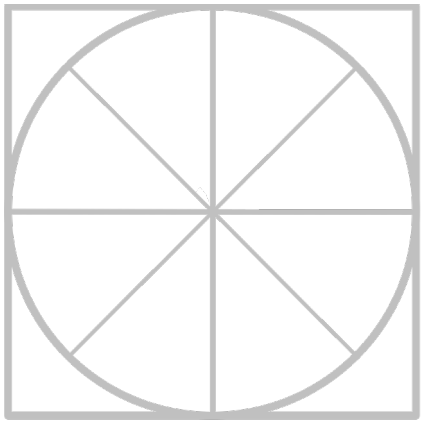
The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Advanced Persistent Threat (APT) Protection - Market Quadrant 2017



An Analysis of the Market for APT Protection Solutions Revealing Top Players, Trail Blazers, Specialists and Mature Players.

March 2017

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 posses 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.

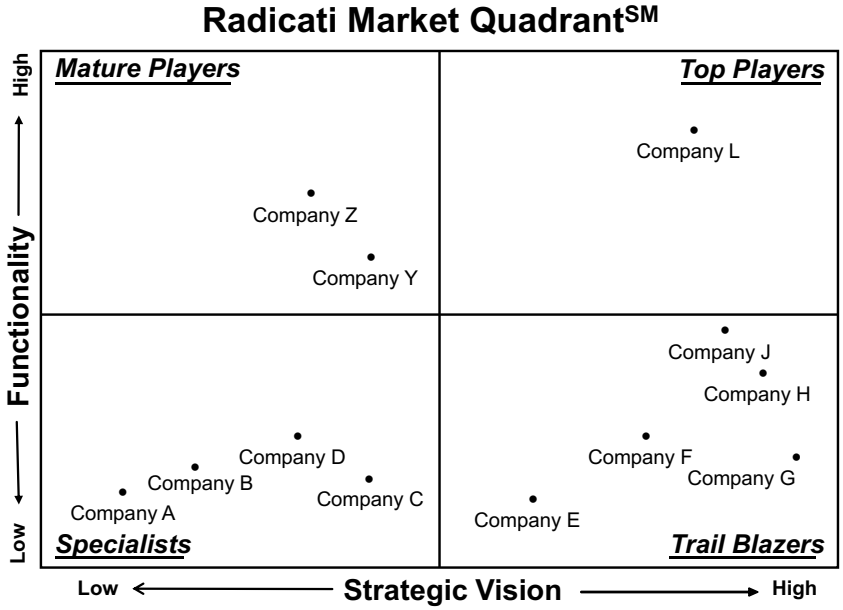


Figure 1: Sample Radicati Market Quadrant

MARKET SEGMENTATION – ADVANCED PERSISTENT THREAT (APT) PROTECTION

This edition of Radicati Market Quadrants[SM] covers the "**Advanced Persistent Threat (APT) Protection**" segment of the Security Market, which is defined as follows:

- **Advanced Persistent Threat Protection –** are a set of integrated solutions for the detection, prevention and possible remediation of zero-day threats and persistent malicious attacks. APT solutions may include but are not limited to: sandboxing, reputation networks, threat intelligence management and reporting, forensic analysis and more. Some of the leading players in this market are *BAE Systems, Barracuda Networks, Cisco, FireEye, Forcepoint, Fortinet, Intel Security, Kaspersky Lab, Palo Alto Networks, Symantec, Webroot,* and *others.*

- This report only looks at vendor APT protection installed base and revenue market share in the context of their enterprise business, it does not include solutions that target service providers (carriers, MSPs, etc.).

- APT protection solutions can be deployed in multiple form factors, including software, appliances, private or public cloud, and hybrid models. Virtualization and hybrid solutions are increasingly available through most APT security vendors.

- APT solutions are seeing rapid adoption across organization of all business sizes and industry segments, as organizations grow increasingly concerned about zero-day threats and targeted malicious attacks.

- The worldwide revenue for APT Protection solutions is expected to grow from over $3.2 billion in 2017, to over $7.5 billion by 2021.

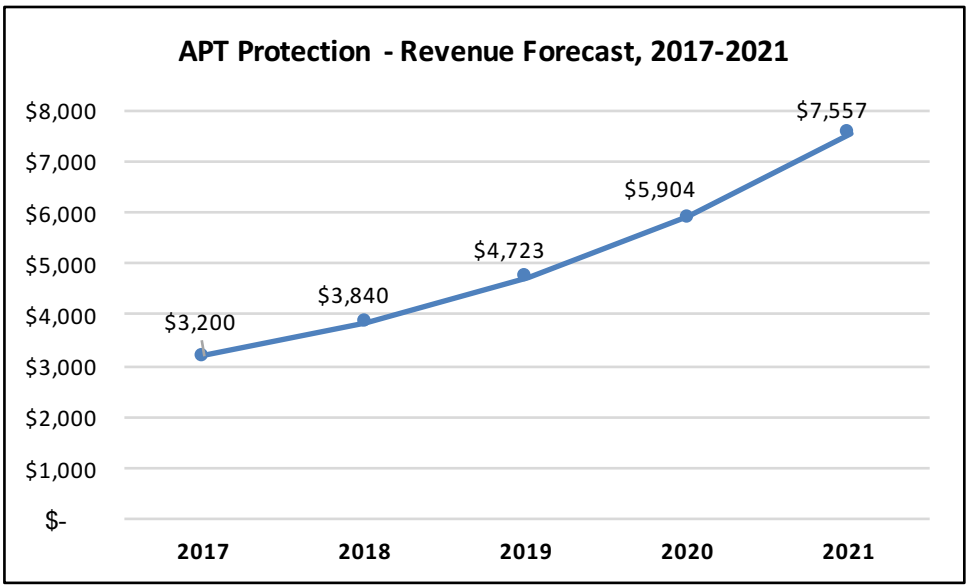


Figure 2: APT Protection Market Revenue Forecast, 2017 – 2021

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 *APT Protection* 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 solutions, cloud-based services, hybrid, appliances and/or virtual appliances.

- ***Malware detection*** – usually based on behavior analysis, reputation filtering, advanced heuristics, and more.

- ***Firewall & URL*** – filtering for attack behavior analysis.

- ***Web and Email Security*** – serve to block malware that originates from Web browsing or emails with malicious intent.

- ***SSL scanning*** – traffic over an SSL connection is also commonly monitored to enforce corporate policies.

- ***Encrypted traffic analysis*** – provides monitoring of behavior of encrypted traffic to detect potential attacks.

- ***Forensics and Analysis of zero-day and advanced threats*** – provide heuristics and behavior analysis to detect advanced and zero-day attacks.

- ***Sandboxing and Quarantining*** – offer detection and isolation of potential threats.

- ***Directory Integration*** – for instance integration with Active Directory or LDAP, to help manage and enforce user policies.

- ***Data Loss Prevention (DLP)*** – allows organizations to define policies to prevent loss of sensitive electronic information.

- ***Mobile Device Protection*** – the inclusion of Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) features to help protect mobile endpoints.

- ***Administration*** – easy, single pane of glass management across all users and network resources.

- ***Real-time updates*** – to rapidly block, quarantine and defend against newly identified threats or attacks across all network resources.

- ***Remediation*** – refers to the ability to automatically restore endpoints, servers and other devices to a healthy state, in the event they have been compromised. Remediation may involve re-imaging and/or other cleanup processes and techniques.

- ***Environment threat analysis*** – to detect existing exposure and potential threat sources.

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 – APT PROTECTION

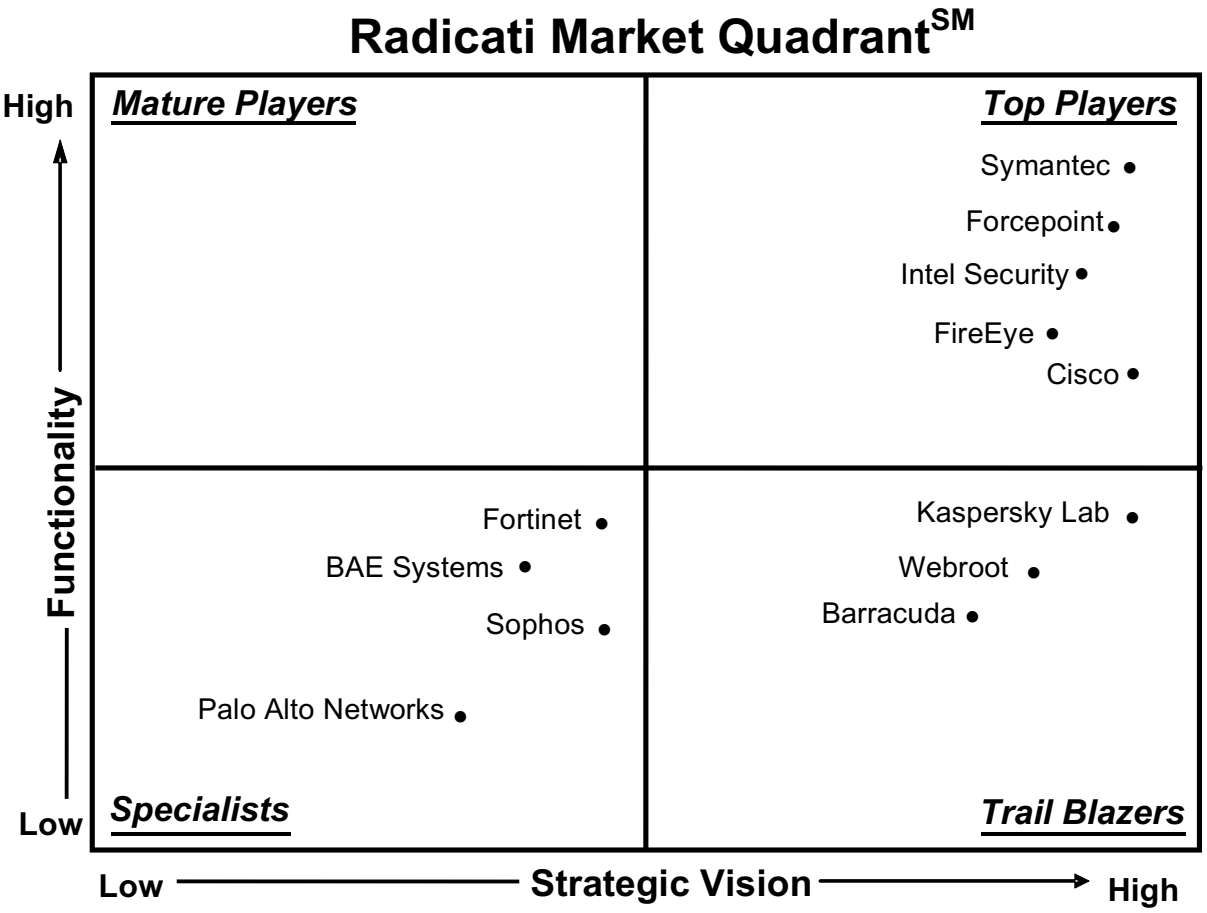


Figure 3: APT Protection Market Quadrant, 2017

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

KEY MARKET QUADRANT HIGHLIGHTS

- The **Top Players** in the market are *Symantec*, *Forcepoint, Intel Security, FireEye,* and *Cisco***.**
- The **Trail Blazers** quadrant includes *Kaspersky Lab*, *Webroot,* and *Barracuda Networks*.
- The **Specialists** quadrant includes *Fortinet, BAE Systems, Sophos, and Palo Alto Networks*.
- There are no **Mature Players** in this market at this time.

APT PROTECTION - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

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

Founded in 1982, Symantec has grown to be one of the largest providers of enterprise security technology. In 2015, Symantec completed its split into two independent public traded companies, Symantec focused on security, and Veritas focused on information management. In 2016, Symantec completed its acquisition of Blue Coat, a leading provider of web security technology. Symantec's security solutions are powered by its *Global Intelligence Network* which combines technologies from both Symantec and Blue Coat, to offer real-time threat intelligence.

SOLUTIONS

Symantec provides on-premises, hybrid and cloud-based solutions for advanced threat protection to safeguard against advanced persistent threats and targeted attacks, detect both known and unknown malware, and automate the containment and resolution of incidents. Symantec's security portfolio comprises the following components:

- ***Symantec Advanced Threat Protection (ATP)*** **–** is a unified platform that uncovers, prioritizes, investigates, and remediates advanced threats across multiple control points from a single console. It aggregates and correlates threat events from the four ATP modules: Endpoint, Email, Network, and Roaming. Symantec ATP is a hybrid solution that consists of an on-premises appliance (or virtual appliance) that uses cloud services for sandboxing and correlation. Symantec's cloud sandbox leverages global threat intelligence and advanced machine learning, as well as bare-metal execution, to uncover threats. The solution platform provides a single pane of glass across all four modules, providing visibility into attacks in real-time and the ability to quickly remediate attacks across multiple threat vectors. Symantec ATP aggregates threat events across endpoint, network, email, and web traffic, making it easier for security teams to identify and respond to the most relevant incidents.

    - *Symantec ATP: Endpoint module* **–** provides Endpoint Detection and Response (EDR) capabilities without adding a new endpoint agent. It leverages the Symantec Endpoint Protection product, to look for Indicators-of-Compromise (IoC) across all endpoints; remediate all instances of threats, isolate compromised endpoints and blacklist malicious files, all with a single click.

    - *Symantec ATP: Network module* **–** provides automated threat prevention and detection at the network layer by examining both inbound and outbound traffic across all ports and protocols and extracting any suspicious payloads from the network stream. It uncovers stealthy threats with multiple technologies, including: file reputation analysis, IPS, and a cloud-hosted sandbox and detonation capability. Organizations can search for IoCs across their network, and blacklist files or URLs once they are identified as malicious.

    - *Symantec ATP: Email module* **–** protects against email-borne targeted attacks and advanced threats, such as spear-phishing. It leverages a cloud based sandbox and detonation capability and Symantec Email Security.cloud to expose threat data from malicious emails. It inspects URLs embedded in email twice: once when the email passes through the services, and again when the user clicks on the links. It can also export indicators of compromise from the inspected email and integrate with third-party SIEM solutions

    - *Symantec ATP: Roaming module* **–** protects users from advanced threats when they are outside of the corporate network browsing the Internet and provides deep threat visibility into web attacks. It detects and remediates advanced threats, including in encrypted traffic, by leveraging machine learning and a cloud hosted sandbox.

- ***Blue Coat ProxySG appliance, Secure Web Gateway Virtual Appliance, or Cloud Service –*** these solutions serve to block known threats, malicious sources, unknown categories, and malware delivery networks at the gateway in real-time. *Symantec Content Analysis* integrates with the ProxySG appliance to orchestrate malware scanning and application blacklisting, while *Symantec SSL Visibility* provides additional visibility into threats hidden in encrypted traffic across all Symantec components, as well as third party tools.

- ***Symantec Content and Malware Analysis –*** analyzes and mitigates unknown malware by automatically inspecting files though multiple layers of in house proprietary technology as well as third party technology (reputation, dual anti-malware engines, static code analysis, etc.). It then brokers suspicious content to the *Symantec Malware Analysis* solution or other third parties for sandboxing. As the behaviors and characteristics of an unknown threat are identified through automated analysis, intelligence is shared through the *Symantec Global Intelligence Network,* providing enhanced protection across the entire security infrastructure.

- ***Symantec Security Analytics –*** utilizes high-speed full-packet capture, indexing, deep packet inspection (DPI) and anomaly detection to enable incident response and eradicate threats that may have penetrated the network. Intelligence on threats is used to investigate and remediate the full scope of the attack, including other instances of malicious files already residing in the environment. Intelligence is shared across the *Symantec Global Intelligence Network* to automate detection and protection against newly identified threats, for all Symantec customers.

- ***Symantec Global Intelligence Network (GIN)*** – is the combined Blue Coat and Symantec intelligence networks that provides a complete view of all Internet interactions. Symantec's GIN enables the discovery of threats from multiple vectors (e.g. endpoint, network, web, email, application, and more) and proactively protects other vectors of ingress without the need to re-evaluate the threat. It includes an extensive file, URL, IP and mobile app reputation repository.

STRENGTHS

- Symantec offers on-premises, cloud, and hybrid options across most of its security product portfolio. Symantec's endpoint protection and management, traditionally an on-premises solution, was updated in 2016 to offer cloud provisioning and management option.

- Symantec uses a wide array of technologies (both in house and third party) to provide multi-layered protection, including heuristics scanning, file and URL reputation and behavioral analysis, dynamic code analysis, blacklists, machine learning, exploit prevention, and application control. Symantec also utilizes static code analysis, sandboxing and payload detonation technologies to uncover zero-day threats.

- Symantec provides a fully integrated portfolio of solutions to guard against threats across all vectors, including endpoint, network, web, email, application and more.

- Symantec Malware Analysis offers a highly customizable hybrid sandbox solution. In addition, Symantec Advanced Threat Protection leverages its Cynic cloud sandbox with both physical and virtual execution to uncover threats that have "virtual-awareness" and that would otherwise evade traditional sandbox detection.

- Symantec offers a market leading DLP solution that integrates with endpoints, gateways, and cloud applications to prevent data leaks and help achieve industry and regulatory compliance.

- Symantec can analyze mobile device traffic to detect mobile-based APTs, even when users are off the corporate network. The Symantec sandbox includes support for Android files.

- Symantec has integrated Blue Coat's threat intelligence and now offers Total Cloud Protection, which enables Symantec products to query Symantec on-demand for real-time file disposition.

- Symantec ATP provides a single pane of glass across all its modules, providing real-time visibility into attacks, as well as the ability to orchestrate remediation of threats across control points.

WEAKNESSES

- While Symantec offers integration with its DLP solution, the DLP component is a separate add-on product.

- Symantec ATP does not include MDM or EMM features for mobile device protection.

- Symantec is working to offer more flexible reporting options within the product, and to enhance its forensic capabilities.

- While the combination of Symantec and Blue Coat technologies offers a powerful anti-APT and security portfolio, Symantec is still working through all the nuances of integration across its entire product set. Customers should check carefully on the features they expect in each solution component.

FORCEPOINT

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

Forcepoint, is a Raytheon and Vista Equity Partners joint venture, formed in 2015 through the merger of Websense and Raytheon Cyber Products. In 2016, Forcepoint acquired the Stonesoft next generation firewall (NGFW) and Sidewinder firewall assets from Intel Security, and added the Skyfence CASB business from Imperva to its portfolio in 2017.

SOLUTIONS

Forcepoint's product portfolio spans web and email security, CASB, next generation firewalls, DLP, insider threat and government-focused cross domain / network segmentation products.

In the APT space, Forcepoint's product portfolio includes:

- *Forcepoint Web Security* – a Secure Web Gateway solution designed to deliver protection to organizations embracing the cloud, as their users access the web from any location, on any device.

- *Forcepoint Email Security* – a Secure email gateway solution designed to stop spam and phishing emails that may introduce ransomware and other advanced threats.

- *Forcepoint CASB* – allows organizations to safely embrace the cloud by providing visibility and control of cloud applications such as Office 365, Google G Suite, Salesforce, and others.

- *Forcepoint NGFW* – Next Generation Firewalls that connect and protect people and the data they use throughout offices, branches, and the cloud.

- *Forcepoint Advanced Malware Detection* – provides dynamic behavioral analysis of advanced, targeted zero-day threats and advanced persistent threats (APTs) that may attack through various channels. Forcepoint's AMD solution provides last mile detection for advanced and targeted threats.

- *Forcepoint DLP* – a content-aware data loss prevention solution designed to discover and secure an organization's sensitive information and prevent data theft.

- *Forcepoint Insider Threat* – serves to detect risky users and suspicious activities, whether they come from hijacked systems, rogue insiders or users simply making a mistake, in order to prevent damage to organizations.

Key aspects of Forcepoint solutions include:

- *Flexible Deployment Options* – Forcepoint supports cloud deployments, but also provides on-premises, or hybrid options.

- *High-availability, high-performance, secure cloud* – that complies with strict regulations and offers a wide range of cloud connectivity and tunneling options.

- *Forcepoint ThreatSeeker Intelligence* – serves to collect potential indicators of emerging threat activity daily on a worldwide basis, providing fast network-wide updates.

- *Advanced DLP capabilities* – including OCR, Drip-DLP, custom encryption detection, machine learning, and fingerprinting of data-in-motion, data-at-rest, or data-in-use.

Forcepoint's APT solution, Forcepoint Advanced Malware Detection is a scalable, easy-to-deploy, behavioral sandbox that identifies targeted attacks and integrates with Forcepoint Web Security, Forcepoint Email Security, Forcepoint CASB, and Forcepoint Next Generation Firewall products. Forcepoint Advanced Malware Detection is available as a cloud-based

solution, or as an appliance. It provides file and email URL sandboxing, detailing forensic reporting and phishing education.

STRENGTHS

- Forcepoint offers a broad set of integrated security solutions spanning Web, Email, DLP, Insider Threat, Cloud Applications and firewalls, with threat intelligence that is shared and applied across all channels.

- Forcepoint's flexible packaging allows customers to purchase the product and features they need, and add more advanced capabilities over time as threats and needs evolve.

- Forcepoint's CASB product provides deep visibility into the usage of cloud applications like Office 365, Google G Suite, Salesforce and others.

- Context-aware DLP provides enterprise-class data theft protection across endpoints, Web and Email gateways, and both networked and cloud storage, protecting from insider theft and loss as well as against external threat actors. Advanced detection techniques, such as OCR (Optical Character Recognition), 'Drip-DLP', and encrypted payloads ensure effectiveness.

- Forcepoint partners with Lastline, a sandbox technology vendor, to provide its Forcepoint Advanced Malware Detection capability.

WEAKNESSES

- Forcepoint needs to continue to innovate with advanced protection for malware attacks and data theft aimed at roaming endpoints.

- Forcepoint needs to integrate the Forcepoint Insider Threat and Forcepoint NGFW products with its Web Security and Email Security products, as well as with third-party solutions, as it builds out its next generation platform vision.

- Forcepoint provides quarantining and blocking of endpoints, but does not provide endpoint remediation.

- Forcepoint needs to provide predictive, actionable threat intelligence reporting across the entire threat lifecycle.

INTEL SECURITY (MCAFEE)

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

McAfee, now part of Intel Security, delivers security solutions and services for business organizations and consumers. The company provides security solutions, threat intelligence and services that protect endpoints, networks, servers, and more.

SOLUTIONS

McAfee Advanced Threat Defense enables organizations to detect advanced targeted attacks and convert threat information into immediate action and protection. Intel Security offers physical appliances, virtual appliances and a cloud-based service, which allows customers to deploy the advanced threat analysis capabilities that best fit their business and security requirements.

Unlike traditional sandboxing, Advanced Threat Defense includes static code analysis, which provides additional inspection capabilities that broaden detection and expose evasive threats. Tight integration between Intel Security solutions, from network to endpoint, enables instant sharing of threat information. Protection is enhanced as attempts to infiltrate the organization are blocked. Indicators of compromised data are used to find and correct threat infiltrations, helping organizations recover post-attack.

Advanced Threat Defense comprises the following characteristics:

- *Advanced analysis* – ensures that dynamic analysis through sandboxing, and static code analysis, together provide inspection and detection capabilities. Malicious activity is observed in the sandbox environment and simultaneously examined with in-depth static code analysis to broaden detection and identify evasive maneuvers.

- *Centralized deployment* – allows customers to leverage shared resources for malware analysis with a high performance architecture that scales with fewer appliances.

- *Security Connected* – an Intel Security-wide initiative, allows integrated solutions to move organizations from analysis and conviction to protection and resolution. At the data level, Advanced Threat Defense integrates with other solutions so that they can make immediate decisions about blocking traffic or executing an endpoint service, or whether an organized attack is taking place against targeted organization individuals.

Out-of-the-box, Advanced Threat Defense plugs in and integrates other McAfee solutions, including: Network Security Platform (IPS), Enterprise Security Manager (SIEM), ePolicy Orchestrator (ePO) and McAfee endpoint solutions, McAfee Active Response (EDR), Web Gateway, and McAfee Threat Intelligence Exchange. These integrations operate over the Data Exchange Layer (DXL), which serves as the information broker and middleware messaging layer for McAfee security products.

STRENGTHS

- Intel Security delivers deployment and purchasing flexibility by offering appliance, virtual appliance and cloud form factors with CapEx and OpEx purchase options.

- Combination of in-depth static code and dynamic analysis through sandboxing, provide strong analysis and detection capabilities.

- Report and outputs include sharing of IOC data that can be used to target investigations.

- Intel Security/McAfee offers complete protection across endpoints, desktop computers and servers.

- Additional detection engines, including signatures, reputation, and real-time emulation enhance analysis speed.

- Centralized analysis device acts as a shared resource between multiple Intel Security devices.

- Advanced Threat Defense handles encrypted traffic analysis, and in addition uses a proprietary technique which allows for the unpacking, unprotecting, and unencrypting of

samples so they can be analyzed.

- Tight integration between Advanced Threat Defense and all Intel Security solutions, directly or through the McAfee Data Exchange Layer (DXL), allows instant information sharing and action across the network when attacks are detected. Intel Security Innovation Alliance partners are also integrating to publish and subscribe to threat intelligence over DXL.

- Intel Security supports centralized, vector-agnostic deployments, where customers can purchase based on volume of files analyzed, regardless of originating vector (e.g. web, endpoint, or network).

- DLP technology is applied in-line to traffic by an integrated Web Gateway.

WEAKNESSES

- Intel Security no longer offers its own email gateways solution, however it is working to add support for integration with third party email solutions to provide email file attachment analysis.

- Mobile malware inspection is supported only for Android (.apk) applications.

- McAfee Advanced Threat Defense works best in the context of a full Intel Security deployment across computers, servers, and mobile devices.

- Management of Intel Security on-premises and cloud solutions currently relies on disparate interfaces. The vendor is working to address this through a unified management platform, which will work across both its cloud and on-premises solutions.

FIREEYE

1440 McCarthy Blvd.
Milpitas, CA 95035
www.fireeye.com

FireEye, founded in 2004, offers solutions to simplify, integrate and automate an organization’s security operations. The company's solutions consist of network security, web security, email

security, file security, and malware analysis. In addition, the company offers deep security forensics products. In 2014, FireEye acquired Mandiant, a provider of endpoint security and professional services. Also in 2014, FireEye acquired nPulse Technologies, a provider of rich network forensics solutions. In January 2016, it acquired iSIGHT Partners, a provider of cyber threat intelligence for global enterprises. In February 2016, FireEye acquired Invotas, a provider of cross-product and cross-vendor security orchestration and automation solutions.

SOLUTIONS

FireEye's solutions portfolio comprises the following components:

- ***FireEye Helix*** – introduced in Q1 2017, merges capabilities from its own organic development as well as from its strategic acquisitions into a unified platform for network and endpoint security which can be delivered on-premises, in the cloud or as a hybrid deployment. It offers a unified user experience across the FireEye product portfolio. Organizations are also able to send event data from non-FireEye components of their IT and security infrastructure into FireEye Helix and overlay FireEye iSIGHT Intelligence on that data to triage any buried threats. Helix helps centralize security data across the infrastructure to detect lateral movement, data exfiltration, account abuse and user behavior anomalies.

- ***FireEye Network Security*** – helps organizations detect and block advanced, targeted and other evasive attacks hiding in Internet traffic. It uses a combination of multi-stage virtual execution, intelligence from FireEye as well as third parties, intrusion prevention, and callback analysis to detect and prevent commodity (e.g. adware, spyware) as well as evasive and destructive threats (e.g. drive-by-downloads, ransomware). It also packages contextual intelligence to enable the security teams to gain threat insights and accelerate response. FireEye Network Security offers several different deployment options including physical or virtual appliance, on-premises or private cloud-based.

- ***FireEye Endpoint Security*** – allows organizations to gain endpoint visibility for threat detection and response. It allows analysts to detect and correlate activities that indicate an exploit is in progress, inspect compromised endpoints and analyze gathered information to create custom IOCs and address previously unknown threats, as well as isolate compromised endpoints with a single click (whether the endpoints are on or off-premise).

- ***FireEye Email Security*** – offers a combination of intelligence-based analysis and virtual execution (detonation) to analyze suspicious email attachments and embedded URLs. It also provides anti-virus and anti-spam protection to protect against commodity malware. It is available as either an on-premises or a cloud-based solution.

- ***FireEye Content Se****curity* – enables scanning internal file shares for malicious content that may have been brought into the organization from outside sources, such as online file shares and portable file storage devices.

- ***FireEye Network Forensics & Investigation Analysis system*** – combines high performance network data capture and retrieval, with centralized analysis and visualization.

- ***FireEye Threat Analytics Platform*** – applies threat intelligence, expert rules and advanced security data analytics to noisy event data streams to reveal suspicious behavior patterns. It brings together enterprise-wide visibility with investigation workflows to aid security teams in prioritizing and optimizing their response efforts on critical alerts.

- ***FireEye Security Orchestrator*** – allows security teams to respond to threats by connecting disparate technologies and incident handling processes into a cohesive automated solution.

FireEye also leverages its Mandiant and iSIGHT acquisitions to offer customized subscriptions and professional services for threat intelligence, threat prevention, detection, analysis, and response. Lastly, FireEye as a Service offers a managed detection and response capability that packages various FireEye technologies along with expertise and intelligence.

STRENGTHS

- Protects against unknown, zero-day attacks through a signature-less engine, FireEye Multi-vector Virtual Execution (MVX), which executes suspicious binaries and Web objects against a range of browsers, plug-ins, applications, and operating environments. As the attack plays out, the FireEye MVX engine captures callback channels, dynamically creates blocking rules, and transmits the information back to FireEye Network, which enables to then protect other organizations.

- Protection across a broad attack surface: network, web, email, content, endpoint and mobile devices.

- FireEye offers a security orchestration solution that supports the integration of detection and analysis capabilities of FireEye and non-FireEye technology solutions, to reduce operational overhead and increase productivity.

- Dynamic threat intelligence sharing, which includes callback coordinates and communication characteristics, can be shared through the FireEye Dynamic Threat Intelligence (DTI) cloud to notify all subscribers of new threats.

- FireEye Network, Email, and Content are an easy-to-manage, clientless platform that deploys quickly and requires no tuning. It can be deployed out-of-band, for in-line monitoring, or as in-line active blocking.

- FireEye Network also supports integration with the active fail open switch to ensure no link downtime and drives availability for in-line hardware deployments in the event of power or link failures. It leverages heartbeat technology to monitor availability of the FireEye Network device and automatically switches to bypass in case of failure.

- FireEye Network with IPS consolidates advanced threat prevention with traditional security. It automates alert validation, reduces false alerts and helps detect hidden attacks.

- FireEye Helix offers a single integrated console to simplify and manage the entire security operations workflow by bringing together FireEye capabilities, third party technology, with intelligence and automation.

WEAKNESSES

- FireEye's APT solutions taken "a la carte" tend to be somewhat more expensive than competitors. However, FireEye's new Cloud MVX Essentials edition is attractively priced for midmarket and distributed enterprise customers.

- FireEye currently offers attack prevention and containment but not remediation. This is, however, on its future roadmap.

- FireEye has a comprehensive offering for APT protection. However, customers may find it difficult to understand how to put together an effective APT deployment, without significant

design support by the vendor. The newly released FireEye Helix, however, is aimed at easing customer complexity through a single integrated solution.

- FireEye does not offer a firewall solution, however, it leverages several capabilities, including URL analysis and Intrusion Prevention (IPS), to detect malicious intent.

- FireEye does not offer a mobile security solution. However, FireEye partners with several mobile device management providers to allow them to act on threats originating from mobile devices.

CISCO

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

Cisco is a leading vendor of Internet communication and security technology. In 2015, Cisco added to its security portfolio by acquiring OpenDNS, which offers cloud-delivered advanced threat protection solutions. Also in 2015, Cisco acquired Lancope, a company that provides network behavior analytics, network visibility, and security intelligence. In August 2016, Cisco acquired CASB technology firm, CloudLock. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), which is made up of leading threat researchers.

SOLUTIONS

Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-managed endpoint security solution designed to prevent cyber attacks, as well as to rapidly detect, contain, and remediate advanced threats if they get inside endpoints. Cisco AMP for Endpoints can be deployed to protect PCs, Macs, Linux, mobile devices and virtual systems. AMP for Endpoints uses global threat intelligence from Talos and AMP Threat Grid to strengthen defenses in order to prevent breaches before they occur. It also uses a telemetry model to take advantage of big data, continuous analysis, and advanced analytics.

AMP for Endpoints delivers the following functionality:

- *Prevention* – AMP for Endpoints combines Global Threat Intelligence, malware blocking, file sandboxing and offers proactive protection by closing attack pathways before they can be exploited.

- *Detection* – AMP for Endpoints continually monitors all activity on endpoints to identify malicious behavior, and detect indicators of compromise. Once a file lands on the endpoint, AMP for Endpoints continues to monitor and record all file activity. In addition, AMP detection gives visibility into what command line arguments are used to launch executables to determine if legitimate applications, including Window utilities, are being used for malicious purposes. If malicious behavior is detected, AMP can automatically block the file across all endpoints and show the security team the entire recorded history of the file's behavior. AMP for Endpoints delivers agentless detection, which serves to detect compromise even when a host does not have an agent installed. Using Cisco's Cognitive Threat Analytics (CTA) technology, AMP for Endpoints inspects web proxy logs to uncover issues such as memory-only malware and infections that may live in a web browser only.

- *Response* – AMP for Endpoints provides a suite of response capabilities to quickly contain and eliminate threats across all endpoints before damage is done. AMP for Endpoints offers surgical, automated remediation where once a threat is uncovered it is automatically remediated across all endpoints without the need to wait for a content update.

- *Malware protection* – is provided through a combination of file reputation, cloud-based sandboxing, and intelligence driven detection. Cisco's Talos Security Intelligence provides the ability to identify and filter/block traffic from known malicious IP addresses and sites, including spam, phishing, Bot, open relay, open proxy, Tor Exit Node, Global Blacklist IPs and Malware sites in addition to domains and categorized, risk-ranked URLs.

- *Email and Web security* – all file disposition and dynamic analysis information is shared across AMP products via collective intelligence. If a file is determined to be malicious via AMP for Email or Web Security that information is immediately shared across all AMP-enabled platforms, both for any future detection of the malicious file and retrospectively if the file was encountered by any of the other AMP platforms.

- *Firewall and NGIPS* – AMP for Endpoints integrates with AMP for Networks. All detection information is sent to the Firepower management platform and can be used to correlate against other network threat activity.

- *Patch Assessment* – AMP for Endpoints uses a feature called Vulnerable Software that identifies if installed software across all endpoints has an installed version with exploitable vulnerability.

- *Reporting* – AMP for Endpoints offers static, dynamic, and historical reports. These include reporting on high-risk computers, overall security health, threat root cause activity tracking, identification of various APTs, and mobile-specific root cause analysis.

- *Management* – AMP for Endpoints comes with its own management console and can also integrate with the Firepower console for tighter management across all deployed Cisco security solutions.

The **Cisco AnyConnect Secure Mobility Client** offers VPN access through Secure Sockets Layer (SSL), endpoint posture enforcement and integration with Cisco Web Security for comprehensive secure mobility. The latest version assists with the deployment of AMP for Endpoints and expands endpoint threat protection to VPN-enabled endpoints, as well as other Cisco AnyConnect services.

STRENGTHS

- Cisco offers a broad security portfolio, which encompasses threat intelligence, heuristics, behavioral analysis and sandboxing to predict and prevent threats from edge to endpoint.

- AMP tracks all file activity. With continuous monitoring, organizations can look back in time and trace processes, file activities, and communications to understand the full extent of an infection, establish root causes, and perform remediation.

- AMP has the ability to roll back time on attacks to detect, alert, and quarantine files that become malicious after the initial point of entry.

- AMP for Endpoints offers protection across PCs, Macs, mobile devices, Linux, virtual environments, as well as an on-premise private cloud option.

- Cisco AMP for Endpoints can be fully integrated with the Cisco AMP for Networks solution to further increase visibility and control across an organization. AMP capabilities can be added to Cisco Email and Web Security Appliances, Next-Generation Intrusion Prevention

Systems, Firewalls, Cisco Meraki MX, and Cisco Integrated Services Routers to offer faster, easier protection in more places across the organization.

WEAKNESSES

- Cisco AMP for Endpoints does not integrate with Active Directory or LDAP to help enforce user policies.

- Cisco needs to add sandbox support for iOS/macOS.

- Cisco does not offer Data Loss Prevention (DLP), customers who feel they require this functionality will have to secure it through an additional vendor.

TRAIL BLAZERS

KASPERSKY LAB

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

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

SOLUTIONS

The **Kaspersky Anti Targeted Attack Platform** includes different features focused on malware detection (both known, unknown and advanced malware). An Advanced Sandbox offers file behavior analysis and URL detonation, and is complemented with malware knowledge from the Kaspersky Security Network (KSN), which receives threat intelligence in real time from across the world, and allows Security Officers to distinguish targeted attacks from malware outbreaks.

The Kaspersky Anti Targeted Attack Platform uses an event-centric approach to deliver threat analysis results that correlate data from the Advanced Sandbox, anti-malware analysis, network monitoring with endpoint data collection and anomaly detection in an easy to use console that gives Security Officers a comprehensive picture of corporate IT network security incidents.

The platform provides the following functionality:

- Multiple sensors to detect activities at multiple areas of the customer's IT environment. This allows the Kaspersky Anti Targeted Attack Platform to achieve 'near real-time' detection of complex threats.

    - The Network Sensor is able to extract the information about source, destination, volume of the data and periodicity from the network traffic (including encrypted). This information is typically enough to make a decision about the level of suspicion of the traffic and to detect potential attacks. It supports SMTP, HTTP, FTP and DNS protocols.

    - The ICAP sensor connects to the proxy server and intercepts Web traffic through the ICAP protocol. The ICAP sensor can also have objects transmitted by HTTPS.

    - The Email Sensor supports integration with mail servers, via a POP3S and SMTP connection to the specified mailbox. The sensor can be configured to monitor any set of mailboxes.

- The Targeted Attack Analyzer receives network traffic metadata from both the Network Sensors and the Endpoint Sensors and plays a central role in achieving high-performance detection. It uses advanced, intelligent processing, plus machine learning techniques and Kaspersky Security Network cloud technologies to ensure it can rapidly detect abnormal behavior on the customer's network.

- To assist with incident response and post-attack investigations, detailed logs of alerts are recorded for analysis within the Kaspersky Anti Targeted Attack Platform, or the logs can be imported into the customer's SIEM (Security Information and Event Management) system.

- URL reputation analysis based on reputation data from the cloud-based, global Kaspersky Security Network helps detect suspicious or undesirable URLs. It also includes the

knowledge about URLs and domains, which are connected to the targeted attacks.

- The Kaspersky Anti Targeted Attack Platform includes industry-standard Intrusion Detection System (IDS) technology. By combining both traditional security and advanced threat detection, the platform helps to boost protection against sophisticated threats. The IDS rule sets are automatically updated.

- The Kaspersky Anti Targeted Attack Platform provides traffic analysis – across the entire customer corporate network. It offers a scalable architecture for sandboxes and sensors compatible with heterogeneous IT environments.

STRENGTHS

- The Kaspersky Anti Targeted Attack Platform provides advanced threat and targeted attack detection across all layers of a targeted attack – initial infection, command and control communications, and lateral movements and data exfiltration.

- Kaspersky offers a flexible implementation, with separate network sensors and compatible, optional lightweight endpoint sensors, as well as hardware-independent software appliances.

- The Kaspersky Security Network offers one of the largest threat intelligence databases, which gives an ability to check files, URLs, domains and behavior popularity and reputation in order to detect suspicions and reduce false alerts.

- Kaspersky Private Security Network (KPSN) also offers private threat intelligence database installation capabilities for isolated networks in support of regulatory compliance requirements.

- Kaspersky also offers targeted attack mitigation services, which include training, response, and discovery.

WEAKNESSES

- Kaspersky Lab's Anti Targeted Attack Platform is geared mainly for on-premises deployments.

- Kaspersky Lab's Anti Targeted Attack Platform does not yet integrate with Kaspersky Labs' Secure Web Gateway, however this is currently in development.

- Currently the Kaspersky Anti Targeted Attack Platform acts mainly as an expert system focused on attack detection. Automatic response is not yet available, but is on the roadmap.

- Mobile device protection is not yet available, but an EDR agent for mobile platforms is on the roadmap for a next release.

- Kaspersky Lab does not offer Data Loss Prevention (DLP), customers who feel they require this functionality need to secure it through an additional vendor.

- Kaspersky Anti Targeted Attack Platform does not decrypt SSL traffic, however this can be handled through integration with third party solutions.

WEBROOT, INC.

385 Interlocken Crescent, Suite 800
Broomfield, CO 80021
www.webroot.com

Webroot, founded in 1997, delivers next-generation endpoint security and threat intelligence services based on its cloud-based collective threat intelligence network.

SOLUTIONS

Webroot SecureAnywhere Business – Endpoint Protection is a real-time, cloud-based approach to preventing malware. It is compatible with Microsoft Windows PCs, Laptops and Servers, Mac OS and Google Android and Apple iOS devices. It is also deployed on Terminal Servers and Citrix; VMware; VDI; Virtual Servers and point of sale (POS) systems. SecureAnywhere's file pattern and predictive behavior recognition technology is designed to stop malware, including APT's and zero-day threats at the time of infection. Unlike conventional AV there are no definition or signature updates to deploy, and no management issues with ensuring that endpoints are properly updated.

Webroot's continuous endpoint monitoring agent ensures malware detection is in real-time and that every endpoint is always protected and up-to-date. The agent/cloud architecture eliminates device performance issues, allows for fast scheduled system scans, and ensures that device performance is not affected.

SecureAnywhere's architecture is also designed to coexist alongside existing AV with no immediate need to remove or replace because of software conflicts. SecureAnywhere also offers infection monitoring, journaling and rollback auto-remediation. If new or changed files and processes cannot be immediately categorized, then full monitoring and journaling is started. In this endpoint state the uncategorized files and processes are overseen and any permanent system damage averted until categorization is completed. If a threat is then determined to be malware, any system changes made are reversed and the endpoint auto-remediated to its last 'known good' state. This extra layer helps ensure minimal false positives, but if they occur administrators can easily override the Webroot categorization so business disruption is minimized. Webroot's approach to malware prevention offers visibility of endpoint infections through its dwell-time alerting reporting.

STRENGTHS

- The scanning, benchmarking and whitelisting of individual endpoint devices, coupled with continuous monitoring of each individual endpoint provides an individual/collective prevention approach that ensures malware identification and prevention is both individualized (to counter highly targeted attacks) and offers the benefits of collective prevention.

- The Webroot Threat Intelligence Platform uses machine learning, maximum entropy discrimination (MED) Big Data processing techniques, coupled with high computational scalability and actionable security intelligence to detect and prevent APTs in real-time.

- Individual endpoint infection visibility and information on endpoint infections is made available via dwell time alerts and reporting that allows administrators to easily understand and take action, if necessary.

- Webroot offers continuous monitoring, journaling, protection and auto-remediation, which means that as soon as files and processes are categorized as undetermined the endpoint system is protected from extensive damage until a good or bad determination can be made.

- Webroot's solution is affordably priced for small and medium sized customers.

WEAKNESSES

- Webroot focuses on advanced endpoint protection, but does not integrate with network, web or email security gateway solutions.

- While Webroot provides threat visibility and threat information it does not yet provide in-depth forensics information.

- Webroot needs to add interoperability with SIM's and SIEM's to allow internal audit, correlation and analyses of their endpoint data.

- Webroot does not provide direct integration with Active Directory services.

- Webroot does not offer Data Loss Prevention (DLP), customers who feel they require this functionality will need to secure it through a third-party vendor.

BARRACUDA NETWORKS

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

Founded in 2003, Barracuda is a provider of security and storage solutions that simplify IT for organizations of all sizes. Barracuda Networks is a publicly traded company.

SOLUTIONS

Barracuda **Advanced Threat Protection (ATP)** provides comprehensive real-time protection against known and unknown advanced threats. The service shares threat intelligence across all Barracuda security products ensuring networks, users, data, and web applications are dynamically protected from the evolving threat landscape.

Barracuda ATP is integrated into Barracuda NextGen Firewalls, Email Security Gateway, Essentials for Email Security, Essentials for Office 365, Web Security Gateway, and Web Application Firewall's in all deployment options (hardware, virtual appliances, SaaS, and Public Cloud). It provides the following features:

- *Full System Emulated Sandbox* – helps detect targeted and persistent attacks, as well as malware that was designed to evade detection by traditional sandboxes used by first generation advanced persistent threat solutions.

- *Link Protection* – evaluates and rewrites fraudulent URLs so that, when clicked, the user is safely redirected to a valid domain, or to a Barracuda domain warning of the fraud.

- *Email Threat Scanner* – Scans mailboxes for latent advanced threats and provides threat and risk exposure, attack trends, and remediation to remove identified threats.

- *Automatic User and IP Quarantine* – based on identified malware activities, allows infected users to be automatically blocked from the corporate network.

- *Spyware/Botnet Detection* – if malicious sites or domains are accessed by any protocol (not just HTTP or HTTPS), traffic is redirected to a fake IP address and access is monitored to identify infected clients.

- *Automatic Email Notifications* – in case malware activity has been identified, notifications minimize administrator reaction time in order to mitigate network breaches.

- *SSL Inspection* – integrated SSL Inspection files can be extracted and checked in order to detect advanced malware in an encrypted stream.

- *Intrusion Detection/Protection* – analyzes network traffic and continuously compares against an internal signature database to detect any malicious code patterns.

- *End-Point Security Extension* – is a browser extension that enables remote enforcement of web security policies. Can be used both on- and off-network.

STRENGTHS

- The Barracuda ATP infrastructure is integrated across all products, including: firewalls, email gateways, and web security gateways, in all form factors; and shares threat information in real time across the entire customer installed base.

- SSL/TLS encrypted traffic can be intercepted and decrypted to help detect malicious behavior.

- Barracuda security solutions provide DLP features using encryption and VPN tunnels (depending on whether it is email or network security) triggered by custom or pre-defined alpha-numeric patterns.

- All Barracuda Security Products using the Barracuda ATP service are fully user and group membership aware by integrating with all known widely used user authentication mechanisms, such as LDAP, Active Directory, Radius, RSA Secure ID, TACACS+, as well as Citrix and Microsoft Terminal Servers.

- Barracuda solutions are attractively priced to fit the needs of small and medium customers as well as large organizations.

WEAKNESSES

- Barracuda provides only basic DLP functionality customers with more advanced needs will need to add a third-party DLP solution.

- Barracuda ATP is focused on detection and prevention across its entire security portfolio, however, Barracuda's portfolio does not include endpoint protection.

- Customers of Barracuda's email solution, we spoke with, indicated some problems with email spoofing detection.

SPECIALISTS

FORTINET

899 Kifer Road
Sunnyvale, CA 94086
www.fortinet.com

Founded in 2000, Fortinet is a leading vendor of security and networking solutions. The company offers physical and virtual appliances, security subscription services and SaaS offerings aimed at the needs of carriers, data centers, enterprises, distributed offices, SMBs and MSSPs.

SOLUTIONS

Fortinet offers an integrated advanced threat protection (ATP) solution set, which includes technologies to prevent, detect and mitigate threats at network, application and endpoint layers. Fortinet's product portfolio includes:

- **FortiGate Next Generation Firewall** – consists of physical and virtual appliances that provide a broad array of security and networking functions, including firewall, VPN, anti-malware, intrusion prevention, application control, Web filtering, DLP, WAN acceleration, WLAN control and more.

- **FortiMail Secure Email Gateway** – provides a single solution to protect against inbound attacks, including advanced malware, as well as outbound threats and data loss. It includes: anti-spam, anti-phishing, anti-malware, sandboxing, data leakage prevention (DLP), identity based encryption (IBE), and message archiving.

- **FortiWeb Web Application Firewall** – protects web-based applications and internet-facing data from attack and data loss with bi-directional protection against malicious sources, application layer DoS Attacks, and sophisticated threats such as SQL injection and cross-site scripting.

- **FortiClient Endpoint Protection** – offers endpoint client protection for desktops, laptops, tablets and smartphones.

- **FortiSandbox** – provides deep analysis of at risk objects to discover new and unknown malware, malicious or compromised sites, command and control servers and more. It can set up a full virtual sandbox environment where it performs deep analysis of file behavior. To expedite discovery, FortiSandbox employs a multi-step approach to analyzing objects. Often file attributes (including evasion techniques) are identified in earlier steps and FortiSandbox can skip directly to reporting findings, speeding up the time to action. FortiSandbox delivers deep analysis of new threats, including their intended behavior and endpoints that may have been infected. Following analysis, FortiSandbox generates real-time local threat intelligence that is immediately available to integrated Fortinet ATP components for automated response as well as accessible via APIs as third party update packages. Integration between FortiSandbox and the flagship FortiGate enables administrators to quarantine infected endpoints with one click of a button, while integration with FortiMail and FortiClient give organizations the option to hold new objects for sandbox analysis and block previously unknown attacks.

New threat information uncovered by FortiSandbox can also be shared with and used by the **FortiGuard Labs** threat research team, to create new security updates to be sent to all Fortinet products.

Fortinet also integrates a range of Fabric-ready partners (with certified compatible solutions) into its Advanced Threat Protection solution and offers a range of services itself to help mitigate attacks including Resident Engineers, Premier Signature Services and more.

STRENGTHS

- Effective threat prevention validated through independent testing with NSS Labs, Virus Bulletin, ICSA Labs, and AV Comparatives for anti-malware, IPS, anti-phishing, anti-spam, NGFW, and sandboxing.

- Fortinet offers a broad portfolio to facilitate a coordinated and effective approach to advanced threat protection, but also enjoys a broad set of Technology Partners with certified integrations.

- Fortinet offers both stand-alone and integrated approaches to sandboxing, integrated at all common entry points and available in all form factors making it easy to deploy and

affordable in most use cases.

- Custom Security Processors and hardware to deliver high performance, thus enabling more security to be deployed at each inspection point.

- All Fortinet products are all developed in-house (without relying on OEM solutions), which allows the vendor to deliver solutions that offer broad threat insight and seamless operation across all products.

WEAKNESSES

- Fortinet only supports firewall-based capabilities to set/manage mobile device policies in support of BYOD, however customers will have to add full MDM or EMM capabilities from a third party vendor. Fortinet works with a number of certified Fabric-ready partners that offer this capability.

- Support for custom images in the sandbox requires professional services.

- Fortinet's depth of forensic packet capture/replay is currently somewhat limited and may need to be supplemented with an integrated offering from a Fabric-ready partner.

- Customers we spoke with, indicated that FortiAnalyzer reporting and report customization could be improved.

BAE SYSTEMS APPLIED INTELLIGENCE

265 Franklin Street
Boston, MA 02110
www.baesystems.com/businessdefense

BAE Systems provides on-premises and managed threat analytics as well as cloud-based messaging, compliance, and cyber security services to governments and businesses of all sizes on a software-as-a-service (SaaS) platform. The BAE Systems Email Protection Services platform delivers a fully integrated suite of email security solutions, including: Zero Day Prevention, Insider Threat Prevention, Email Data Loss Prevention (DLP), Email Security

(AV/AS), Email Encryption, Email Compliance Archiving, Email Continuity, and more.

SOLUTIONS

The BAE Systems **Advanced Persistent Threat Portfolio** consists of the cloud-based Zero Day Prevention solution and the Threat Analytics platform. The two services combine comprehensive threat analytics to help manage threat intelligence, detect and investigate unknown cyber threats, and detect and defend against advanced persistent threats (APTs), targeted attacks, and zero-day exploits.

- **Zero Day Prevention –** is a cloud-based solution that provides static and dynamic analysis to catch zero-day malware that traditional sandbox scanning may miss by analyzing email in the cloud for malicious content, before it reaches the recipient. Zero Day Prevention also includes a click time protection component with immediate detect and block capabilities for protection against malicious links, and is deployed directly in-line with mail flow, which provides a real-time view into the app and produces faster, more accurate results than traditional out-of-band sandboxing. Zero Day Prevention includes the following capabilities:

    - Protection against unknown malware in spear phishing attacks, advanced persistent threats, and zero-day exploits.

    - Protection for all third-party cloud and on-premises email, including Google and Office 365.

    - Performs granular analysis within the browser process to detect and defeat environment-aware malware before it can deploy and evade detection.

- **Threat Analytics** – provides a set of ingest, analysis/detection, prioritization and investigation capabilities to detect advanced attacks. It can be delivered as a managed service or as an on premises implementation and includes:

    - *Data Storage and Querying Platform* – A solution that allows months of high-resolution metadata to be collected and queried at high speed.

    - *Threat Intelligence Manager* – A tool that enables analysts to collect and collate

contemporary threat intelligence, and use it to distil actionable insight that can be used to identify impending threats and focus resources.

- *Threat Detection* – A system for regular, large scale processing of data through a combination of statistical and probabilistic algorithms, that can be rapidly developed as new threats evolve, with the output prioritized and presented to the analyst alongside any information that may be needed to interpret and understand a threat.

- *Alert/Incident Investigation* – A capability that automatically enriches the data with other information that could be relevant, which allows analysts to visualize linkages between disparate data elements and historical investigations. It allows indicators of compromise to be detected quickly and fed into security devices to enable rapid mitigation of cyber risks.

STRENGTHS

- BAE Systems offers a full suite of cloud-based email security solutions that defend against known and unknown malware, phishing-style emails, spam, viruses, zero-hour threats, and malicious email attachments before they reach a customer network.

- Email Protection Services from BAE Systems are fully integrated and easily controlled with BAE's web-based Security Management Console to provide organizations with security and control over inbound and outbound corporate messaging.

- BAE Systems Threat Analytics provides data ingestion, analysis, prioritization and in-depth investigation in one solution. This allows analysts to quickly uncover the full extent of attacks and plan complete remediation

- Threat Intelligence Management capabilities aggregate, organize, and enrich large amounts of threat intelligence from multiple sources to provide insight into likely or actual attacks, as well as help improve security planning.

- Email Protection Services from BAE Systems supports all third-party email including Google G Suite and Microsoft Office 365.

- BAE Systems offers a wide range of security and compliance services including threat

analytics, web security, vulnerability management, log management, event monitoring and response, as well as UTM management.

WEAKNESSES

- BAE's Mobile Device Management's management interface is not unified with the security management console for its other cloud services.

- BAE's Threat Analytics solution currently cannot analyze the contents of encrypted network traffic.

- BAE's Zero Day Prevention does not integrate with directory services (e.g. Active Directory or LDAP).

- BAE's Zero Day Prevention provides response capabilities but the Threat Analytics solution focuses more on detection, prevention and remediation recommendations than the actual remediation actions. Full incident response is available as a separate service.

- BAE does not offer its own mobile device security capabilities, but partners with AirWatch for MDM and EMM.

SOPHOS, LTD.

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

Sophos provides IT and data security solutions for businesses on a worldwide basis. SophosLabs is the R&D division behind the vendor's advanced security and malware research. Sophos provides synchronized security solutions, that include endpoint and mobile security, enterprise mobility management, encryption, server protection, secure email and web gateways, next-generation firewall and unified threat management (UTM).

SOLUTIONS

Sophos offers a set of complementary solutions for APT, which comprise: **Sophos SG UTM & XG Firewall,** for network protection, **Sophos Endpoint Protection** for workstations and mobile devices, and **Sophos Labs** which provides unified threat intelligence across all platforms. Sophos also offers **Intercept X**, a signature-less next generation endpoint protection product (EDR) which has been integrated into the existing endpoint protection solution. Sophos Intercept X can also be deployed alongside competing AV products.

Sophos SG UTM - is an integrated network security system that combines a next-gen firewall and IPS with web, email, remote access, and wireless security functionality. It includes Advanced Threat Protection through:

- *Sandboxing* – which analyzes and "detonates" suspicious content in a safe, cloud-based environment to identify and block previously unseen threats.

- *Suspicious traffic detection* – which identifies when an endpoint is trying to communicate with a malicious server. Once detected, the UTM blocks the traffic and notifies the administrator. This lets organizations detect the presence of compromised endpoints and prevent attacks from spreading, ex-filtrating data, or receiving commands.

Sophos Endpoint Protection – is a suite of endpoint security solutions designed to prevent, detect, and remediate threats. It is available as a cloud-managed SaaS offering or on-premises solution. It helps administrators reduce the attack surface through features such as application control, device control, and web filtering. It uses an integrated system of security technologies that correlates application behavior, website reputation, file characteristics, network activity (including Malicious Traffic Detection), and more to identify and block exploits and previously unseen malware. It is controlled by the Sophos System Protection (SSP), which automatically applies the correct protection mechanisms based on the threat. Cleanup and quarantine capabilities neutralize detected threats and help return users' systems to a clean state.

Sophos Labs – is the company's global research network, which collects, correlates, and analyzes endpoint, network, server, email, web, and mobile threat data across Sophos's entire customer base. It simplifies configuration by feeding advanced threat intelligence directly into Sophos products in the form of preconfigured settings and rules. This allows systems to be

deployed quickly without the need for dedicated, trained security staff to update and test the configuration over time.

In 2015, Sophos introduced its new Sophos Firewall-OS (SF-OS) that runs on SG Series appliances and includes new synchronized security technology, which integrates endpoint and network security for protection against advanced threats. For instance, SF-OS Sophos SG Series Appliances can link the next-generation firewall with Sophos Endpoint Protection through its Security Heartbeat synchronized security technology which enables the network and endpoint to correlate health, threat, and security indicators for prevention, detection, actionable alerting, and remediation. This provides automated incident response that can restrict network access to endpoints on which malware has been detected, or that have had their endpoint agent disabled. It also extends UTM Advanced Threat Protection so that when it sees malicious traffic from an endpoint, it can engage Endpoint Protection to verify and clean up the infection. The SF-OS comes preinstalled on Sophos XG Firewall Series appliances.

STRENGTHS

- Sophos synchronized security integrates Endpoint and Network security for protection against APTs through automation of threat discovery, investigation, and response.

- Sophos APT solutions emphasize simplicity of configuration, deployment, and management to minimize the time and expertise required to use the solutions.

- Sophos solutions can remove malware from compromised endpoints, where other vendors may only issue an alert or temporarily block malicious code.

- Sophos offers real-time threat intelligence between the Sophos UTM and Sophos Endpoint Protection solutions for faster, more cohesive APT protection.

- Sophos recently launched Sophos Sandstorm a cloud-based sandbox for the detonation of suspect files to confirm malicious activity in the controlled environment. Sophos Sandstorm integrates with the UTM/Firewall/Email and Web solutions.

- Sophos offers a full-featured EMM solution for iOS, Android, and Windows Phone, along with integrated threat protection for Android. Sophos Mobile Control and Sophos UTM

combine to provide stronger security.

- Sophos UTM and endpoint protection solutions are attractively priced for the mid-market.

WEAKNESSES

- Sophos's synchronized security and Intercept X solutions are still relatively new to the market, and will need more time to grow to maturity through more extensive real-life customer deployment.

- While Sophos APT solutions' forensic analysis capabilities are used within the product for automated detection and remediation, not all the information is exposed to administrators.

- In pursuit of simplicity, Sophos solutions sometimes favor features and rule sets that are configured automatically by Sophos Labs, over providing administrators with granular, do-it-yourself controls.

- Currently, Sophos' application whitelisting is limited to servers; the company does, however, offer category-based application control for workstations.

PALO ALTO NETWORKS

4401 Great America Parkway
Santa Clara, CA 95054
www.paloaltonetworks.com

Palo Alto Networks, founded in 2005, is well known for its next-generation firewall solutions. The company covers a wide range of network security functions, including advanced threat protection, firewall, IDS/IPS, and URL filtering.

SOLUTIONS

WildFire is Palo Alto Networks' APT solution. It can be deployed on any Palo Alto Networks security platform, or as a private cloud option where all analysis and data remain on the local network. WildFire provides complete visibility into all traffic, including advanced threats, across

nearly 400 applications, including Web traffic, email protocols (SMTP, IMAP, POP), and FTP, regardless of ports or encryption (SSL).

Wildfire offers native integration with the Palo Alto Networks Enterprise Security Platform, a service which brings advanced threat detection and prevention to all security platforms deployed throughout the network, automatically sharing protections with all WildFire subscribers globally in about 15 minutes. The service offers:

- A unified, hybrid cloud architecture, either deployed through the public cloud, or via private cloud appliance that maintains all data on the local network.
- Dynamic analysis of suspicious content in a cloud-based virtual environment to discover unknown threats.
- Automatic creation and enforcement of best-in-class content-based malware protections.
- Link detection in email, proactively blocking access to malicious websites.

STRENGTHS

- Palo Alto Networks is well known innovator in network security, the company is one of the early developers of APT technology.
- Wildfire is available in a variety of form factors including on-premises, or as a private cloud solution.
- Wildfire integrates across Palo Alto Networks' entire product portfolio to offer rapid, up to date threat intelligence.

WEAKNESSES

- Palo Alto Networks focuses on next generation firewalls and network security, this means its APT protection tends to be aimed mainly at the network layer rather than at applications.

- Palo Alto Networks focuses on detection and prevention, but does not offer incident remediation (IR) capabilities.

- Palo Alto Networks solutions are somewhat costly when compared with other vendors in this space.

- While Palo Alto Networks provides strong real-time analysis, forensics and static analysis could be improved to ease investigations and reporting.

- Palo Alto Networks does not offer DLP functionality, customers with a need for this functionality will need to look for third party solutions.

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

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

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

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

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim. The Radicati Group, Inc. was founded in 1993.

Consulting Services:

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

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

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

MARKET RESEARCH PUBLICATIONS

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

Currently Released:

Title	Released	Price*
Social Networking Statistics Report, 2017-2021	Feb. 2017	$3,000.00
Instant Messaging Market, 2017-2021	Feb. 2017	$3,000.00
Email Statistics Report, 2017-2021	Feb. 2017	$3,000.00
Endpoint Security Market, 2016-2020	Dec. 2016	$3,000.00
Secure Email Gateway Market, 2016-2020	Dec. 2016	$3,000.00
Microsoft SharePoint Market Analysis, 2016-2020	Jul. 2016	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2016-2020	Jul. 2016	$3,000.00
Email Market, 2016-2020	Jun. 2016	$3,000.00
Cloud Business Email Market, 2016-2020	Jun. 2016	$3,000.00
Corporate Web Security Market, 2016-2020	May 2016	$3,000.00
Advanced Threat Protection Market, 2016-2020	Mar. 2016	$3,000.00
Enterprise Mobility Management Market, 2016-2020	Mar. 2016	$3,000.00
Information Archiving Market, 2016-2020	Mar. 2016	$3,000.00
US Email Statistics Report, 2016-2020	Mar. 2016	$3,000.00
Mobile Growth Forecast, 2016-2020	Jan. 2016	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Enterprise Mobility Management Market, 2017-2021	Apr. 2017	$3,000.00
Advanced Threat Protection Market, 2017-2021	Apr. 2017	$3,000.00

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

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