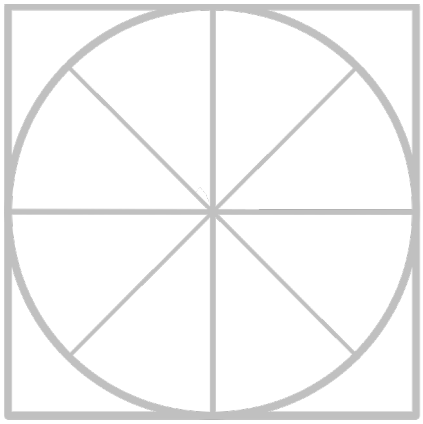
The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Advanced Persistent Threat (APT) Protection - Market Quadrant 2018



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

February 2018

Radicati Market Quadrant[SM] is copyrighted February 2018 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

==========

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 EXPLAINED

Radicati Market Quadrants are designed to illustrate how individual vendors fit within specific technology markets at any given point in time. All Radicati Market Quadrants are composed of four sections, as shown in the example quadrant (Figure 1).

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

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

3. ***Specialists*** – This group is made up of two types of companies:

    a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.

    b. Established vendors that offer very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.

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

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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.

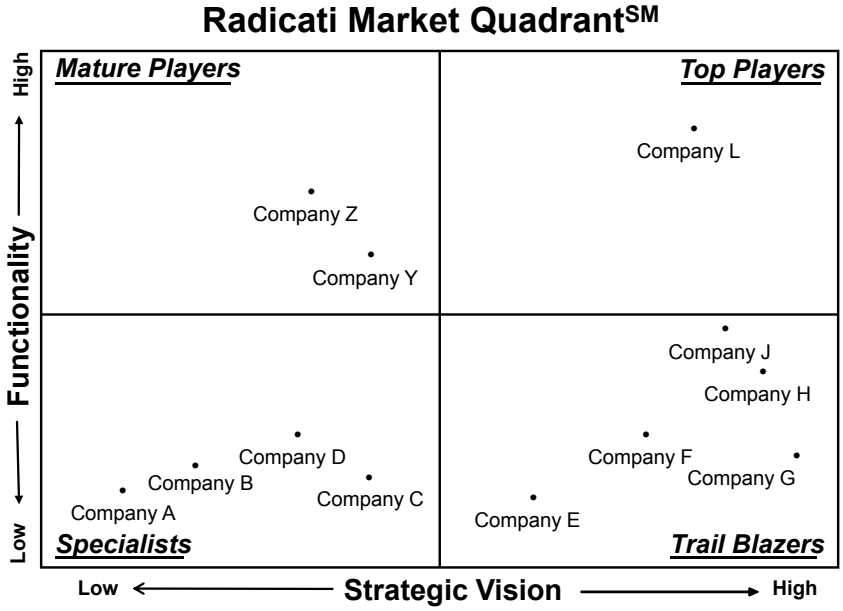


Figure 1: Sample Radicati Market Quadrant

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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 *Barracuda Networks, Cisco, FireEye, Forcepoint, Fortinet, Kaspersky Lab, McAfee, Microsoft, Palo Alto Networks, Sophos, Symantec,* and *Webroot.*

- This report only looks at vendor APT protection solutions aimed at the needs of enterprise businesses. It does not include solutions that target primarily service providers (i.e. carriers, ISPs, etc.).

- APT protection solutions can be deployed in multiple form factors, including software, appliances (physical or virtual), 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 all organizations are increasingly concerned about zero-day threats and highly targeted malicious attacks.

- The worldwide revenue for APT Protection solutions is expected to grow from over $3.7 billion in 2018, to over $8.6 billion by 2022.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

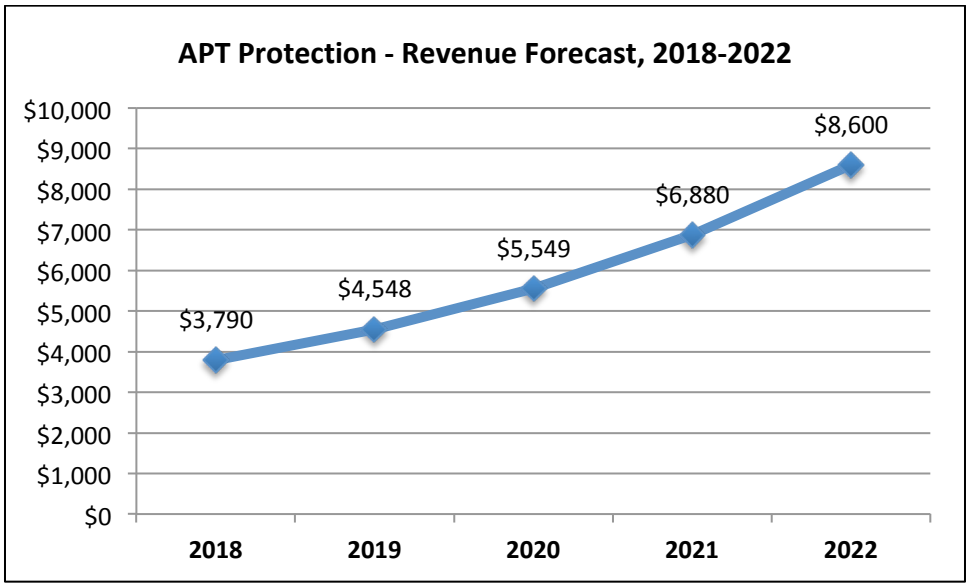


Figure 2: APT Protection Market Revenue Forecast, 2018 – 2022

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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.

- *Platform Support* – support for threat protection across a variety of platforms including: Windows, macOS, Linux, iOS, and Android.

- *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.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- *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.

- *Endpoint Detection and Response (EDR)* – is the ability to continuously monitor endpoints and network events, in order to detect internal or external attacks and enable rapid response. EDR systems feed information into a centralized database where it can be further analyzed and combined with advanced threat intelligence feeds for a full understanding of emerging threats. Some EDR systems also integrate with sandboxing technologies for real-time threat emulation. Most EDR systems integrate with forensic solutions for deeper attack analysis.

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

- *Cloud Access Security Broker (CASB)* – are on-premises or cloud-based solutions that sit between users and cloud applications to monitor all cloud activity and enforce security policies. CASB solutions can monitor user activity, enforce security policies and detect hazardous behavior, thus extending an organization's security policies to cloud services.

- *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.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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

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.*

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

MARKET QUADRANT – APT PROTECTION

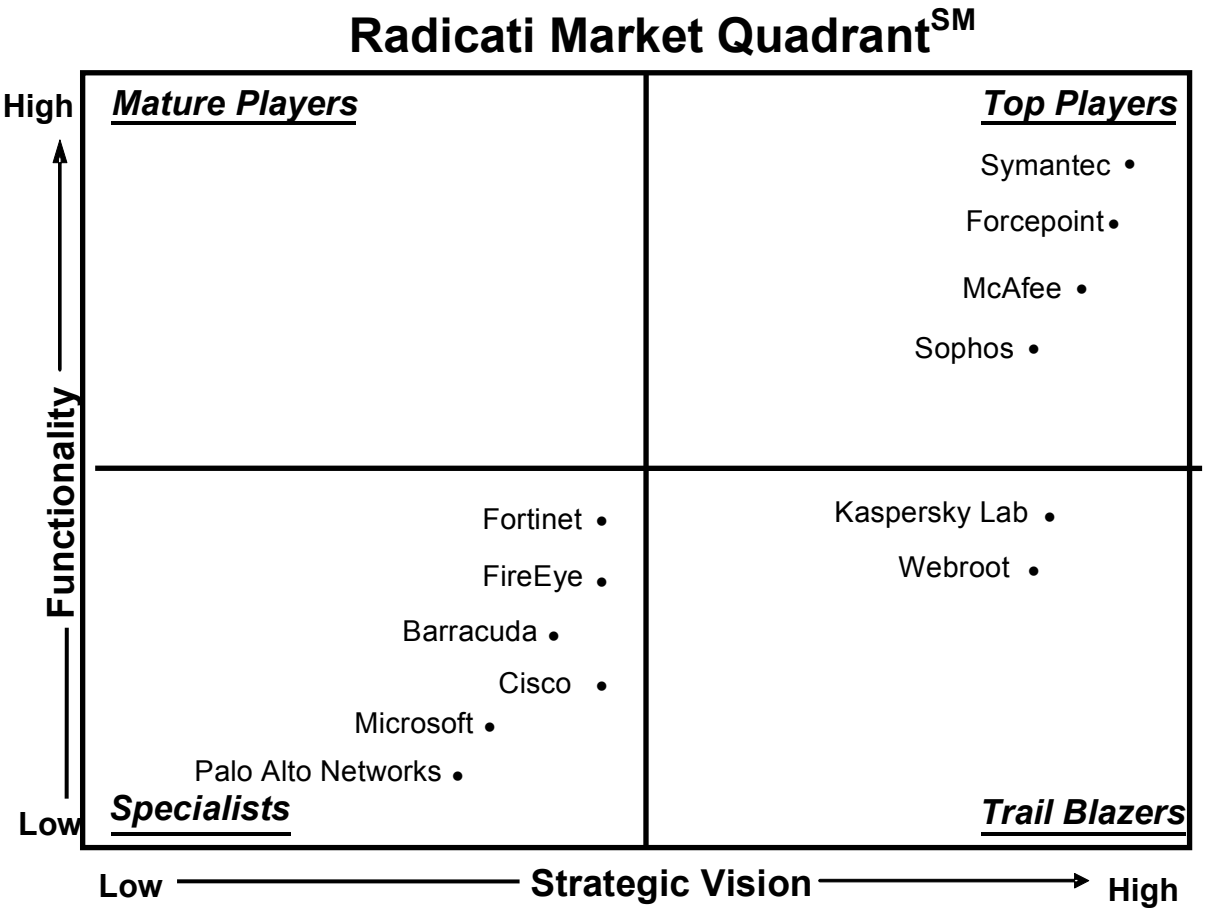


Figure 3: APT Protection Market Quadrant, 2018

· Radicati Market Quadrant℠ is copyrighted February 2018 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT HIGHLIGHTS

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

APT PROTECTION - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

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

Founded in 1982, Symantec has grown to be one of the largest providers of enterprise security technology. In 2016, Symantec completed its acquisition of Blue Coat, a leading provider of web security technology. Symantec's security solutions are powered by its *Global Intelligence Network* which combines technologies from both Symantec and Blue Coat, to offer real-time threat intelligence. Symantec is a publicly traded company.

SOLUTIONS

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- ***Symantec Advanced Threat Protection (ATP)*** **–** is a unified platform that uncovers, prioritizes, investigates, and remediates advanced threats across multiple control points from a single console. It aggregates and correlates threat events from the three ATP 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. The solution platform provides a single pane of glass across all three modules, providing visibility into attacks in real-time and the ability to quickly remediate attacks across multiple threat vectors.

  - *Symantec ATP: Endpoint module* **–** provides Endpoint Detection and Response (EDR) capabilities without adding a new endpoint agent. It leverages the Symantec Endpoint Protection product, to look for Indicators-of-Compromise (IoC) across all endpoints; remediate all instances of threats, isolate compromised endpoints and blacklist malicious files, with a single click. ATP: Endpoint 3.0 has added full endpoint activity recording, direct searching of endpoints for indicators of compromise, file-less threat detections (including suspicious PowerShell scripts and memory exploits) and hybrid sandboxing (cloud-based and on-premises).

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

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

  - *Symantec Endpoint Detection and Response (EDR) Cloud* **–** delivers in-depth threat visibility and breach response across the entire enterprise. It offers multiple layers of detection, visual analysis of complex cyber data and automated playbooks to ease administration. In addition, Symantec's EDR cloud solution provides full visibility and automated threat hunting across all endpoints through applied forensic reasoning and

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

expertise to identify suspicious activity. Organizations can conduct a point-in-time scan of the entire environment to automatically hunt and remediate suspicious activity in the enterprise. The solution does not require the deployment of new endpoint agents.

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

- ***Symantec Content Analysis –*** analyzes and mitigates unknown content by automatically inspecting files from ProxySG, Symantec Messaging Gateway, or other sources though multiple layers of in-house proprietary technology as well as third-party technology (reputation, dual anti-malware engines, static code analysis, etc.). It then brokers suspicious content to the Symantec Malware Analysis solution or other third parties for sandboxing. Content Analysis inspection and sandboxing are available as on-premises, hybrid or cloud-hosted solutions. Intelligence is shared through the Symantec Global Intelligence Network, providing enhanced protection across the entire security infrastructure.

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

- ***Symantec Global Intelligence Network (GIN)*** – provides a centralized, cloud-based, threat indicator repository and analysis platform. It enables the discovery, analysis, and granular classification of threats from multiple vectors (e.g. endpoint, network, web, email, application, IoT, and others) and proactively protects other vectors of ingress without the need to re-evaluate the threat. GIN distributes critical threat indicators derived from a combination of human and AI (artificial intelligence) research processes, including file hashes, URLs, IP addresses, and application fingerprints. GIN technology can be rapidly deployed into virtually any product or

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

service, including cloud applications, IoT to server class hardware (x86 and ARM), Windows, iOS, Linux, and MacOS.

STRENGTHS

- Symantec offers on-premises, cloud, and hybrid options across most of its security product portfolio. Symantec's endpoint protection and management, as well as Symantec' Endpoint Detection and Response, offer a 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, web isolation, mobile protection, CASB 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, mobile, cloud application and more.

- Symantec Content Analysis, which incorporates Malware Analysis sandboxing, offers a customizable hybrid sandbox solution with both physical and virtual execution to uncover threats that have "virtual-awareness". Content Analysis and Symantec Advanced Threat Protection also leverage this sandboxing capability via a cloud-hosted option.

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

- Symantec recently acquired Skycure, to provide dedicated mobile device protection and 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's Global Intelligence Network (GIN) provides a comprehensive source of real-time threat intelligence from multiple sources, including the entire Symantec and former Blue Coat customer base, which provides Symantec products with on-demand real-time URL and file disposition.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- 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

- Symantec solutions are typically a good fit for larger enterprises with complex needs and an experienced security team. However, some of Symantec's cloud solutions offer streamlined protection for smaller customers.

- Symantec ATP customers we interviewed indicated, that while feature-rich, the product is somewhat difficult and complex to set up.

- Symantec is still working through all the nuances of integration across its combined Symantec and Blue Coat portfolio, but making progress. Customers should check carefully on the features they expect in each solution component.

FORCEPOINT

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

Forcepoint, is a Raytheon and Vista Equity Partners joint venture, formed in 2015 through the merger of Websense and Raytheon Cyber Products. In 2017, Forcepoint acquired the Skyfence CASB business from Imperva, as well as RedOwl, a vendor of User and Entity Behavior Analytics (UEBA).

SOLUTIONS

Forcepoint's APT solution, Forcepoint **Advanced Malware Detection (AMD)** 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 partners with Lastline, a sandbox technology vendor, to provide its Forcepoint AMD capability. Forcepoint AMD is available as a cloud-based solution, or as an

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

appliance. It provides file and email URL sandboxing, detailing forensic reporting and phishing education. All Forcepoint products work together as part of what the vendor calls, the *Human Point System*, which focuses on the intersection of human behavior analysis and data.

There are currently two types of AMD offerings:

- **AMD Cloud (Previously known as Threat Protection Cloud)** – is a SaaS solution that integrates out of the box with Forcepoint Web Security, Email Security, CASB, and NGFW products.

- **AMD On Premises (Previously known as Threat Protection Appliance)** – is an on-premises appliance-based solution that integrates out of the box with Forcepoint Web Security, Email Security, and Next Generation Firewall products.

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 provides 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 DLP** – a full content-aware data loss prevention solution which includes OCR, Drip-DLP, custom encryption detection, machine learning, and fingerprinting of data-in-motion, data-at-rest, or data-in-use.

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- **Forcepoint UEBA** - Forcepoint User and Entity Behavior Analytics (UEBA) enables security teams to proactively monitor for high-risk behavior inside the enterprise. The security analytics platform provides context information by fusing structured and unstructured data to identify and disrupt malicious, compromised or negligent users.

The **Forcepoint Security Manager Console** allows integrated policy management, reporting and logging for multiple on-premise gateways and/or cloud for hybrid customers. The unified management and reporting functions streamline work for security teams, giving them the context and insights they need to make better decisions, minimize the dwell time of attacks and prevent the exfiltration of sensitive data.

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 User and Entity Behavior Analytics (UEBA), enables security teams to proactively monitor for high-risk behavior inside the enterprise. The security analytics platform provides context information by fusing structured and unstructured data to identify and disrupt malicious, compromised and negligent users.

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

- Forcepoint offers its own context-aware DLP, which provides enterprise-class data theft protection across endpoints, Web and Email gateways, as well as networked and cloud storage. Advanced detection techniques, such as OCR (Optical Character Recognition), 'Drip-DLP', and encrypted payloads ensure effectiveness.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

WEAKNESSES

- Forcepoint does not yet offer AMD protection for endpoints. However, the vendor has this on the roadmap for later in 2018.

- 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.

- For remediation, Forcepoint solutions currently provide identification, blocking and alerts of compromise, but do not provide malware removal or device re-imaging.

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

- Forcepoint does not provide and EDR solution. However, Forcepoint AMD can tie into third party EDR solutions through custom integrations.

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

MCAFEE

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

McAfee delivers security solutions and services for business organizations and consumers. The company provides security solutions, threat intelligence and services that protect from cloud to endpoints, networks, servers, and more. McAfee recently acquired Skyhigh Networks, a leading CASB provider.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

SOLUTIONS

McAfee Advanced Threat Defense enables organizations to detect advanced targeted attacks and convert threat information into immediate action and protection. McAfee offers physical appliances, virtual appliances and cloud options.

Unlike traditional sandboxing, Advanced Threat Defense includes static code analysis and machine learning, which provide additional inspection to broaden detection and expose evasive threats. Tight integration between security solutions, from network and endpoint to investigation and support for open standards, enables instant sharing of threat information across an organization including multi-vendor environments. 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, static code analysis and machine learning, together provide inspection and detection capabilities. Malicious activity is observed in the sandbox environment and simultaneously examined with in-depth static code analysis and machine learning to broaden detection and identify evasive maneuvers.

- *Centralized deployment* – allows customers to leverage shared resources across protocols and supported products for malware analysis with a scalable appliance-based architecture. Flexible deployment options include physical appliances, virtual appliances and cloud options, including Azure.

- *Integrated security framework* – a McAfee-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 to make immediate decisions about next steps from blocking traffic, executing an endpoint service, investigation and/or detection of whether an organized attack is taking place against targeted individuals.

Advanced Threat Defense plugs in and integrates out-of-the-box with other McAfee solutions, including:

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- Network Security Platform (IPS)
- Enterprise Security Manager (SIEM)
- ePolicy Orchestrator (ePO)
- McAfee Endpoint Solutions
- McAfee Active Response (EDR)
- Web Gateway
- 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. McAfee Data Exchange Layer (DXL) and REST APIs facilitate integration with third party products. McAfee supports threat-sharing standards, such as Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) to enable further integration with third party solutions. Advanced Threat Defense also supports third party email gateways, and integration with BRO-IDS, an open source network security monitor.

STRENGTHS

- McAfee offers deployment and purchasing flexibility through appliance, virtual appliance and cloud form factors with CapEx and OpEx purchase options. McAfee Advanced Threat Defense is also available from the Azure Marketplace.

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

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

- Report and outputs include sharing of Indicators of Compromise (IOC) data through threat sharing standards (STIX/TAXII) to better target investigations, or take action.

- McAfee offers full protection across endpoints, desktop computers and servers.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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

- Centralized analysis device acts as a shared resource between multiple security devices from McAfee, as well as from other vendors.

- 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.

- McAfee 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).

- McAfee offers its own DLP technology, which is applied in-line to traffic by an integrated Web Gateway.

WEAKNESSES

- McAfee does not offer its own email gateway solution. However, McAfee Advanced Threat Defense can now integrate with third party email solutions to provide file attachment analysis.

- McAfee Advanced Threat Defense does not support Apple macOS, or Linux platforms.

- McAfee Advanced Threat Defense mobile malware inspection is only available for Android (.apk) applications.

- Management of McAfee 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.

- For remediation, McAfee Endpoint initiates several actions, which may include blocking, cleaning up malware, and quarantining endpoints as needed. However, it does not currently rollback to a known good state.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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, data science, and malware research. Sophos provides synchronized security solutions, that include endpoint and mobile security, enterprise mobility management, encryption, server protection, secure email and web gateways, next-generation firewall and unified threat management (UTM).

SOLUTIONS

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

Sophos XG Firewall - 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 firewall 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.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- *Intrusion Prevention System* – which can identify and block APTs attempting to enter the network, or move laterally across the network by exploiting vulnerabilities in servers and systems.

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

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.

Sophos' Firewall-OS (SF-OS) runs on SG Series appliances and includes *synchronized security* technology, which integrates endpoint and network security for protection against advanced threats. For instance, SF-OS Sophos SG Series Appliances can link the next-generation firewall with Sophos Endpoint Protection through its Security Heartbeat synchronized security technology, which enables the network and endpoint to correlate health, threat, and security indicators for prevention, detection, actionable alerting, and remediation. This provides automated incident response that can restrict network access to endpoints on which malware has been detected, or that have had their endpoint agent disabled. It also extends Firewall 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.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

STRENGTHS

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

- Synchronized Application Control explicitly identifies all networked applications (including APTs and malware) by sharing application information between endpoint and firewall. This eliminates the issue with signature-based app control that often categorize the majority of app traffic as generic HTTP or HTTPS.

- 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 and remnants of 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 XG Firewall and Sophos Endpoint Protection solutions for faster, more cohesive APT protection.

- Sophos Sandstorm was recently upgraded to use Deep Learning technology, which can help detect zero-day threats faster and more accurately. Sophos Sandstorm integrates with Sophos 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

- 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 SophosLabs, over providing administrators with granular, do-it-

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

yourself controls.

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

- Sophos does not currently offer a CASB solution, or APIs for integration with third party CASB solutions. However the vendor has this on its near-term roadmap.

- Sophos does not currently offer a full EDR solution, however, Intercept X does offer some capabilities, through its Root Cause Analysis feature, that are typically part of an EDR solution.

- For remediation, Sophos currently offers capabilities to block, quarantine and remove malware and associated remnants but it does not offer full device reimaging capabilities.

TRAIL BLAZERS

KASPERSKY LAB

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

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

SOLUTIONS

The **Kaspersky Anti Targeted Attack Platform (KATA)** includes different features focused on malware detection (known, unknown and advanced malware). An Advanced Sandbox offers file behavior analysis and URL detonation, and is complemented with malware knowledge from the

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

Kaspersky Security Network (KSN), which receives threat intelligence in real time from across the world and allows security officers to distinguish targeted attacks from malware outbreaks.

Kaspersky Anti Targeted Attack Platform (KATA) combines with Kaspersky Endpoint Detection and Response (EDR) through a shared console and server architecture, to give endpoint visibility and rapid response. This approach can be supplemented with Kaspersky Cybersecurity Intelligence Services and Premium Support to offer advanced threat protection with centralized administration, helping automate and facilitate the threat management cycle.

The platform comprises the following functionality:

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

    - The network sensor is able to extract the information about source, destination, volume of the data and periodicity from network traffic (including encrypted). This information is typically enough to make a decision about the level of suspicion of the traffic and to detect potential attacks. It supports SMTP, POP3S, HTTP, ICAP, FTP and DNS protocols.

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

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

- *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 swiftly detect abnormal behavior on the customer's network.

- *Incident response and analysis* – to assist with incident response and post-attack investigations, detailed logs of alerts are recorded for analysis within the Kaspersky Anti

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

Targeted Attack Platform, or the logs can be imported into the customer's SIEM (Security Information and Event Management) system.

- *URL reputation analysis* – based on reputation data from the cloud-based, global Kaspersky Security Network helps detect suspicious or undesirable URLs. It also includes information about URLs and domains, which are connected to targeted attacks.

- *Intrusion Detection* – KATA also includes industry-standard Intrusion Detection System (IDS) technology, combining both traditional and advanced threat detection, to protect against sophisticated threats. IDS rule sets are automatically updated.

- *Traffic Analysis* – KATA provides traffic analysis across the entire customer corporate network. It offers a scalable architecture for sandboxes and sensors compatible with heterogeneous IT environments.

- *EDR* – KATA is fully integrated with Kaspersky's EDR product, which gives security officers the ability to run a full incident response process in the same console, from incident discovery to remediation actions.

- *Email Security* – KATA is fully integrated with the Kaspersky Security Mail Gateway product, allowing it to block email threats.

STRENGTHS

- KATA provides advanced threat and targeted attack detection across all layers of a targeted attack, from initial infection, command and control communications, and lateral movements and data exfiltration.

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

- Integration with the Kaspersky Security Mail Gateway provides the ability to block suspicious files in email traffic.

- The Kaspersky Security Network offers a large threat intelligence database which allows to check files, URLs, domains and behavior in order to detect suspicious activity and reduce

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

false alerts.

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

- The use of the same console and server architecture in Kaspersky Anti Targeted Attack platform and Kaspersky EDR provides security offices with seamless workflow during the incident response process.

- 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.

- 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.

- Kaspersky does not offer a CASB solution, however, it provides APIs for integration with third party CASB solutions.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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

Webroot, founded in 1997, delivers endpoint security, network security, security awareness training and threat intelligence solutions. Webroot is headquartered in Colorado, and operates globally across North America, Europe and the Asia Pacific region. Webroot is a privately held company.

SOLUTIONS

Webroot offers the **SecureAnywhere** suite of security products for endpoints and mobile devices. This set of cloud-based solutions offer continuous, real-time updates on threats.

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, macOS 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 solutions combine real-time intelligence from Webroot BrightCloud services with advanced machine learning and behavior-based heuristics, to detect, analyze, categorize, score, and accurately predict the threats each endpoint is experiencing in real time.

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 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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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.

- Webroot relies on behavioral analysis (versus static lists), which allows for continuous updates to known bad and known good files, allowing the solution to track the activity of unknown or not known good files.

- 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 roll-back and journaling, when an executable is deemed bad, the solution will automatically rollback the activity of the malicious files and auto-remediate infected endpoints.

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

WEAKNESSES

- Webroot focuses on advanced endpoint protection, but does not currently integrate its endpoint solution with network, web or email security gateway solutions, requiring in-line file scanning.

- 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, but does offer AD mirroring in its management console.

- 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.

- Webroot does not offer a CASB solution, or provide APIs for integration with third party CASB solutions.

- Webroot SecureAnywhere contains some elements of EDR, but Webroot does not offer a full EDR solution.

SPECIALISTS

FORTINET

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

Founded in 2000, Fortinet develops security and networking solutions. The company offers physical and virtual appliances, security subscription services, IaaS and SaaS offerings aimed at

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

the needs of carriers, data centers, enterprises, distributed offices, SMBs and MSSPs. Fortinet is a publicly traded company.

SOLUTIONS

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

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

- **FortiMail Secure Email Gateway** – provides a single solution to protect against inbound attacks, including advanced malware, as well as outbound threats and data loss. It includes: anti-spam, anti-phishing, anti-malware, content disarm and reconstruction, sandboxing, data leakage prevention (DLP), identity based encryption (IBE), and message archiving. FortiMail is available in all form factors, including physical and virtual appliance (e.g. Azure, AWS), SaaS or as a Managed Security Service.

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

- **FortiClient Endpoint Protection** – offers endpoint client protection for desktops, laptops, tablets and smartphones. It includes next generation capabilities, such as anti-exploit protection, support for Chromebooks, and more.

- **FortiSandbox** – provides deep analysis of at risk objects to discover new and unknown malware, malicious or compromised sites, command and control servers and more. FortiSandbox integrates with FortiWeb and FortiMail. 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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

skip directly to reporting findings, speeding up the time to action. FortiSandbox delivers deep analysis of new threats, including their intended behavior and endpoints that may have been infected. Following analysis, FortiSandbox generates real-time local threat intelligence that is immediately available to integrated Fortinet ATP components for automated response as well as accessible via APIs as third party update packages. Integration between FortiSandbox and the flagship FortiGate enables administrators to quarantine infected endpoints with one click of a button, while integration with FortiMail and FortiClient give organizations the option to hold new objects for sandbox analysis and block previously unknown attacks. FortiSandbox is available as a physical or virtual appliance, as well as a public cloud service in AWS.

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

New threat information uncovered by FortiSandbox can be directly shared among a customer's deployed Fortinet and third party Fabric Ready components, as well as used by the **FortiGuard Labs** threat research team, to create new security updates to be sent to all Fortinet products.

STRENGTHS

- Fortinet solutions available in all form factors, including physical and virtual appliance (e.g. Azure, AWS), SaaS or as a Managed Security Service, which helps it address the complex deployment needs of a broad range of customers.

- 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.

- FortiSandbox delivers deep analysis of new threats, including their intended behavior and endpoints that may have been infected, and generates real-time threat intelligence that is immediately available to integrated Fortinet ATP components, as well as accessible via APIs by its Fabric-ready partners.

- Fortinet delivers custom security processors and hardware to deliver high performance, thus enabling more security to be deployed at each inspection point.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- Most Fortinet products are 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 certified Fabric-ready partners (e.g. Centrify) that offer this capability.

- Fortinet does not offer its own EDR solution, but integrates with solutions from Carbon Black, Ziften and others.

- Fortinet offers its own homegrown API-based CASB solution (FortiCASB), which is still in the early stages of development.

- 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.

- For remediation, Fortinet currently offers capabilities to block, quarantine and remove malware but it does not offer full reimaging capabilities.

FIREEYE

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

FireEye, founded in 2004, offers solutions to simplify, integrate and automate an organization's security operations. The company's solutions consist of network security, web security, email security, file security, endpoint security, malware analysis and security analytics. In addition, the company offers managed detection and response services, incident response services, threat intelligence and deep security forensics. In 2017, FireEye acquired Email Laundry, a provider of email security, and X15, a provider of next-generation Big Data management platform. FireEye is a publicly traded company.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

SOLUTIONS

FireEye's solutions portfolio comprises the following components:

- **FireEye Helix** – is a cloud-based, unified security operations platform, which offers a unified user experience across the FireEye product portfolio including network, email and endpoint security. Organizations can also send event data from non-FireEye components of their IT and security infrastructure into FireEye Helix, and overlay FireEye iSIGHT Threat Intelligence on that data to triage any buried threats. Helix helps centralize security data across the infrastructure and provides orchestration and automation capabilities.

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

- **FireEye Endpoint Security** – combines endpoint protection, detection and response capabilities to provide organizations with visibility against known and advanced threats. It blocks common attacks and then allows analysts to detect and correlate activities that indicate an exploit is in progress, inspect compromised endpoints and analyze gathered information to create custom IOCs and address previously unknown threats. It also helps isolate compromised endpoints with a single click (whether the endpoints are on or off-premise).

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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

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

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

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

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

STRENGTHS

- FireEye solutions can be deployed as on-premise appliances, virtual appliances, as well as in the cloud (through Amazon AWS).

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

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

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- FireEye Network, Email, and Content are easy-to-manage, clientless solutions that deploy quickly and require no tuning. The solutions can be deployed out-of-band, for in-line monitoring, or as in-line active blocking.

- 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 and third party technology, with intelligence and automation.

WEAKNESSES

- FireEye Network Security offers attack prevention and containment, but not orchestrated and automated remediation. This is provided via the FireEye Helix security operations platform.

- 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 some design support by the vendor.

- 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.

- FireEye currently supports SSL inspection through a separate standalone appliance. The vendor plans to include some basic SSL inspection capabilities in its Network Security solution later in 2018.

- FireEye Network Security does not offer Data Loss Prevention (DLP). DLP is currently only available as part of the FireEye Email Security solution.

- FireEye does not offer a CASB solution, however, it provides APIs for integration with third party CASB solutions.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

BARRACUDA NETWORKS

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

Founded in 2003, Barracuda is a provider of security and storage solutions that simplify IT for organizations of all sizes. Barracuda Networks was acquired in February 2018 by private equity firm Thoma Bravo in a move that took the company private.

SOLUTIONS

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

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

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

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

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

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

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

to identify infected clients.

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

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

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

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

Barracuda **Sentinel** is a real-time spear phishing and cyber fraud solution geared to Microsoft Office 365, which leverages artificial intelligence to analyze an organization's communication patterns and identify anomalous traffic. It combines the following capabilities:

- *Artificial Intelligence driven analysis* – artificial intelligence capability to identify Spear Phishing attacks without requiring time consuming manual configuration of keywords, phrases, and more.

- *Stops "payloadless" attacks* – identifies attacks based on a range of features and can easily identify, and stop, attacks that don't include a conventional malware or hostile link payloads.

- *DMARC enforcement* – includes DMARC enforcement capabilities to prevent domain impersonation and protect a customer's brand.

- *Integrated training* – includes user training and attack simulation, to increase an organization's defense posture.

Barracuda also recently acquired **PhishLine,** which delivers user education and advanced spear phishing simulation for email, SMS, and voicemail. It gives users the knowledge they need to identify targeted attacks before they take the bait. Barracuda PhishLine also gives organizations in depth analytics on user behavior, allowing them to provide targeted user training as needed.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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.

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

- Barracuda Sentinel requires minimal configuration, and integrates seamlessly with Office 365.

- Barracuda PhishLine offers advanced simulation of spear phishing attacks with expansive configuration options across email, SMS, voice mail, and physical media vectors.

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

WEAKNESSES

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

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

- Barracuda Sentinel is currently geared to detect spear phishing attempts only Microsoft Office 365 environments. Barracuda has additional support for on-premises Microsoft Exchange, Slack and other communication channels on the roadmap for future release.

- Barracuda Sentinel DMARC enforcement is not yet widely supported by third parties.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- Barracuda does not provide its own CASB solution. However, Barracuda Essentials for Office 365 offers some integrated, basic CASB functionality and Barracuda's Web Security Gateway supports ICAP for integration with third party CASB solutions.

- Barracuda does not provide a full EDR solution, but Barracuda NextGen Firewalls provide some basic built-in EDR capabilities.

- Barracuda remediation capabilities are limited to blocking, quarantining and removing malware, but do not offer full device reimaging.

CISCO

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

Cisco is a leading vendor of Internet communication and security technology. In August 2016, Cisco acquired CASB technology firm, CloudLock. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), which is made up of leading threat researchers.

SOLUTIONS

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

AMP for Endpoints delivers the following functionality:

- *Prevention* – AMP for Endpoints combines Global Threat Intelligence, malware blocking, file sandboxing and offers proactive protection by closing attack pathways before they can be exploited. A newly released exploit prevention engine detects and blocks exploitation

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

techniques that are commonly used to exploit memory corruption vulnerabilities in common applications.

- *Detection* – AMP for Endpoints continually monitors all activity on endpoints to identify malicious behavior, and detect indicators of compromise. Once a file lands on the endpoint, AMP for Endpoints continues to monitor and record all file activity. In addition, AMP detection gives visibility into what command line arguments are used to launch executables to determine if legitimate applications, including Window utilities, are being used for malicious purposes. If malicious behavior is detected, AMP can automatically block the file across all endpoints and show the security team the entire recorded history of the file's behavior. AMP for Endpoints delivers agentless detection, which serves to detect compromise even when a host does not have an agent installed. Using Cisco's Cognitive Threat Analytics (CTA) technology, AMP for Endpoints offers agentless detection when deployed alongside compatible web proxies (e.g. Cisco WSA, Symantec ProxySG, or other third parties). It helps uncover file-less or memory-only malware, web browser only infections, and stop malware before it compromises the OS-level.

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

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

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

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

against other network threat activity.

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

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

- *Management* – AMP for Endpoints comes with its own management console and can also integrate with the Firepower console for tighter management across all deployed Cisco security solutions. Cisco added an Inbox to provide users a workflow for incident response management and redesigned the dashboard to make it easier for users to access information and options from a central place in the portal.

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

In 2017, Cisco released a dedicated MSSP offering for endpoint security that includes: a dedicated portal to manage MSSP customers, a multi-tenant console, and OpEx-based pricing to reduce up-front investment costs.

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.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- 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.

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.

MICROSOFT

1 Microsoft Way
Redmond, WA 98052
www.microsoft.com

Microsoft provides a broad range of products and services for businesses and consumers, with an extensive portfolio of solutions for office productivity, messaging, collaboration, and more.

SOLUTIONS

Microsoft Advanced Threat Protection (ATP) is a cloud-based email filtering solution that provides protection against phishing, malware and spam attacks. It also offers near real-time protection against high-volume spam campaigns, with DKIM and DMARC support. It also adds

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

protection against "zero-day" attachments and harmful URL link, through real-time behavioral analysis and sandboxing. It can be deployed as an add-on to on-premises Microsoft Exchange Server deployments, Microsoft Exchange Online cloud mailboxes, or hybrid environments. It is included in Office 365Enterprise E5 and Office 365 Education A5 plans, or it can be added to other select Office 365 plans.

Microsoft ATP provides the following capabilities:

- *Safe Links* – protect users by blocking access to malicious urls in emails.
- *Spoof Intelligence* – detects when a sender appears to be sending email on behalf of one or more other users in an organization, and allows blocking of spoofed emails.
- *Quarantining* – allows messages identified as spam, phishing, or malware to be quarantined.
- *Advanced anti-phishing* – relies on machine learning capabilities to detect phishing emails.

Microsoft also offers **Advanced Threat Analytics (ATA)** an on-premises platform designed to protect enterprises from advanced targeted attacks and insider threats through machine learning techniques. ATA provides behavioral analytics, information on attack timelines, SIEM integration, email alerts, and builds a security graph detailing interactions of users, devices and resources.

STRENGTHS

- Microsoft ATP comes bundled free of charge with some Microsoft Office 365 plans, and is a low-cost to most other plans. Likewise Microsoft ATA is available free of charge to customers with Enterprise CAL licenses. Where an additional fee is required it is typically very small.
- Microsoft has been investing heavily to address growing concerns over spam, spoofing, phishing attacks, as well as blended attacks through attachments and harmful URLs.
- As a cloud service, Microsoft ATP is easy to deploy, and manage for customers of all sizes.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

- Microsoft ATA is a good first step for organizations looking for a low-cost EDR solution that is easy to deploy and manage.

WEAKNESSES

- While Microsoft has been investing heavily in its anti-malware, antispam, anti-phishing, and zero-day protection capabilities, customers still report high degrees of spam, malware and other forms of attack. Most Microsoft customers tend to also deploy additional email security solutions from best-of-breed security vendors.

- Customers with hybrid (on-premise and cloud) environments may find it difficult to understand how to effectively layer and combine the many different Microsoft security solutions.

- Microsoft offers many different plans at different price points, but it is sometimes difficult for customers to understand exactly what security features they are getting with what plans.

- Microsoft Office 365 customers we spoke to as part of this research, often indicated that Microsoft's customer support organization is not sufficiently knowledgeable when it comes to security issues.

PALO ALTO NETWORKS

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

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

SOLUTIONS

WildFire is Palo Alto Networks' APT solution. It can be deployed on any Palo Alto Networks security platform, or as a private cloud option where all analysis and data remain on the local

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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). It combines four independent techniques for threat discovery:

- *Dynamic analysis* – observes files as they detonate in a purpose-built virtual environment, which enables detection of zero-day exploits and malware using hundreds of behavioral characteristics.

- *Static analysis* – enables detection of exploits and malware that attempt to evade dynamic analysis, as well as identifies variants of existing malware.

- *Machine learning* – which extracts unique features from each file, training a predictive machine learning model to identify new malware.

- *Bare metal analysis* – which allows threats to be sent to a real hardware environment for detonation, removing the ability to deploy anti-VM analysis techniques.

WildFire executes suspicious content in Windows XP, Windows 7, Android and macOS operating systems. It offers visibility into commonly exploited file formats, such as EXE, DLL, ZIP, PDF, Microsoft Office documents, Java files, Android APKs, Adobe Flash applets and links within emails.
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 within minutes. It offers a unified, hybrid cloud architecture, which can be deployed either through the public cloud, or via a private cloud appliance that maintains all data on the local network.

WildFire offers integrated logging, reporting and forensics through a number of its own management solutions, including: the PAN-OS management interface, Panorama network security management, AutoFocus and the WildFire portal. An open API is available for integration with third-party security tools, such as SIEM (Security Information and Event Management) solutions.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

STRENGTHS

- Palo Alto Networks was an early innovator in network security, and one of the early developers of anti-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 full, 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 tend to be more costly when compared with other vendors in the 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 which need this functionality will need to look for third party solutions.

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

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

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

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

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

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

Consulting Services:

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

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

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited

MARKET RESEARCH PUBLICATIONS

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

Currently Released:

Title	Released	Price*
Email Statistics Report, 2018-2022	Mar. 2018	$3,000.00
Social Networking Statistics Report, 2018-2022	Mar. 2018	$3,000.00
Instant Messaging Statistics Report, 2018-2022	Feb. 2018	$3,000.00
Mobile Statistics Report, 2018-2022	Mar. 2018	$3,000.00
Endpoint Security Market, 2017-2021	Oct. 2017	$3,000.00
Secure Email Gateway Market, 2017-2021	Nov. 2017	$3,000.00
Enterprise Data Loss Prevention Market, 2017-2021	Nov. 2017	$3,000.00
Microsoft SharePoint Market Analysis, 2017-2021	Jun. 2017	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2017-2021	Jun. 2017	$3,000.00
Corporate Web Security Market, 2017-2021	Jun. 2017	$3,000.00
Email Market, 2017-2021	Jun. 2017	$3,000.00
Cloud Business Email Market, 2017-2021	Jun. 2017	$3,000.00
Advanced Threat Protection Market, 2017-2021	Apr. 2017	$3,000.00
Enterprise Mobility Management Market, 2017-2021	Apr. 2017	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Information Archiving Market, 2018-2022	Mar. 2018	$3,000.00
Advanced Threat Protection Market, 2018-2022	Mar. 2018	$3,000.00
Unified Endpoint Management Market, 2018-2022	Mar. 2018	$3,000.00

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

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

Copyright © February 2018, The Radicati Group, Inc. Reproduction Prohibited