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

* Radicati Market QuadrantSM is copyrighted March 2017 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 QuadrantsSM 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 QuadrantsSM 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 .......................................................... 3
- Market Segmentation – Advanced Persistent Threat (APT) Protection ............... 5
- Evaluation Criteria ......................................................................................... 7
- Market Quadrant – APT Protection .............................................................. 10
  - Key Market Quadrant Highlights .............................................................. 11
- APT Protection - Vendor Analysis ................................................................. 11
  - Top Players ................................................................................................. 11
  - Trail Blazers ............................................................................................. 20
  - Specialists ................................................................................................. 24

Please note that this report comes with a 1-5 user license. If you wish to distribute the report to more than 5 individuals, you will need to purchase an internal site license for an additional fee. Please contact us at admin@radicati.com if you wish to purchase a site license.

Companies are never permitted to post reports on their external web sites or distribute by other means outside of their organization without explicit written prior consent from The Radicati Group, Inc. If you post this report on your external website or release it to anyone outside of your company without permission, you and your company will be liable for damages. Please contact us with any questions about our policies.
Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

1. **Top Players** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as possess a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don’t become Top Players overnight. Most of the companies in this quadrant were first Specialists or Trail Blazers (some were both). As companies reach this stage, they must fight complacency and continue to innovate.

2. **Trail Blazers** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don’t necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for “disrupting” the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

3. **Specialists** – This group is made up of two types of companies:
   a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.
   b. Established vendors that offer very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.

4. **Mature Players** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered “movers and shakers” in this market as they once were.
   a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, they may choose to slow development on existing products.
b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.

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

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

The horizontal “x” strategic vision axis reflects a vendor’s understanding of the market and their strategic direction plans. It is common for vendors to move in the quadrant, as their products evolve and market needs change.
**MARKET SEGMENTATION – ADVANCED PERSISTENT THREAT (APT) PROTECTION**

This edition of Radicati Market Quadrants℠ 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**

![Radicati Market Quadrant SM](image)

*Figure 3: APT Protection Market Quadrant, 2017*

* Radicati Market QuadrantSM 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 QuadrantsSM 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 QuadrantsSM 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

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.

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

**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.

**Intel Security (McAfee)**

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


- 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

**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.
APT Protection - Market Quadrant 2017

- 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

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

**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

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
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

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

**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

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

**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. 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:**

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

* Discounted by $500 if purchased by credit card.

**Upcoming Publications:**

<table>
<thead>
<tr>
<th>Title</th>
<th>To Be Released</th>
<th>Price*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Mobility Management Market, 2017-2021</td>
<td>Apr. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Advanced Threat Protection Market, 2017-2021</td>
<td>Apr. 2017</td>
<td>$3,000.00</td>
</tr>
</tbody>
</table>

* Discounted by $500 if purchased by credit card.

All Radicati Group reports are available online at [http://www.radicati.com](http://www.radicati.com)