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

THE RADICATI GROUP, INC.

Advanced Persistent Threat (APT) Protection - Market Quadrant 2016

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

April 2016

· Radicati Market Quadrant^{SM} 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^{SM} 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^{SM} 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.

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 a niche product.

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

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

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

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

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

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

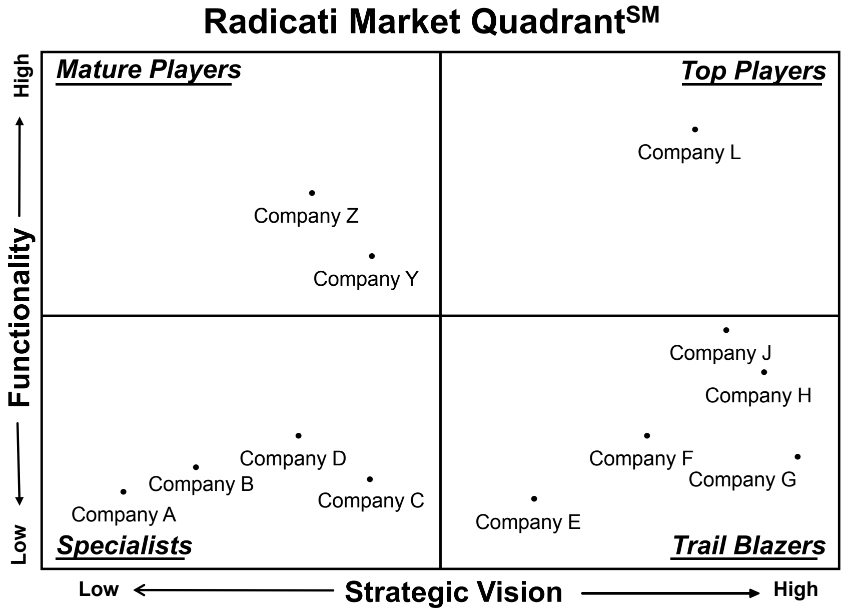

Figure 1: Sample Radicati Market Quadrant

MARKET SEGMENTATION – 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 Applied Intelligence, Barracuda Networks, Blue Coat Systems, Cisco, FireEye, Forcepoint, Fortinet, Intel Security, Kaspersky Lab, Palo Alto Networks, Sophos, 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 $2.6 billion in 2016, to over $7.3 billion by 2020.

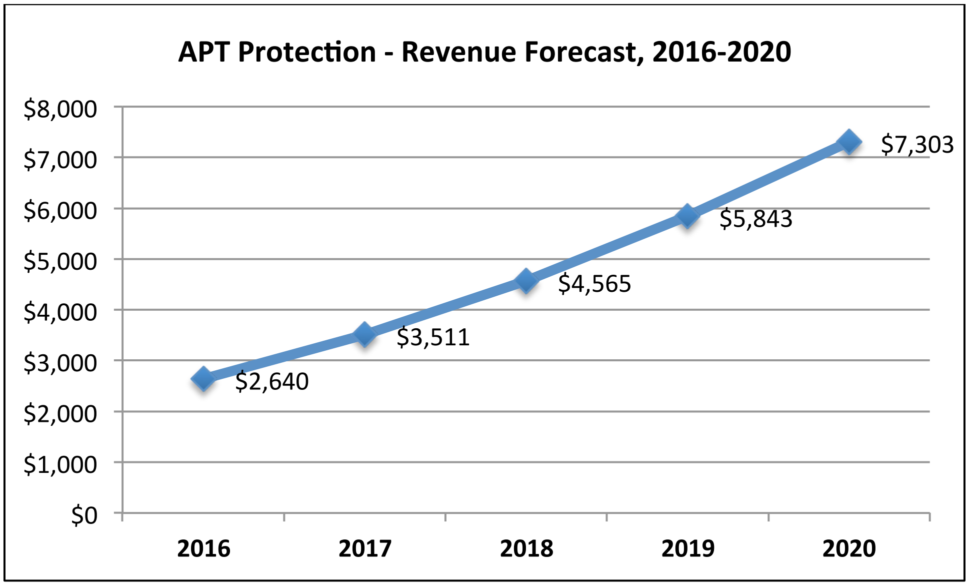

Figure 2: APT Protection Market Revenue Forecast, 2016 – 2020

EVALUATION CRITERIA

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

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

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

Vendors in the *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 that 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

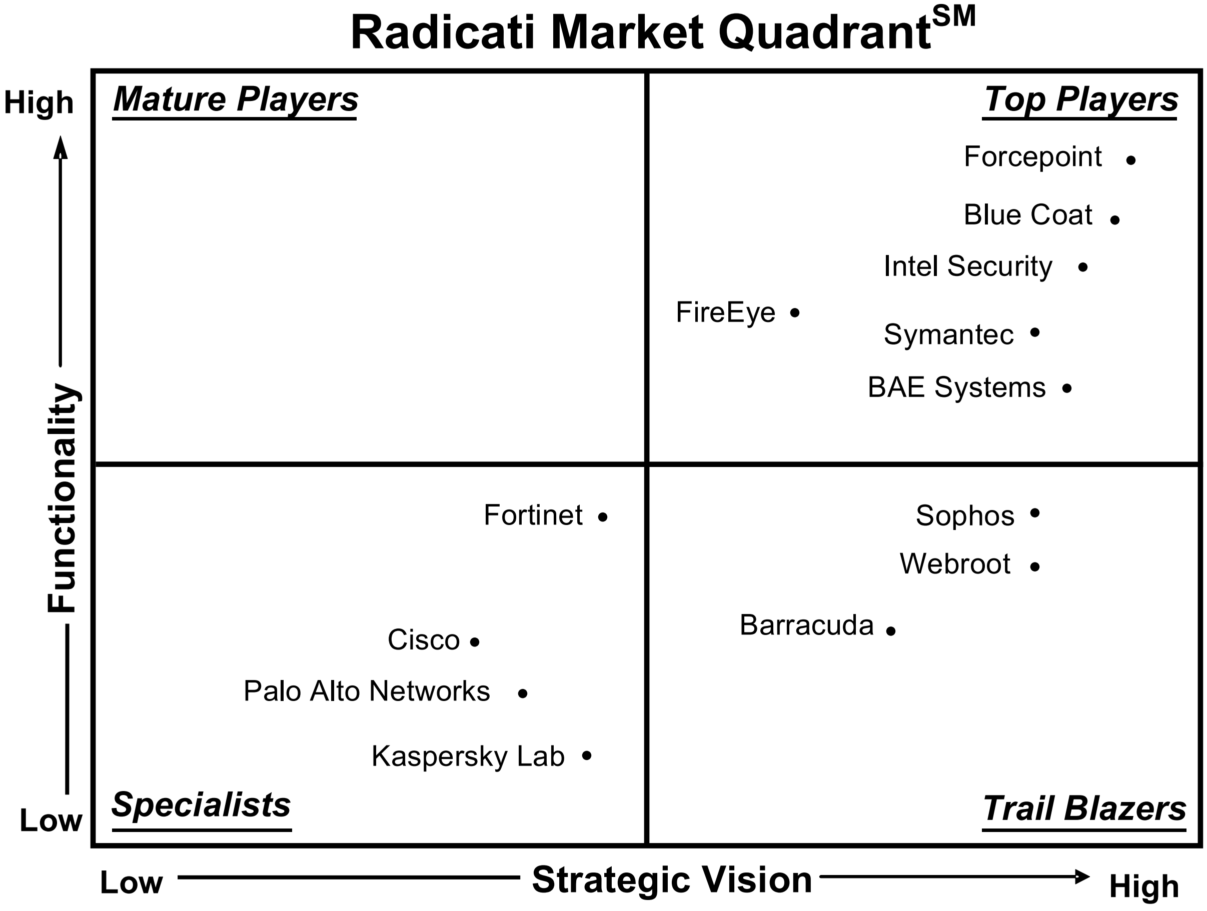

Figure 3: APT Protection Market Quadrant, 2016

· Radicati Market Quadrant^{SM} 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^{SM} 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^{SM} 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 *Forcepoint, Blue Coat, Intel Security, FireEye, Symantec,* and *BAE Systems***.**

- The **Trail Blazers** quadrant includes *Sophos*, *Webroot,* and *Barracuda Networks*.

- The **Specialists** quadrant includes *Fortinet, Cisco, Palo Alto Networks,* and *Kaspersky Lab*.

- There are no **Mature Players** in this market at this time.

APT PROTECTION - VENDOR ANALYSIS

TOP PLAYERS

FORCEPOINT

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

Forcepoint was formed in 2015 through the merger of Websense and Raytheon Cyber Products. In 2016, Forcepoint acquired the Stonesoft NGFW and Sidewinder firewall assets from Intel Security. Forcepoint focuses on delivering transformative technologies – cloud, mobility, Internet of Things (IoT), and others – through a unified, cloud-centric platform designed to safeguard users, networks and data.

SOLUTIONS

Forcepoint's **TRITON APX Suite** is an integrated Web, email and DLP gateway security solution for distributed organizations looking to stop advanced threats across multiple channels and prevent data theft. The integrated TRITON platform, offers a unified management console, reporting, and flexible deployment options allowing organizations to offer anywhere protection – in the office, cloud, or on the road. Key aspects of the solution include:

- **The TRITON architecture** – unifies web, email and data security, reducing the time and effort required to create and manage polices, monitor and assess threats, deliver key reports, or perform in-depth forensic investigations.

- **Threat Protection** – solutions provide dynamic behavioral analysis for the most advanced, targeted zero-day threats and advanced persistent threats (APTs) that may attack through web or email channels.

- **Forcepoint's ThreatSeeker Intelligence Cloud** – collects up to 5 billion potential indicators of emerging threat activity per day from over 155 countries, providing updates at an average rate of 3.2 per second.

- **Effective security for Office 365 and other cloud apps** – with inbound and outbound defenses to protect users and data on and off the network.

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

- **Multiple Deployment Options** – Forcepoint supports cloud deployments, but also provides on-premise, or hybrid options with the same TRITON unified protection and management capabilities.

The basic TRITON APX Suite includes:

- *TRITON AP-WEB* – Web gateway proxy available for on-premise, cloud-based, or hybrid deployment modes.

- *TRITON AP-EMAIL* – Secure email gateway with integrated DLP protection available in the cloud, on-premise, virtual appliance, or in a hybrid on-premise with cloud pre-filtering modes.

- *TRITON AP-DATA* – Content-aware data loss prevention solution to discover and secure an organization's sensitive information and prevent data theft.

- *TRITON AP-ENDPOINT* – Protects roaming users against data theft and retains control of sensitive information on Mac and Windows endpoint systems, both on and off the network.

To obtain the full data theft prevention capabilities, Forcepoint offers the following advanced modules that can be added to the core TRITON APX solutions for Web, Email, Data and Endpoint products described above:

- *Threat Protection Cloud Module* – Forcepoint Threat Protection Cloud is a scalable, easy-to-deploy sandbox solution that integrates with TRITON AP-WEB and TRITON AP-EMAIL. It provides:

  - File sandboxing for AP-WEB – monitors Web traffic for real-time code analysis in a behavioral sandbox for advanced threat identification.

  - File sandboxing for AP-EMAIL – intercepts attachments in real time for additional threat analysis in a behavioral sandbox to identify targeted attacks.

  - Email URL sandboxing – reassesses suspicious links in email when they are accessed, not only when the email arrives.

  - Detailed forensic reporting – uses sandbox results to guide any necessary response or proactive measures against future attacks.

  - Phishing education and reporting – helps increase phishing awareness at both the user and network levels to improve user behavior.

- *Email Encryption Module* – is a policy-driven technology that enables secure delivery of email communications. It offers easy administration without complex key management or additional hardware.

- *Image Analysis Module* – provides illicit image detection capabilities to help employers monitor images distributed through email, educate staff and enforce the organization's policies.

- *TRITON AP-MOBILE* – protects iOS & Android device users against mobile malware, malicious apps, SMS spoofing, phishing, web threats and data loss. MDM features are provided through integration with VMware AirWatch.

STRENGTHS

- Forcepoint offers Unified Web, Email, Data and Endpoint security. Threat Intelligence is shared and applied across all channels, for inbound and outbound traffic, to stop attacks before they complete their life cycle.

- The unified TRITON architecture offers a single management console which facilitates the management of a sophisticated end-to-end security solution across an enterprise regardless of how customers choose to deploy protection; on-premises, in the cloud or hybrid.

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

- Contextually 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.

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 SureView and Stonesoft products with Triton, 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.

BLUE COAT SYSTEMS

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

Blue Coat is a provider of enterprise security technology, providing on-premises, hybrid and cloud-based solutions for protecting web connectivity, combating advanced threats and resolving security breaches.

SOLUTIONS

Blue Coat Advanced Threat Protection safeguards against advanced persistent threats and targeted attacks, detecting both known and unknown malware and automating the containment and resolution of incidents that have occurred in on-premise and hosted environments. Blue Coat's solution comprises the following components:

- *Blue Coat ProxySG appliance, Secure Web Gateway Virtual Appliance, or Cloud Service* — block in real-time known threats, malicious sources, and malnets (malware delivery networks) at the gateway. *Blue Coat Content Analysis* integrates with the ProxySG appliance to orchestrate malware scanning and application whitelisting, while *Blue Coat SSL Visibility* gives visibility into threats hiding in encrypted traffic.

- *Blue Coat Advanced Threat Protection* — analyzes and mitigates unknown malware using Blue Coat Content Analysis that automatically brokers suspicious content to *Blue Coat Malware Analysis* for sandboxing. As the behaviors and characteristics of an unknown threat are learned through automated analysis, intelligence is shared across the security infrastructure, enhancing protection at the gateway for scalable defense.

- *Blue Coat Security Analytics* — utilizes high-speed full-packet capture, indexing, DPI and anomaly detection to enable incident response and to eradicate threats that have penetrated the network. Intelligence of a new known threat is used to investigate and remediate the full scope of the attack, including other instances of malicious files and threats already on the network. Intelligence is shared across the *Blue Coat Global Intelligence Network* to automate detection and protection against the newly identified threats, allowing all Blue Coat customers to benefit.

STRENGTHS

- Blue Coat offers policy-based encrypted traffic management for both inbound and outbound traffic to uncover encrypted APTs.

- Blue Coat provides extensive filtering and blocking of all known threats using whitelists, blacklists and anti-malware scanning through a hybrid, on-premises and cloud based solution.

- Next-generation sandboxing uses dual detection via emulation and virtual sandbox techniques, enabling users to customize their sandbox in order to replicate production images as needed.

- Blue Coat offers an integrated, easy to use incident response and advanced forensics capability to fully resolve APTs.

- The Blue Coat Global Intelligence Network powers all the products in the solution with the latest threat information.

WEAKNESSES

- Blue Coat's APT solution is aimed primarily at the needs of medium and large enterprises. Small business (SMB) may not have the needed budget to fully deploy all the components of Blue Coat APT solution.

- Blue Coat focuses on detection and prevention, but leverages partnerships to integrate with incident remediation and orchestration capabilities.

- Blue Coat does not offer firewall protection, but relies on its Web Security solution for url filtering.

- Blue Coat is best known for its Web Security and cloud solutions and is now raising visibility for its APT solution.

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. Advanced Threat Defense is currently available as an appliance, where two models are offered that can be clustered as needed to meet scalability requirements. Intel Security plans to expand its solution to offer different form factors, including virtualized appliance and cloud, by the end of 2016. 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 or not 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

- 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.

- 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.

WEAKNESSES

- McAfee's Advanced Threat Defense is currently available only as a hardware appliance. Intel Security is working to expand its offering to include virtualized appliances, cloud and hybrid solutions in the 2016 timeframe.

- Intel Security has retired its McAfee Enterprise Mobility Management (EMM) solution and is in the process of re-defining its mobile protection strategy through partnerships with leading EMM vendors.

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

- Intel Security solutions can be somewhat pricier than offerings from competing vendors, but do offer more feature and functionality.

FIREEYE

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

FireEye, founded in 2004, offers automated threat forensics and dynamic malware protection against APT and spear phishing. The company's solutions consist of network security, web security, email security, file security, mobile security, malware analysis. In addition, the company offers deep security forensics products. In 2013, FireEye acquired Mandiant, a provider of endpoint security and professional services. 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 solutions.

SOLUTIONS

The FireEye Platform is built on three critical components – technology, intelligence, and expertise. It comprises the following:

- *FireEye Network Threat Prevention Platform (NX Series)* - identifies and blocks zero-day Web exploits, droppers (binaries), and multi-protocol callbacks to help organizations deploy advanced network-based threat defenses. It can be deployed in-line or in monitor-only mode at Internet egress points to detect and block Web exploits and outbound multi-protocol callbacks. Additionally, FireEye Network also detects and blocks ransomware (e.g. adware, spyware).

- *Intrusion Prevention System (IPS)* – technology designed to block well-known network-based threats using traditional IPS signatures. It also validates the IPS alerts with the FireEye MVX engine to help drive down false alerts.

- *FireEye Multi-vector Virtual Execution™ (MVX) engine* – is the core FireEye threat detection technology, which is used by FireEye products (Network, Email, etc.) to identify zero-day and targeted threats, create real-time threat intelligence, and capture dynamic callback destinations.

- *FireEye Email Security products (EX and ETP)* – protect against cyber attacks, by detonating and analyzing suspicious email attachments and embedded URLs. FireEye also provides anti-virus and anti-spam protection through Email Threat Prevention (ETP) in the cloud.

- *FireEye Network Forensics Platform (PX series) & Investigation Analysis system (IA series)* – pair network data capture and retrieval, with centralized analysis and visualization.

- *FireEye Endpoint Threat Prevention (HX series)* – provide organizations with the ability to continuously monitor endpoints for advanced malware and indicators of compromise.

- *FireEye Mobile Security (Mobile Threat Prevention)* – detects and prevents mobile threats and provides visibility into mobile device security trends across the enterprise. It also integrates with third party mobile device management (MDM) providers.

- *File content security (FX Series)* – products scan 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.

- *Threat Analytics Platform (TAP)* - applies threat intelligence, expert rules and advanced security data analytics to noisy event data streams from different technologies (such as IPS, FW, AV, security gateways, and others) to reveal suspicious behavior patterns and generate alerts when necessary. This allows security teams can prioritize among thousands of alerts and optimize their response efforts.

- *Invotas Security Orchestrator (Invotas)* – allows security teams to respond to threats with a high degree of automation by connecting hardware, software, tools and policies into a cohesive solution.

FireEye also leverages its Mandiant and iSIGHT acquisitions to offer customized subscriptions and professional services for threat prevention, detection, analysis, and response. Further, 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 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.

- Security orchestration solution (Invotas) that allows the automation and 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.

WEAKNESSES

- FireEye's APT solutions are somewhat more expensive than competitors. The vendor's Essentials edition is a less expensive offering for customers that are early in their security maturity.

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

- FireEye currently lacks preventative capabilities for its endpoint/HX product. However, the vendor has announced that it will address this in future releases.

- 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.

SYMANTEC

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

Founded in 1982, Symantec has grown to be the largest security company with more than 11,000 employees in more than 35 countries. In 2015, Symantec completed its split into two independent public traded companies, Symantec focused on security, and Veritas focused on information management. Symantec's security solutions are powered by the *Symantec Global Intelligence Network*, which offers threat intelligence through real-time updates.

SOLUTIONS

Symantec Advanced Threat Protection is a solution platform that incorporates three modules: Endpoint, Email, and Network. 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 is also working to develop a fully cloud-based ATP solution. The solution platform provides a single pane of glass across all three modules, providing visibility into attacks in real-time, as well as the ability to orchestrate remediation of threats across control points. The platform includes Synapse, a feature that provides correlation for events across control points, making it easier for security teams to prioritize the incidents exposed by the systems.

Symantec Advanced Threat Protection: Endpoint - enables endpoint detection and response capabilities for clients, without the need to deploy a separate endpoint agent. ATP integrates directly with the SEP client to collect telemetry from the endpoints. This telemetry enables lightning fast searches for Indicators of Compromise (IOCs). The telemetry is also fed into machine learning algorithms to identify suspicious files in the organization, and compared against Symantec's global intelligence network. Suspicious files can be collected and sent for analysis to Symantec Cynic, a cloud-based malware analysis platform. ATP also integrates with the SEP Manager, to deploy ATP policies to endpoints to block zero-day and targeted attacks.

Symantec Advanced Threat Protection: Email - is an add-on service available to customers of Symantec Email Security.cloud. It combines traditional layers of security with targeted attack reporting and the advanced threat detection capabilities of Symantec Cynic.

Symantec Advanced Threat Protection: Network - provides automated threat prevention and detection at the network, by combining several Symantec threat prevention technologies with the detection capabilities of Symantec Cynic. It examines traffic across all ports and protocols to discover threats, identify infected clients, and extract potentially malicious payloads from the network stream.

Symantec Cynic, used by all three ATP modules, applies four different analysis techniques to each sample in order to provide detection. In addition to virtual execution, Cynic includes bare-metal execution, to uncover threats that may evade VM analysis. Cynic also uses static and dynamic code analysis to identify threats that are undetected by sandboxes. These results are enriched with data from Symantec's global intelligence network to provide a complete picture for any incident.

STRENGTHS

- Symantec offers a fully integrated solution platform across endpoint, email and network threat surfaces.

- Symantec ATP is a hybrid solution, designed to deliver protection with a low cost of ownership.

- Symantec ATP Endpoint leverages the existing SEP client, so customers who already have SEP do not need to deploy any additional agent software.

- The Symantec ATP leverages multiple technologies and resources (i.e. *Symantec Global Intelligence Network, Synapse, Cynic*) to deliver a comprehensive, well-integrated platform that addresses the evolving threat landscape.

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

- Symantec solutions are available on a global basis with broad language support.

WEAKNESSES

- Symantec ATP does not currently integrate with Directory services, however integration with Active Directory is on the roadmap for 2016.

- DLP is not included with Symantec ATP. However, Symantec offers DLP as a separate add-on product.

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

- Symantec ATP does not include internal environment threat analysis.

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

BAE SYSTEMS APPLIED INTELLIGENCE

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

BAE Systems (including the former SilverSky) provides on-premise 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.

SOLUTION

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-premise 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 premise 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 and Office 365 mailboxes.

- 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 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.

TRAIL BLAZERS

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 work together to provide better protection, such as 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 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-premise 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 a secure communication link, called the **Sophos Security Heartbeat™**, 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 Security Heartbeat™ integrates Endpoint and Network security for better 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 are able to 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 APT solution is still relatively new to the market. While it brings together many of the vendor's well known, proven components, it is still in its early deployment stages and will need 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.

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

- 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 integration with Directory services.

- Webroot is best known for its next generation endpoint protection, but lacks visibility as a next generation APT solution provider.

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

Barracuda Networks

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

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

Solution

Barracuda NextGen Firewall F-Series is a family of hardware and virtual appliances designed to protect network infrastructure. Beyond its network firewall and VPN technologies, the F-Series integrates a set of next-generation firewall technologies, including identity-aware Application Control, intrusion prevention, web filtering, antivirus, anti-spam, and Network Access Control. **Barracuda Networks' Advanced Threat Detection (ATD)** implements full-system emulation, which provides the deep visibility into malware behavior. Files are checked against a cryptographic, constantly updated hash database, and in case the file is not known, it is emulated in a virtual sandbox where malicious behavior can be discovered.

Barracuda NextGen Firewall F-Series supports two types of emulation policies that can be assigned to specific file types. The first policy is the traditional “let the user download a file and forward it to the emulation service.” As soon as the file is scanned and malicious file activity has been identified, a log event is created and the administrator can contact the user to remediate the threat. Barracuda NextGen Firewall F-Series provides an automatic User/IP/machine blacklisting feature that will automatically quarantine victims of advanced malware by blocking further network activities. The second policy that can be assigned on a per-file basis, forces the user to wait until the file is emulated and not malicious or suspicious. Only benign files are then forwarded to the respective user.

Barracuda ATD is available for hardware and virtual appliances as well as for Microsoft Azure and the Amazon AWS Cloud. It provides:

- *Full System Emulation* - helps not only detect targeted and persistent attacks, but also malware that was designed to evade detection by traditional sandboxes used by first generation advanced persistent threat security solutions.

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

- *Automatic Email Notifications* - in case malware activity has been identified can help minimize the time for reaction of the administrator in order to mitigate network breaches.

- *Local cryptographic hash database* – offers emulation optimization.

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

STRENGTHS

- Easy to deploy, use, and affordable Advanced Persistent Threat Protection with single-pane-of-glass management which requires no new equipment.

- Barracuda NextGen Firewalls are available as purpose-built hardware, virtual appliances, as well as for major public clouds including Microsoft Azure, Amazon AWS and Vmware Vcloud Air. This allows Barracuda NextGen Firewall to provide secure, fast connectivity across hybrid on-premises and cloud network components.

- The Web Filter option of the F-Series firewall enables highly granular, real-time visibility into online activity broken down by individual users and applications, this allows administrators to better create and enforce effective Internet content and access policies.

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

- Barracuda NextGen Firewalls 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 special-purpose DLP solution.

- Barracuda APT is focused on detection and prevention at the firewall level, but does not include endpoint protection.

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

- Barracuda does not yet provide deep integration with third party SIEM and Breach Detection Systems.

SPECIALISTS

FORTINET

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

Founded in 2000, Fortinet is a leading vendor of next-generation firewall and network security solutions. The company offers network security appliances and security subscription services aimed at the needs of carriers, data centers, enterprises, distributed offices and MSSPs.

SOLUTIONS

Fortinet offers an integrated advanced threat protection (ATP) framework, which includes technologies to prevent, detect and mitigate threats. 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, anti-spam, DLP, WAN acceleration, and WLAN control.

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: antispam, antiphishing, 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 bidirectional protection against malicious sources, application layer DoS Attacks, and sophisticated threats such as SQL injection and cross-site scripting.

FortiAuthenticator - provides strong two-factor authentication, RADIUS, LDAP and 802.1X Wireless Authentication Certificate management, as well as Single Sign-on.

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

FortiAnalyzer – provides log and reporting to build and maintain a comprehensive view of an organization’s security posture.

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. Integration between **FortiSandbox Cloud** and FortiGate enables administrators to quarantine infected endpoints with one click of a button.

FortiGate – pre-filters traffic so only at risk objects are forwarded to FortiSandbox for analysis. A single FortiSandbox can support multiple FortiGates, eliminating the need to put a sandbox at every ingress/egress point.

New threat information uncovered by FortiSandbox is used by the **FortiGuard Labs** threat research team, to create new security updates to be sent to all Fortinet products. For instance, FortiSandbox can provide an excellent preventative security measure through integration with FortiMail, where FortiMail can hold an email while any risky object in that email is analyzed via FortiSandbox. The email is then delivered to the recipient after it has passed sandbox analysis, or blocked if malicious items are identified.

Fortinet also offers a range of services to help mitigate attacks including Resident Engineers, Premier Signature Services and more.

STRENGTHS

- Effective threat prevention validated through independent testing with NSS Labs, VB100, 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.

- Fortinet offers an integrated approach to sandboxing, making it easy to deploy and affordable.

- Custom ASICs and hardware that deliver performance, enabling more security to be deployed at each inspection point.

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

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

- Fortinet's depth of forensic packet capture/replay is currently somewhat limited.

- Fortinet does not offer remediation capabilities.

CISCO

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

Cisco is a leading vendor of Internet communication and security technology. In October 2013, Cisco completed its acquisition of Sourcefire, and in June 2014, it completed the acquisition of ThreatGRID, which offers a cloud-based malware analysis and on-premise sandboxing appliance. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), which is made up of leading threat researchers.

Cisco Advanced Malware Protection (AMP) for Endpoints can detect, analyze, block, track, and remediate advanced malware outbreaks across endpoints, including PCs, Macs, Linux, mobile devices and virtual systems. AMP for Endpoints uses global threat intelligence from Talos Research and AMP Threat Grid to strengthen defenses to prevent breaches before they occur. It also uses a telemetry model to take advantage of big data, continuous analysis, and advanced analytics.

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 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 – AMP for Endpoints integrates with AMP for Networks. All detection information is sent to the FireSIGHT 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 the installed software is up to date according to the vendor, or if the installed version has an 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, Advanced Malware assessments, and mobile-specific root cause analysis.

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

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 entering the 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 and alert to files that become malicious after the initial point of entry.

- AMP for Endpoints offers protection across PCs, Macs, mobile devices, 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 can be added to Email, Web, Next-Generation Intrusion Prevention Systems, and Cisco routers, to offer faster, easier protection in more places across the organization.

WEAKNESSES

- Cisco needs to improve on the management of its solutions through a more unified management console that can bring together its broad range of security solutions.

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

- Cisco AMP for Endpoints needs to provide more in-depth incident response capabilities.

- Cisco AMP for Endpoints needs to expand its coverage of Linux platforms.

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

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

PALO ALTO NETWORKS, INC.

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 as an on-premise, or 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.

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.

SOLUTION

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 is complemented with malware knowledge from the Kaspersky Security Network (KSN), which receives threat intelligence in real time from across the world, which 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 and anomaly detection in an easy to use console that gives Security Officers a comprehensive picture of corporate IT network security incidents.

The platforms provides the following functionality:

- Multiple sensors to detect activities at multiple areas of the customers 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 level of suspicion of the traffic and detect potential attacks. It supports HTTP, FTP and DNS protocols.

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

  - The Email Sensor supports integration with mail servers, via a POP3S 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 customers 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.

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

- The Kaspersky Anti Targeted Attack Platform is a newly released solution from Kaspersky Lab that brings together many of the vendor's known, proven components into a cohesive platform, however it is still in its early development stages and will need to mature through customer deployment.

- Full integration with many other security products from Kaspersky Lab (such as Kaspersky Endpoint Security, Secure Web Gateway, Secure Mail Gateway) is currently still in development.

- Currently the Kaspersky Anti Targeted Attack Platform acts only as an expert system focused on attack detection. Automatic response is not yet available, and is on the roadmap after further integration with Kaspersky Lab security products (e.g. Kaspersky Endpoint Security, Secure Web Gateway, Secure Mail Gateway).

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

THE RADICATI GROUP, INC.

http://www.radicati.com

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

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

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

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

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

Consulting Services:

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

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

Multi-Client Studies

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

MARKET RESEARCH PUBLICATIONS

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

Currently Released:

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

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

Upcoming Publications:

Title	To Be Released	Price*
Information Archiving Market, 2016-2020	May 2016	$3,000.00
Advanced Threat Protection (APT) Market, 2016-2020	May 2016	$3,000.00

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

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