform innovation. The heterogeneity of corporate IT infrastructure, the significant rise in the use of SaaS applications, and the rapidly distributed nature of corporate assets have made it difficult for system administrators to maintain visibility and control. Compounding the challenge is customer demand for a robust SaaS Web security offering that ties to an on-premises gateway. All security vendors have rolled out SaaS Web security services to various degrees, but more work needs to be done to reduce deployment pains and provide unified reporting and other centralized management capabilities.

This IDC MarketScape assesses the current Leaders, Major Players, Participants, and Contenders in the worldwide Web security market and rates these vendors based on the criteria most important to enterprise customers. Key factors enterprises must consider when selecting a Web security vendor include:

- **Breadth of capabilities.** As defined by end users IDC spoke with, these include antimalware, URL/content filtering, DLP, outbound threat detection, social media controls, user/authentication-based policy enforcement, and SSL inspection.
- **Range of form factors and delivery models.** The ability to offer on-premises software or hardware appliances, cloud-based software as a service, and hybrid offerings blends these delivery models in a complementary way.

- **Adjacencies to other security technologies including integration with specialized threat analysis and protection products.** Technologies that complement Web security include DLP, email security, endpoint/gateway antimalware, network security, and encryption.
- **Scalability and availability.** Delivering key Web security capabilities to a diverse set of end users and devices, and at very large scale in terms of connections and global availability, is a key capability.

VENDOR SUMMARY PROFILES

Barracuda

Barracuda is positioned as a Major Player in this IDC MarketScape due partly to its strong brand recognition, its customer support, and lucrative channel program. The Barracuda Web Filter is available as a hardware or virtual appliance or SaaS Web security offering and offers malware and virus protection, URL and application filtering, and social media controls and can be configured to extend protection to remote PCs and mobile devices. The company's SaaS Web security service uses software agents and a Safe Browser application for iPhones and iPads that redirects Web traffic to its cloud proxy. It also supports a hybrid deployment that includes an on-premises appliance in conjunction with its SaaS Web security service. Barracuda supports SSL traffic inspection and provides visibility and control over Google Apps, Facebook, and other social media and SaaS services. The company provides cloud-based sandboxing technology to identify and analyze advanced threats through a partnership with Lastline. The company's product portfolio appeals to small and midsize businesses. The company's target customer base is up to 5,000 employees and the bulk of its current customers have 100–2,000 employees. Barracuda pulls its product portfolio together through Barracuda Central, a centralized management console. Barracuda offers Web and email security products in its content security portfolio. In addition to Web and email security gateways, Barracuda has an extensive portfolio of network and application security and storage and a growing base of cloud-based productivity solutions.

Strengths

- Nearly 100% of Barracuda's sales are driven through the company's 5,000 channel reseller partners, and the company maintains a lean manufacturing operation, building appliances for customers as they are ordered. If a unit malfunctions, the company pledges to provide a new appliance replacement within 24 hours via its Instant Replacement Program and also includes a free replacement model every four years.
- Customers have repeatedly praised Barracuda's intuitive management console, which consists of a Web-based user interface that is consistent across all Barracuda products. The company also maintains a 24 x 7 customer support hotline and a malware removal tool to remove spyware infections from client machines.
- Barracuda offers a flexible deployment model, enabling customers to choose from on-premises hardware appliances, subscribe to its SaaS Web security service, or adopt a hybrid approach for additional application controls and granular identity management capabilities.

Challenges

- Barracuda offers a broad line of network security products, but the company lacks more extensive capabilities for the detection of zero-day malware and sophisticated threats used in targeted attacks. Customers typically buy the Barracuda NG Firewall in combination with the Web Filter for more robust threat detection capabilities. Executives tell IDC the company is

developing an advanced threat detection package and has plans for more robust application control.

- Barracuda has built-in SSL decryption capabilities, but users have commented on the negative performance impact prompted by SSL inspection for certain appliance models. The company plans to provide SSL acceleration in its high-end hardware to improve performance.
- Barracuda does not use APIs to integrate natively into cloud application services for increased visibility and control, and instead provides some limited controls through traffic streams. Executives say customers are not yet asking for the capability.

Blue Coat

Blue Coat Systems is positioned as a Leader in this IDC MarketScape, driven in part by its strong leadership team, its growing install base, and ability to add components that address emerging trends and changes in end-user behavior. Blue Coat has been building out its product portfolio via acquisitions while steadily adding Web security capabilities to its line of ProxySG appliances. The company offers three ProxySG models that provide up to 1Gbps throughput and connect to Blue Coat's Global Intelligence Network for additional protection.

Blue Coat was an early entrant with SaaS and hybrid Web security offerings. Customers interviewed by IDC have praised the SaaS and hybrid models, indicating better-than-expected performance and unified reporting, giving administrators the ability to view a single, contextual view of users, regardless of whether they are mobile, in a remote office, or on the corporate network. Blue Coat offers the same feature and management capabilities in its SaaS and hybrid deployment models as its traditional on-premises ProxySG appliances. Blue Coat charges a base price for on-premises hardware and then charges a per-user subscription pricing.

In addition to strong antimalware capabilities and protection from malicious URLs and other Web-based threats, the company provides support for visibility into popular SaaS services such as salesforce.com and Box. The 2015 acquisition of Perspecsys should be a welcome addition for ProxySG customers interested in applying advanced controls into sanctioned SaaS services and eliminating employees attempting to get around restrictions by using unauthorized SaaS services, known as shadow IT.

Blue Coat's customer base begins with deployments in large Fortune 100–sized enterprises, where scalability is a major requirement. The addition of SaaS Web security capabilities is also drawing upper midmarket enterprises. Early interest is in hybrid deployments, according to Blue Coat.

The company is also gaining attention for its growing security portfolio, which includes products complementary to ProxySG, including a separate content inspection appliance for malware scanning and whitelisting and a standalone SSL decryption appliance. The company also has an integrated security analytics and malware analysis sandbox solution as part of its specialized threat analysis and protection offering for detecting targeted attacks and other advanced threats.

Customers are also adding on the Blue Coat Content Analysis System, which bridges the ProxySG with Blue Coat's advanced threat protection products. To capture the rising interest, Blue Coat launched an Advanced Secure Gateway model, which combines the ProxySG and Content Analysis System in a single appliance. Blue Coat associates some of the increased interest in its Content Analysis System with rapid demands in increased capacity associated with Office 365 and Google Docs deployments, which significantly increases traffic flow through Ports 80 and 443.

Bain Capital acquired Blue Coat from private equity firm Thoma Bravo in a $2.4 billion deal in which Bain would prepare Blue Coat for an initial public offering.

Strengths

- Blue Coat claims to provide the fastest response and points to its ability to analyze new URLs in real time and provide responses in about 800ms. The analysis engine can detect 55 languages and conducts full inspection of the Web page, including PDFs, executables, and other embedded files. Blue Coat assigns a risk level to all URLs it inspects.
- Blue Coat's portfolio is one of the most exhaustive for providing protection from known and new threats, with traditional Web security components, integrated with the vendor's advanced threat protection portfolio.
- Blue Coat's flexible deployment model includes unified reporting for organizations managing a hybrid approach of on-premises hardware appliances, a virtual deployment, or the SaaS Web security service.

Challenges

- Customers tell IDC that Blue Coat often comes out as the expensive option when evaluated against competitors. Additional licensing options and integration with Blue Coat's advanced threat protection offerings will add to the premium price tag.
- Blue Coat's potential public offering will likely place more scrutiny on how senior executives spend on research and development (R&D), support, and operations, and could delay the launch of innovative features and capabilities.
- Customers requiring an integrated DLP solution should note that Blue Coat partners with Code Green Networks for the functionality in its appliance. Code Green integrates with ProxySG but lacks the robustness of some competitor solutions.

Check Point

Check Point Software Technologies is positioned as a Leader in this IDC MarketScape for its strong SaaS offering and growing portfolio of products designed to detect advanced threats. Check Point's Web security software blades provide enterprise-grade Web security features and is available as a SaaS service, a software blade, and a virtual gateway and is capable of supporting a cloud-based or hybrid deployment. The Check Point Secure Web Gateway can inspect SSL-protected content and contains granular controls to manage privacy and compliance-related traffic that should not be inspected. The offering also comes with ThreatCloud integration for access to protection and analysis of threats from the vendor's research team.

Check Point's Secure Web Gateway as a Service provides full secure Web gateway functionality found in the company's on-premises SWG software blade. Executives tell IDC that hybrid deployments are trending with Check Point's customer base. Customers are adding the service to apply policies to roaming devices.

Check Point's Web security offering provides three layers of capabilities: URL filtering, dynamic URL coverage for live inspection of a visited site for malicious activity, and application control, which enables administrators to create policies against one of 64 categories and provides a risk score to each application. The solution also gives an administrator the ability to create logic sections for applying policy against specific traffic. The administrator can create sections to cover all the Port 80 right down into the Internet access.

To address targeted attacks and custom malware, Check Point has also provided connectors for its optional CPU-level threat prevention technology and a Threat Emulation Blade and cloud-based emulation sandbox service to detonate and analyze suspicious files. Check Point also rolled out Threat Extraction, which can identify and reconstruct Microsoft Office files and Adobe PDFs to eliminate any signs of embedded malicious components.

Strengths

- Check Point customers that have invested in the company's software blade approach can easily add the Web Gateway capabilities and integrate it with Check Point's advanced threat defense products as part of a unified defense posture.
- Check Point provides granularity to enable administrators to create controls over Web traffic in any direction. Extensive toolsets are available for increased visibility over events and enforcement of controls, and reporting capabilities provide usage and activity statistics.
- Check Point is ahead of other Secure Web Gateway competitors with its SaaS-based offering, which has the same capabilities and management features as its on-premises models. The service enables organizations to address remote offices and roaming devices, regardless of the networking infrastructure in place.

Challenges

- Organizations considering Check Point for remote workers should take note that its SaaS Secure Web Gateway service and its Capsule Cloud offering are supported by 30 datacenters globally. The security vendor said it is expanding its datacenter footprint to more than 70 different datacenters.
- Customers considering Check Point for SaaS security integration should consider the maturity of Check Point's Web security offering. Check Point introduced Application Control in 2011 and is continuing to add visibility and control functionality at the application level. The latest version added SAML integration and comes with prebuilt plugins to salesforce.com, Office 365, Google Apps, Dropbox, and others.
- At the time of writing this study, Check Point's SaaS Web security offering did not provide full policy control for IPS capabilities. The company is also planning to add support for Data Loss Prevention in the cloud.

Cisco

Cisco Systems is positioned as a Leader in this IDC MarketScape after reestablishing its presence in the security market via acquisitions and plans to build out a strong SaaS portfolio. Cisco's offerings include Web security gateway appliances and its SaaS offering, Cisco Cloud Web Security. An on-premises/cloud configuration is also available for Cisco Web Security Appliance/service deployments via a hybrid licensing offering.

Cisco added the Advanced Malware Protection (AMP) capabilities via its 2013 acquisition of Sourcefire to its Web Security, Cloud Web Security, and Email Security gateways. The integration adds file reputation functionality, file analysis sandboxing via Cisco's ThreatGRID acquisition, and a feature called "file retrospection" to identify malicious files designed to appear benign to antimalware inspection engines and are programmed to become malicious at a later time. The features require an additional license.

Cisco also recently added support for its Identity Services Engine (ISE), a network admission control technology that extends policies and controls to third-party partner solutions and other Cisco products

that make up the Cisco security architecture. The integration enables customers to use ISE identity information when setting Web security policy.

Cisco's Web Security Appliance offers threat protection capabilities via several licensing options. An essentials bundle limits functionality to Web reputation and Web usage control, an antimalware bundle provides malware detection, and a premium bundle provides Web and antimalware features. The company maintains a separate licensing structure for its cloud offering.

Cisco was one of the earliest vendors with a SaaS-based Web security offering via its acquisition of ScanSafe in 2009 and currently has more than 10,000 users of the service. It also sells a Web Security Appliance (WSA).

Cisco engineers are still working on bringing the specific product features to parity with its on-premises Web security gateway appliances. The SaaS offering currently offers unified policy setting for the appliance and cloud solution from the cloud interface. Cisco integrated Cognitive Threat Analytics to identify threats more quickly in both of its Web Security offerings. Unified reporting is currently available for the SaaS and on-premises versions from the Web Security Reporting Application.

Cisco has an open, partner ecosystem approach to providing cloud access security broker functionalities. Cisco currently offers the Cloud Access Consumption Service from its Advanced Services group, providing customers visibility into Shadow IT.

Strengths

- The Cisco Web security offerings integrate with its advanced threat protection portfolio, giving customers access to the Advanced Malware Protection offering and file analysis sandboxing capabilities for detection of targeted attacks and custom malware.
- Cisco Web Security is fed by information from Talos, the largest global threat telemetry network of any company that updates file reputation and Web reputation scores.
- Cisco's Cognitive Threat Analytics offering is a unique differentiator against competitor Web security solutions. Available as an add-on, the cloud-based solution attempts to identify threats by monitoring for subtle changes in network behavior.

Challenges

- Cisco offers appliance or virtual deployment options for Web security. Its licensing model may be a challenge for some organizations with various bundles for Web reputation capabilities, standard antimalware protection, and a separate advanced malware protection license. Adding to the challenge are different bundles available for cloud Web security or on-premises Web security appliances. Cisco is also still working on unified reporting capabilities for organizations that are adopting a hybrid strategy.
- IDC views Cisco's acquisition of OpenDNS as a positive one, but customers should heed caution while Cisco integrates the offering with Web Security components. OpenDNS could be used as the backbone for future SaaS-based security offerings, including Web Security.
- Hybrid deployments require two separate consoles for reporting and policy, but engineers are working on providing a consolidated reporting offering that doesn't include third-party products.

Forcepoint

Forcepoint Security is positioned as a Leader in this IDC MarketScape due partly because of its global install base and success in positioning the former Websense brand as a leader in threat intelligence

and attack prevention. In May 2015, Raytheon completed its $1.9 billion deal with Vista Equity Partners to acquire an 80.3% controlling stake in Websense. The move creates a new company that combines Websense with the Raytheon Cyber Products commercial cybersecurity business unit. The name of the new company was announced in 2016.

In addition to the Websense portfolio, Raytheon's Cyber Products business consists of its SureView analytics platform for incident response. Forcepoint executives stress the commercial portfolio is being run independently of the Raytheon defense arm.

Forecepoint offers software, hardware, and cloud-based security products and services. It is also a front-runner in the data loss prevention market and has unified its offerings into the TRITON-branded content security platform, giving Web security customers access to integrated data protection and specialized threat analysis and protection capabilities.

Forcepoint has been working on getting customers off its legacy offerings to move to TRITON or adopt its SaaS cloud components. Many legacy Web security customers came from SurfControl and used it mainly for URL filtering and content inspection. They have generally sought lower-cost options for the functionality. The entrance of competitive SaaS-based Web security cloud services also attracted Websense customers attempting to reduce complexity and deployment pains.

To make matters worse, deployment problems stemming from poorly configured appliances also fueled customer churn and prompted Websense executives to establish an internal team to handle technical support for disgruntled customers. Senior executives say the issues have been addressed. The company increased its global frontline support team by 30% and opened a support center in Texas in July 2014. The company reports that its customer satisfaction rating has increased by 45% since the move and is now at historical highs for the company as well as industry standards.

Websense also launched new deployment services to assist customers with the proper rollout of its product components. In addition to more direct access to customers, the company has been building relationships with larger systems integrators. Under Raytheon, the company will likely gain resources to bolster technical support, enhanced access to public sector markets, and a broader security portfolio, which could stimulate sales activity.

At the core of the company's product portfolio is its Advanced Classification Engine, which provides the risk scoring and analytics used to inspect inbound and outbound Web traffic. The Websense TRITON APX Enterprise suite contains the Web security component and additional malware detection, data loss prevention, endpoint protection, and mobile security modules, as well as a centralized management console for managing policies and generating reports. Customers can also adopt a cloud or hybrid deployment to protect remote employees, roaming users, and branch offices via a cloud proxy server.

Forcepoint maintains 20 datacenters globally and two service operation centers.

TRITON AP-WEB is available as software or as a hardware appliance. The gateway supports an optional Web sandboxing module for suspicious file analysis. The gateway can conduct SSL inspection and social media and application controls as well as full port monitoring via a network agent. Users of the TRITON AP-WEB gateway can expand the solution to gain Web channel data loss prevention controls and protection for remote users. The company's TRITON AP-EMAIL solution can be added and integrated into a single administrative interface.

TRITON AP-WEB can be deployed as a pure SaaS solution via the Web Cloud Module. Its features include the ability to scan and analyze social media sites. It uses the ACE engine for analysis and provides URL filtering and access to granular social Web controls. Users can set policies and generate reports using a Web-based console.

Strengths

- Forcepoint's SaaS platform has reached parity with the company's other delivery options, putting it ahead of competitors with SaaS offerings that are not complete. Customers can leverage an optional sandbox module to detect custom malware and a strong threat intelligence team bolsters protection against targeted attacks.
- TRITON users can gain granular SSL inspection capabilities associated with the Web security module to monitor encrypted traffic and set restrictions over visibility of sensitive data to maintain privacy and regulatory compliance. Websense also has tight integration with Web, DLP, email, and endpoint products, which benefits users.
- Now under the Raytheon umbrella, existing customers should benefit from the stability and access to a broader portfolio of security products. Raytheon is retaining Websense CEO John McCormack and the two companies have hinted at working on tighter integration with Raytheon's SureView analytics platform and adding additional capabilities to bolster threat assessments and incident response.

Challenges

- Raytheon gains access to Websense sales channel partners but integration of Websense technology into the Raytheon Cyber Products business is still ongoing. The company has demonstrated progress with a federal offering but is still developing a fully integrated platform.
- Forcepoint maintains a SaaS offering, but its core focus is on enterprise-grade threat defense, coupled with specialized threat analysis and protection capabilities. Market share estimates suggest the platform's premium price prompted customers with limited IT resources to move to low-cost alternatives.
- Forcepoint is retooling the back-end infrastructure supporting its SaaS platform in 2016 to increase scalability and support of additional capabilities. This overhaul must be done systematically to avoid disruption to existing users.

Intel Security

Intel Security is positioned as a Leader in this IDC MarketScape, partially for providing a fully capable Web security offering that contains the flexibility to deploy as on-premises hardware, a virtual deployment, a SaaS service, or hybrid model. Customers can also extend policy enforcement to protect mobile users. In addition to the McAfee antivirus engine, the gateway offering does emulation of the code to stop zero-day malware, even if it is malicious JavaScript embedded in a Web page.

The offering provides application visibility over popular SaaS services, such as Box and salesforce.com. It can identify Web applications in use and control acceptable use policies. Single sign-on and multifactor authentication is built-in and includes Active Directory integration.

The on-premises gateways have full DLP dictionaries built into them for defining and enforcing policy. Customers also have the ability to apply encryption for Box and other SaaS services. Customers also have the ability to set policy once and push it out on-premises and in the cloud. Administrators can also redirect users onto the SaaS solution when they are off the network through a client agent.

Content is inspected based upon reputation, geolocation, URL categorization and filtering, and media and file analysis. The Web protection offering can identify botnets attempting to communicate with command and control servers and performs emulated Web site code analysis to identify threats. It integrates with Intel Security DLP technology and performs SSL decryption for analysis of user-generated content across HTTPS-encrypted communications.

The McAfee SaaS Web Protection offering secures inbound and outbound Web traffic, provides granular controls over social media and Web site use, and can enforce encryption and other data governance policies. It includes antimalware, signature-based antivirus, and threat reputation filters and can strip malicious elements from Web pages. Setup can be done by changing client browser proxy settings or a proxy auto configuration (PAC) file. McAfee also makes available its automated client proxy.

The Web security solution also provides granular control over more than 1,000 popular Web applications. Intel also provides centralized reporting and management across its Web security offerings through the management console. It connects with McAfee ePolicy Orchestrator (ePO) for integration with adjacent security products. The gateway is tied to Intel Security antimalware protection and Global Threat Intelligence (GTI) service.

Strengths

- Intel has a strong data loss prevention engine with full dictionaries built into its appliances and the ability to enforce policies in some cloud-based services, such as Box.
- Intel is examining code behavior of Web pages that use JavaScript and can stop zero-day malware by doing an emulation of the code being used on a user's system.
- A botnet client can identify botnets attempting to communicate with command-and-control infrastructure. The company can also force employees onto the SaaS solution when they are off the network.

Challenges

- Intel sold its Stonesoft UTM and Sidewinder legacy firewall appliances to Raytheon, exiting the firewall market, surprising some customers and channel partners. The move could bolster its research and development into cloud and Web security protection, but it also could lead to considerable changes to its channel partner base.
- The ePolicy Orchestrator, the central management hub that is at the core of the company's third-party technology partner ecosystem, is still largely an on-premises platform. A SaaS ePO product has been introduced but it is still too early to assess its effectiveness.
- The Intel and McAfee engineering teams are working closely under the leadership of Christopher Young, the general manager of the Intel Security Group at Intel. Young must balance the chip maker's strategic priorities with further development of established security products in the portfolio.

Sophos

Sophos is positioned as a Major Player in this IDC MarketScape. Sophos introduced its secure Web software in 2007 and today offers the Sophos Web Appliance and SaaS-based Web security gateway, which is part of the company's cloud-managed security offering. The company targets small and midmarket enterprises and is currently rolling out the components of its unified threat defense strategy, which consists of a fully interoperable mobile, endpoint, and networking security platform that can be managed through a single console.

Sophos' SaaS-based Web security consists of its Mojave Networks acquisition and the offering has a different management console and features. It supports cloud management, enforcement, and reporting and relies on a separate endpoint agent. Sophos has integrated its malware detection engine into the Mojave product. It requires its own endpoint agent, which needs a connection to the Sophos proxy for malware detection in the cloud. There are plans to offer a hybrid deployment option in 2016.

Sophos customers tell IDC that the Sophos Web Appliance is easy to manage and affordable and many reported that the deployment also included other products within the company's portfolio to solve endpoint, mobile, Web, and email inspection requirements. Sophos' technical support and assistance during initial deployments was also praised. Many customers report using other solutions for their network security strategy but said that long-term plans include evaluating Sophos' UTM in support of a fully integrated security infrastructure as well as products offered via Sophos' cloud-managed portfolio.

Sophos' Web security appliance includes role-based access control administration, Web-based management console, and real-time dashboard reporting for end-user Web activities. It has granular social media controls and extends minimal policy restrictions to popular SaaS-based services. The appliance also has data loss prevention capabilities to prevent the exposure of sensitive data.

Sophos supports SSL decryption to enable the inspection of encrypted (HTTP) Web traffic for threats. It offers controls that can be enabled by administrators to avoid scanning financial and healthcare-related traffic to address privacy issues and maintain the protection of regulated data.

Strengths

- Sophos has been diligently working on its long-term plan to create a full-featured, easy-to-use unified suite that addresses endpoint, networking, Web, email, mobile, and cloud security requirements. Once the vision is fully achieved, the result should appeal to small and midsize enterprises and managed security services providers.
- Sophos sales channel team consists of seasoned veterans who are building out a global program that includes ongoing training and skills development opportunities that are attracting managed security services providers. This should result in strong support.
- The acquisition of Mojave Networks bolsters Sophos' Cloud Web Gateway. Midmarket organizations will value the combination of endpoint, server, and full Web gateway protection managed in the cloud.

Challenges

- Sophos CTO Gerhard Eschelbeck, who headed Sophos' cloud enablement and long-term unified protection strategy, departed the company in October 2014. Sophos named Eschelbeck's replacement, Joe Levy, in February 2015. Levy was at Blue Coat following its acquisition of Solera Networks. Sophos' said the leadership change went smoothly. Levy continues to oversee the long-term vision for a wholly unified threat management suite that incorporates endpoint and network protection as well as mobile and cloud security via a centralized console.
- Customers interested in standardizing on a single vendor for Web, email, networking, and endpoint protection should note that Sophos does not offer products specifically designed for advanced threat detection and prevention, including sandboxing to analyze suspicious files and other threats used in targeted attacks.
- Sophos is still developing a hybrid offering for customers that want an on-premises appliance and a subscription to its Cloud Web Gateway to address remote and mobile employees. The

company does not yet have real-time reporting and is also still relying on the ClamAV engine for the detection of known threats rather than the Sophos engine. Executives say Sophos engineers are still working on the Mojave integration and plan to launch a series of updates in 2016 to address these issues.

Symantec

Symantec is positioned as a Contender in this IDC MarketScape. Symantec offers virtual appliances, hardware appliances, and SaaS/cloud offerings for Web security and is currently planning to overhaul its Web security strategy. Symantec's Web security solutions are the combination of two acquisitions: the acquisition of MessageLabs in 2008, which introduced Web and messaging security SaaS to Symantec, and the acquisition of Mi5 in 2009, which brought hardware/software-secure Web gateway products into Symantec's portfolio.

Symantec did not provide product documentation and customer references or discuss its strategy and road map with regard to its Web security offerings. Symantec still offers Symantec Web Security.cloud for malware protection, URL filtering, and data protection. The Symantec Web Gateway offering integrates with Symantec Data Loss Prevention.

Symantec has been undergoing serious internal restructuring over the past several years. The company is shedding its Veritas storage unit. The company has recently released specialized threat detection and analysis products and updated its endpoint security suite to keep pace with emerging start-up solutions.

Strengths

- Symantec CEO Michael Brown is focusing efforts on modernizing and integrating the company's broad product portfolio. Shedding the storage business is giving the company opportunity to be more nimble to broader market trends.
- Symantec is adding subscription-based services for threat intelligence and targeted attacks. The company also added advanced threat detection that extends across endpoints, networks, and email gateways, which is a major asset to its Web security solutions.
- Symantec leverages threat intelligence from its global customer base to bolster its products. Customers report that the cloud solution had minimal latency and was a good option to extend corporate policies to remote and mobile workers.

Challenges

- Symantec failed to gain wide adoption of its on-premises appliance, which may be an indicator of its desire to focus on a SaaS security strategy. This comes at a time when many organizations are adopting a hybrid approach.
- Symantec has a strong mobile security portfolio it gained through the acquisition of Nukona and Odyssey Software, but internal changes may have set back integration with its Web security offerings.
- Symantec is becoming a much leaner public company, but the company is currently in the awkward position of integrating its aging portfolio while trying to keep up with a flurry of security start-up activity. Existing customers expect the company to modernize its portfolio with new approaches to threat detection and prevention.

Trend Micro

Trend Micro is positioned as a Major Player in this IDC MarketScape. Trend Micro's Web security offering includes the InterScan Web Security Virtual Appliance, a fully capable InterScan Web Security SaaS service, and an integrated hybrid solution, all of which can be integrated with other security products in its portfolio.

Trend Micro offers fully capable Web security products and flexible deployment options. InterScan Web Security Virtual Appliance provides all the standard Web security gateway capabilities. Advanced threat protections include zero-day document exploits detection, C&C callback detection, and real-time browser emulation. The gateway also uses heuristics to monitor the behavior of files. Administrator notifications are sent via email to the designated administrator contacts. Integrated DLP for both HTTP(s) and FTP protocols are supported.

The gateway virtual appliance also integrates with Deep Discovery, the advanced threat protection product that makes up Trend Micro's Custom Defense portfolio. Deep Discovery adds suspicious file analysis in a sandbox environment to identify threats associated with targeted attacks. Deep Discovery is not available as a SaaS offering, but Trend executives tell IDC this will be available in the first half of 2016.

All the advanced threat protections are supported by global threat intelligence from the Trend Micro Smart Protection Network (SPN). It delivers comprehensive Web security protection for customers. SPN correlates over 100TB of threat data daily from its global sensors, across multiple threat vectors. Trend said the network is supported by more than1,200 threat researchers.

InterScan Web Security as a Service includes URL filtering, application control, antimalware protection for uploads and downloads, and advanced threat protection. Organizations must use a proxy or configure port forwarding or proxy chaining to redirect traffic to the InterScan servers. The SaaS service can decrypt SSL-encrypted traffic for inspection. The service relies on mobile VPN to protect iOS and Android-based mobile devices by tunneling traffic to and from Trend Micro servers. The SaaS service also includes an enforcement agent for Windows and Mac users, enabling enforcement of policies, regardless of whether the device is running on the corporate network.

InterScan Web Security Hybrid was launched in 2014 and combines the InterScan SaaS service with the InterScan Web Security Virtual Appliance. The hybrid approach enables organizations to scan incoming and outgoing Internet traffic via the virtual appliance and the SaaS offering. It includes data loss prevention and support for zero-day exploit detection, advanced antimalware scanning, real-time Web reputation, and granular URL filtering and granular application control. The hybrid approach can be managed through a single Web-based console.

Trend Micro customers told IDC the Web security gateway is easy to use and today has flexible licensing options. Customers have the ability to mix and match cloud and on-premises services within the same license. Trend Micro restructured its security suite offerings after getting better visibility into the pure SWG component of its revenue models. Customers and resellers told IDC that the security vendor's growing portfolio of endpoint and custom defense products led to a myriad of bundled components that were difficult to comprehend. Trend executives have worked quickly to simplify its suites. Trend offers two suites, reducing the number of bundled suites from seven.

In addition, Trend Micro executives instituted a formalized review process to eliminate underperforming partners and bolstered training, skills development, and support to the most

committed partners. Customers told IDC that the company's technical support had been a problem in the past. Trend said it has addressed technical support issues, recently adding 24 x 7 customer support as a standard service for customers in North America with a support center in Irving, Texas.

Strengths

- Trend has been focusing on cloud security and its Deep Discovery enterprise-grade advanced threat detection solution, which can fit nicely with its Web security offerings. The extent of the company's portfolio supports a unified threat defense approach that is scalable and adaptive to the evolving threat landscape.
- Trend is ahead of competitors with its hybrid offering, offering a flexible licensing model and integrated management console for users of its virtual appliance and SaaS service for remote offices and mobile device protection. Trend has also simplified its packages, establishing separate offerings that appeal to small and midsize businesses and large enterprises.
- An Enforcement Agent used to send traffic to InterScan Web Security as a Service is lightweight and easy to install. It enables additional capabilities to function such as behavior monitoring, browser emulation, threat sandboxing (in 2016), and granular application control.

Challenges

- Trend Micro Interscan Web Security as a Service has limited advanced threat detection capabilities and integration with on-premises security appliances for log and event management. The company said it has plans to add support for a suspicious file analysis service to identify advanced threats. Trend is also adding support for additional capabilities in its portfolio and third-party security products often used by organizations with mature security programs.
- Trend has largely addressed issues related to technical support and portfolio complexity, but customers evaluating products in the security vendor's portfolio should assess the effectiveness of the changes by speaking with customer references to determine if it resulted in significant improvements.
- Trend Micro is creating a centralized management console to enable administrators with the flexibility to manage multiple – on-premises, SaaS, and hybrid – deployment models. Currently, management capabilities are contained in separate consoles.

Trustwave

Trustwave is positioned as a Contender in this IDC MarketScape for Web security because of its strong compliance heritage and growing managed services practice. Singtel, one of the largest mobile network operators in Singapore, acquired Trustwave in an $810 million deal in 2015.

Trustwave has been taking its various security market acquisitions and turning them into managed services delivery mechanisms. It provides a management services portal where customers can add products in the portfolio. IDC estimates Trustwave's revenue at $216 million in 2014. Trustwave's Web security presence is the result of its acquisition of M86 Security in 2012. The portfolio also includes a wide range of security products, including a Web application firewall, security information event management system, network access control, data loss prevention, secure messaging, and vulnerability management. Many of the products are a critical part of addressing regulatory compliance challenges for Trustwave's customers, which include a mixture of financial institutions, healthcare, government agencies, and education.

Trustwave's Secure Web Gateway is sold in three levels of appliances, a VMware-based virtual appliance, and a hybrid cloud. Flexible deployment options allow varying capacity of the appliance, ranging from 32Mbps to 66Mbps of https at 50% CPU load to the Trustwave blade server, which can handle 16 scanners, each handling 66Mbps for a total of 1,056Mbps or 1Gbps. The blade server works on 10Gb networks. The latest version fully supports Microsoft Outlook Web Access 2013.

Trustwave's Web security offering is powered by the Trustwave SpiderLabs security research team. Trustwave also offers a managed antimalware service that the company guarantees will be 100% effective at blocking malware that propagates over the Web, including zero-day exploits that attackers use in Web-based attacks.

In addition to URL filtering, customers have the option to select a signature-based antivirus engine from Sophos, McAfee, or Kaspersky Lab. Behavior-based engines scans image files, PDFs, and other file types to detect vulnerabilities.

The product also includes the Trustwave Malware Entrapment Engine, which leverages a virtual instance of a browser in real time and analyzes everything that is happening before it is displayed on an end user's browser. The engine does not rely on signatures or heuristics. It is vulnerability based, meaning it conducts static and dynamic page analysis, examining active page content, HTML and scripts, ActiveX content, Java, JavaScript, and other Web components and can write rules to block any potential malicious activity that it finds. The latest version of the secure Web gateway also can identify and block botnet communications. It also has an embedded DLP engine to identify sensitive data or regulated data and can be configured to block or warn end users based on set policies.

The solution has granular controls over Facebook, Twitter, Google+, YouTube, and LinkedIn and can enforce DLP policy for social media. Trustwave also recently released controls for popular cloud storage services, supporting Google Drive, Box, Dropbox, Microsoft OneDrive, and Apple iCloud.

The Trustwave cloud architecture is based on a hosted virtual instance. This model creates virtual images of the Web gateway on the Amazon Web Services platform as well as in the customer's own network infrastructure. Trustwave can support hybrid deployments to extend protection to remote offices and off-premises laptop users.

Trustwave uses a subscription-based model for its Web security gateway, charging organizations for the number of users they have. Larger enterprises have the option to purchase a purpose-built security reporter to log activity detected by the gateway and handle raw data.

Strengths

- Trustwave executives say the secure Web gateway is a core product in the company's portfolio. Singtel has stated that it would not retire products in the portfolio and the Singtel is expected to expand the Web gateway adoption in Asia.
- The combination of Trustwave's managed services practice and the Trustwave SpiderLabs security researcher team differentiates the vendor against competitors. It includes a managed antimalware service that the company guarantees will be 100% effective at blocking malware that propagates over the Web, including zero-day exploits that are used in a Web-based attack.
- Trustwave's Malware Entrapment Engine provides strong malware detection and mitigation of Web-borne threats. The company has built out an enduring customer base in the financial services industry.

Challenges

- The solution only supports single tenancy. Trustwave hosts its proxy servers in Amazon's EC2 cloud infrastructure as opposed to Trustwave owning and maintaining its own datacenters.
- Trustwave's fully SaaS Web security service is expected to be released globally in 2016.
- Trustwave has largely addressed latency issues, but the throughput of its appliances should be evaluated against competitive solutions.

Zscaler

Zscaler is positioned as a Major Player in this IDC MarketScape. Zscaler is a Major Player in the Web security market and remains the only pure-play SaaS vendor among the group. Founded in 2008, Zscaler first offered a Web security cloud service and experienced rapid growth. The company's strategy has been to add features and capabilities supported in its multitenant, distributed cloud service. It has moved toward offering a SaaS-based unified defense strategy with the addition of an extensive set of subscription-based security services, including a file analysis sandbox as part of its advanced threat detection offering and secure wireless service.

Organizations often hold the common misconception that because Zscaler has a cloud-based Internet security platform, it was designed for small and midsize organizations. But a review of the company's customers will find that many of its early adopters include big-name brands in the Fortune 1000. The company claims 18 of the Global 100 are among its 5,000 customers. The company has demonstrated its ability to scale with some global brands protecting the entire user base with Zscaler.

Zscaler received $125 million in new funding rounds in 2015, including a $25 million investment from GV (formerly known as Google Ventures). Today, the company is valued in excess of $1 billion. The company has reported a strong customer retention rate despite increased competition from gateway manufacturers coming to market with fully capable SaaS offerings.

Zscaler's minimal subscription offering includes URL filtering, inline antivirus, and antispyware and real-time reporting with full Active Directory and LDAP integration, granular policy control, and support for remote offices, laptops, and mobile devices. An Enterprise Web Suite adds visibility and controls for social media, Webmail, and other popular SaaS-based services, inline data loss prevention, bandwidth management, and an SSL VPN. It also includes a cloud-based sandbox for suspicious file analysis, SSL decryption for full inspection of encrypted traffic, and the ability to restrict inspection of traffic associated with banking and healthcare data to address privacy concerns and regulatory compliance obligations.

The company has expanded its global datacenter footprint with more than 100 locations for availability and maintaining suitable bandwidth while providing policy enforcement. Zscaler currently has about 5,000 customers and claims that in more than 95% of its deployments, the company's solutions have been adopted across the entire organization. Adoption is almost always through full global rollouts, enabling Zscaler to demonstrate its ability to scale in processing all the Internet traffic of each customer. It also has a service to add a layer of security for Amazon WorkSpaces.

Zscaler was founded by Jay Chaudhry, a successful high-tech entrepreneur in the networking market, and the company includes technical and business executives from such firms as Check Point, Palo Alto Networks, and Motorola, as well as operational expertise from large service providers and enterprises. The company is cash positive and was privately funded from its inception.

Strengths

- Zscaler maintains a SaaS delivery model with no requirement for on-premises management servers. This SaaS model provides immediate access to new offerings, product updates, and rapid protection against emerging attacks.
- Zscaler's management team led by Jay Chaudhry, a networking market veteran, has built out the portfolio's capabilities while maintaining cash positive operations.
- Customers consistently praise Zscaler for its ease of use, its ability to easily extend support to mobile users, and its strong Web-based management capabilities.

Challenges

- SSL decryption is supported with the caveat that there will be performance degradation.
- Zscaler uses a device-based agent to support iOS, Android, and Windows mobile devices, which can be bypassed by employees with technical aptitude. It supports Samsung KNOX to enable customers to extend controls to Samsung's mobility management offerings.
- Zscaler's support of popular-based SaaS applications, such as salesforce.com, is limited to allowing or blocking access to those services. The company is partnering with Adallom for more granular support for SaaS applications and information risk scoring.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of a review board of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

This IDC MarketScape assesses the market for enterprise-class Web security products as defined in IDC's security products taxonomy, with a specific focus on Web security features and submarkets, including Web and URL filtering; antimalware, antivirus, and malicious code and script blocking; detection of botnet traffic and outbound threat activity; and Web application and social media controls and outbound (data leakage) threats.

In addition to these features and functions, delivery models were also a major criteria considered. On-premises software, which includes virtual appliances, hardware appliances, and software as a service or cloud services, were all analyzed, if applicable. Vendors rated higher if they offered more platforms as well as for demonstrating high levels of integration and feature parity across the platforms and support for hybrid-type deployments with unified management, reporting, and policy creation, as well as scalability.

Some of the key functionality and features examined in this study include social media and Web 2.0 controls; the ability to support mobile users including laptops, smartphones, and tablets; and the ability to support branch offices with Web security functionality, whether through WAN backhaul to a centralized appliance or via the cloud proxy service. IDC also considered what adjacencies and synergies existed among the vendors' Web security offerings and other security and IT product offerings.

While Web application firewall (WAF) is a subsegment of the Web security market in IDC's security products taxonomy, WAF features and WAF-focused vendors were not considered in this study. The difference between secure Web gateways and WAF is people versus machines: Web security gateway products examined in this IDC MarketScape are focused on protecting enterprise end-users' activity and access to the Web and HTTP-based applications and services (both on the Internet and private networks), and WAF protects Web servers and applications from intrusions and attacks.

Strategies and Capabilities Criteria

As part of this study, IDC examined vendor offering strategy. This includes a review and comparison of product functionality and available delivery options. Also incorporated into the analysis were competitive licensing and pricing, support, and integration with a portfolio of products. The vendor offering strategy also included a review of the integration strategy and planned development to address customer requirements.

This study examined an offering's ability to monitor inbound and outbound threats, the processing speed of on-premises gateways, and any latency associated with SaaS Web security offerings. IDC also assessed the strength of each vendor's threat intelligence capabilities and how quickly protection can be delivered when new threats are identified.

IDC assessed the relative strength of each Web security vendor's user community and its ability to engage with its customer base. It looked at presale and post-sale activities and ability to keep up with technology and threat trends.

IDC also considered each vendor's go-to-market strategy. The review assessed the marketing strategy, sales and distribution strategy, and customer service effectiveness. The business strategy took into account each vendor's financial strength based on data provided by vendors and collected from publicly available sources. Tables 1 and 2 present the key strategy and capability measures for success for Web security vendors, respectively.

TABLE 1

Key Strategy Measures for Success: Worldwide Web Security

Strategies Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weightings
Offering strategy		
Functionality or offering road map	IDC took into account each vendor's ability to provide fined-grained controls and role-based policy management across end users. Customers are also requiring functionality to enable policies to extend to mobile devices and remote workers. Additional protection and control over employee use of SaaS services is also being requested.	2.0
Delivery model	Web security vendors are establishing a delivery model that encompasses a gateway appliance, a cloud-based service, and/or a virtual software option. Organizations are increasingly choosing a hybrid model that incorporates the management capabilities and controls that Web administrators are accustomed to seeing coupled with a SaaS deployment. Vendors that are ahead typically have feature sets in their SaaS offering that mirror on-premises deployments and have or are creating centralized reporting and management capabilities.	3.0
Cost management strategy	This takes into account each Web security vendor's ability to manage research and development activities, provide additional features and capabilities without disrupting generally accepted workflows and processes, and identify and execute on an innovation curve that takes into account cloud adoption and current datacenter needs.	1.0
Future integration strategy	Future integration strategy takes into account the ability of Web security products to add functionality to address the changing nature in which data is consumed. This includes an examination of mobile security capabilities, cloud security protection, and integration with specialized threat analysis and protection to address advanced threats associated with targeted attacks and custom malware.	1.0
Portfolio strategy	Web security vendors must provide a platform that can support a wide variety of architectures, a myriad of applications, and extend to highly used SaaS services. The portfolio strategy takes into account the extent of support provided for each delivery option, the interoperability with existing and emerging Web protocols, and the length of time the Web security product has been on the market.	1.0
Scalability strategy	IDC took into account the size of the threat intelligence cloud serving the Web security solution, the number of data sources used to collect relevant data about malicious Web activity, and any planned improvements.	2.0
Subtotal		10.0
Go-to-market strategy		
Pricing model	For Web security, IDC is taking into account costs associated with optional capabilities, flexible licensing, and bundling options. It examines the complexity of the vendor's pricing model and ability to work with clients to meet their unique requirements.	3.0
Sales/distribution	For the Web security market, IDC took into account the sales segmentation between cloud and on-premises offerings, the sales distribution model, and number of sales	2.0

TABLE 1

Key Strategy Measures for Success: Worldwide Web Security

Strategies Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weightings
strategy	personnel. IDC also assessed the quality of the channel program for vendors that rely on indirect sales.	
Marketing strategy	The quality of a Web security vendor's marketing strategy is assessed taking into account the strength of messaging targeted to buyer segments, the strength of messaging and activities focused on a specific industry vertical and the trial offerings, and ease at which potential customers can evaluate the product themselves.	2.0
Customer service strategy	For purposes of this study, IDC looked at the strength of the product documentation, the ability for potential customers and current customers to engage with existing customers on challenges they are experiencing, and the ability of sales personnel to stay engaged with customers in presales and post-sales activities.	3.0
Subtotal		10.0
Business strategy		
Growth strategy	IDC took into account the strategic vision of a Web security vendor's product and management teams to expand the product to adjacent security areas and integrate with cloud services.	3.0
Innovation/R&D pace and productivity	IDC examined how well each Web security vendor leveraged its research team and R&D engineers as part of creating innovative components. It also took into account each vendor's plans to bring its SaaS and on-premises capabilities to be compatible and centralized for organizations adopting a hybrid approach. IDC also sought to get vendors to articulate future plans for organic or inorganic growth.	4.0
Financial/funding model	This considers the forecast profitability of a vendor's Web security business unit and the projected revenue three years from now.	2.0
Employee strategy	Web security vendors — all security vendors — face the challenge of finding and retaining skilled workers, taking into account each vendor's retention program and path to promotion.	1.0
Subtotal		10.0

Source: IDC, 2016

TABLE 2

Key Capability Measures for Success: Worldwide Web Security

Capabilities Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weightings
Offering capabilities		
Functionality/offering delivered	IDC examined each Web security vendor's ability to provide a set of intuitive end-user controls across all channels. IDC also takes into account the ability of the product to decrypt encrypted traffic (SSL decryption) and whether granular controls are available to address privacy concerns and regulatory mandates. Finally, IDC reviewed whether each Web security vendor was able to couple simple URL filtering capabilities with antimalware and other security capabilities.	2.0
Delivery model appropriateness and execution	IDC considered each Web Security vendor's ability to support a hybrid deployment (SaaS and on-premises), the execution on providing deep visibility and controls into popular Web applications, and how often Web security gateways are updated to provide protection and functionality.	1.0
Cost competitiveness	To gauge cost-competitiveness, IDC reviewed the hardware efficiencies, whether each Web security vendor owned its core intellectual property or licensed it from another vendor, and examined the cloud-based backbone supporting the SaaS offering and threat intelligence data collection.	1.0
Portfolio benefits delivered	A review was conducted to determine how closely integrated Web security features are delivered with other adjacent security technologies, such as networking security appliances. IDC also examined the strength of each Web security vendor's encryption, data loss prevention, and messaging components integrated into the Web security offering. Finally, IDC looked at the vendor's reporting capabilities, examining whether they can be aggregated and correlated across multiple devices.	1.0
Integration	IDC reviewed whether Web security vendor products integrated with an existing portfolio of security products and whether it could be extended to support third-party security solutions. IDC also took into account whether Web security products provided flexible options to extend controls to branch offices and remote workers.	2.0
Scalability	IDC examined the number of global datacenters and system redundancies that support SaaS Web security offerings to provide the least amount of latency; it also looked at how well the SaaS offering has demonstrated its scalability by the number of nodes it currently can support. In turn, the hardware was reviewed to determine whether it supports multitenancy and can be expanded as an organization's requirements grow.	1.0

TABLE 2

Key Capability Measures for Success: Worldwide Web Security

Capabilities Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weightings
Other offering capabilities	IDC took into account how often threat intelligence was refreshed to provide additional protection, the number of on-premises gateway deployments of each vendor, and the number of subscribers to SaaS-based Web security offerings.	2.0
Subtotal		10.0
Go-to-market capabilities		
Pricing model options and alignment	The analysis in this Web security study focused on whether each vendor provided flexible multiyear/single-year licensing options and whether multiple features and components were included in the base price of the product. IDC also attempted to determine if discounts existed for bundling additional products in a Web security vendor's portfolio.	2.0
Sales/distribution structure, capabilities	IDC examined the strength of the sales team's ability to sell product in multiple regions, the use of skilled resellers and systems integrators to support deployments, and whether the sales structure is in line with customer expectations.	3.0
Marketing	IDC considered brand awareness, messaging, and thought leadership in the area of secure mobility, secure cloud services adoption, and other key themes. Also factored into the analysis was the percentage of marketing spend against product line revenue.	2.0
Customer service	Each Web security vendor's support model was reviewed and service integration required to support hybrid and cloud deployments. Also examined was the support services made available for customer hybrid deployments, and researchers sought customer retention rates as part of the study.	3.0
Subtotal		10.0

TABLE 2

Key Capability Measures for Success: Worldwide Web Security

Capabilities Criteria	Market-Specific Subcriteria Definitions	Subcriteria Weightings
Business capabilities		
Growth strategy execution	IDC examined company financials to include year-over-year revenue growth, plan, and execution on seizing opportunity in adjacent markets and new market segments.	3.0
Innovation/R&D pace and productivity	IDC requested from Web security vendors their estimate of research and development spending as a percentage of revenue from each vendor as well as the number of engineers devoted to research and development activities.	4.0
Financial/funding management	IDC sought to identify clues that a vendor was running the business at a loss and whether enough liquidity was available over the next 18–24 months to withstand changing market conditions and assessed this against the customer install base when available.	2.0
Employee management	IDC examined the strength of the executive leadership team, its background in the security industry, and demonstrated ability to plan and direct the execution of the vendor's strategic priorities. Internal restructuring, management changes, and sales executive departures were incorporated into this analysis.	1.0
Subtotal		10.0

Source: IDC, 2016

LEARN MORE

Related Research

- *Worldwide Web Security Forecast, 2015-2019: Steady Transition to the Cloud* (IDC #258801, September 2015)
- *Worldwide Web Security Market Shares, 2014: Transition to SaaS Continues* (IDC #258804, September 2015)
- *IDC Web Security Vendor Watch List* (IDC #IcUS25907215, September 2015)

Synopsis

This IDC study uses the vendor assessment model called IDC MarketScape, which pulls together a vendor's quantitative and qualitative characteristics to examine each vendor's market potential. The Web security market is mature, with most vendors providing standard functionality. This study examined Web security integration with adjacent security technologies, such as emerging solutions

designed to detect targeted attacks and custom malware. Some security vendors are closely integrating their advanced threat defense portfolio with traditional gateways, network, and endpoint security products. Vendors fared strongly if they could demonstrate a fully capable SaaS Web security offering that mirrors on-premises gateway functionality and centralized reporting and management capabilities.

"Vendors in the Web security market are continuing to transition to the cloud and address changes in end-user behaviors associated with mobile and cloud services adoption. Customers' demand a Web security offering that integrates with their existing security investments and one that can adapt to the increasingly distributed nature of most corporate environments," said Robert Westervelt, research manager for IDC's Security Products.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com