The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Advanced Persistent Threat (APT) Protection - Market Quadrant 2019

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

March 2019

· Radicati Market Quadrant^{SM} is copyrighted March 2019 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.

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.

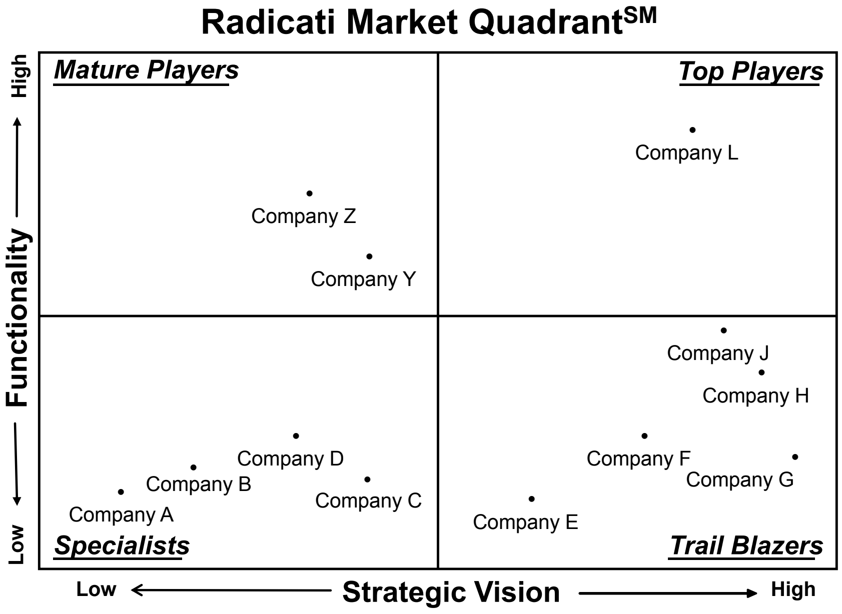

Figure 1: Sample Radicati Market Quadrant

INCLUSION CRITERIA

We include vendors based on the number of customer inquiries we receive throughout the year. We normally try to cap the number of vendors we include to about 10-12 vendors. Sometimes, however, in highly crowded markets we need to include a larger number of vendors.

Copyright © March 2019, 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, EDR, CASB, reputation networks, threat intelligence management and reporting, forensic analysis and more. Some of the leading players in this market are *Carbon Black, 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 $4.3 billion in 2019, to over $9.4 billion by 2023.

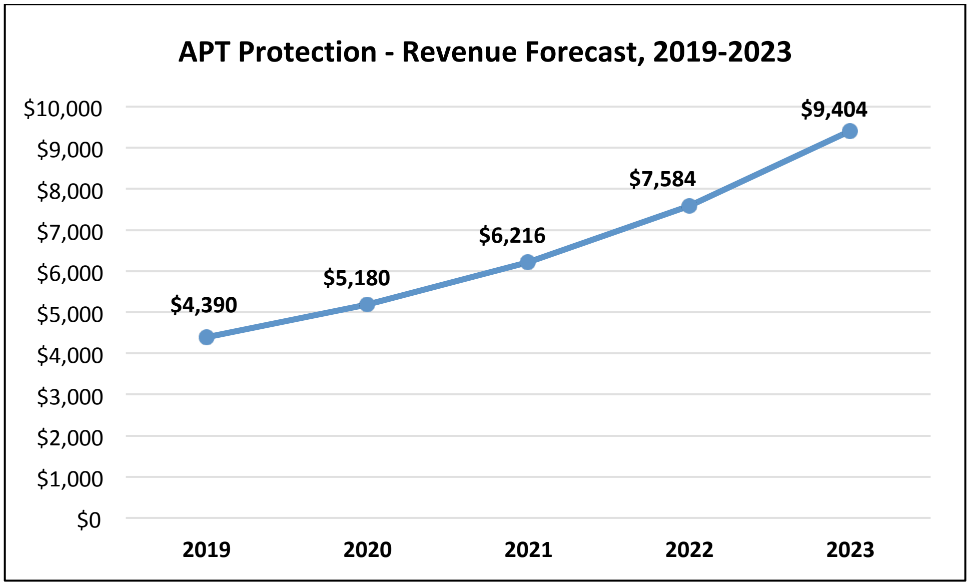

Figure 2: APT Protection Market Revenue Forecast, 2019 – 2023

Copyright © March 2019, 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.

- *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.

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

- *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.

In addition, for all vendors we consider the following aspects:

- *Pricing* – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a "good value".

- *Customer Support* – is customer support adequate and in line with customer needs and response requirements.

- *Professional Services* – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

Note*: On occasion, we may place a vendor in the Top Player or Trail Blazer category even if they are missing one or more features listed above, if we feel that some other aspect(s) of their solution is particularly unique and innovative.*

MARKET QUADRANT – APT PROTECTION

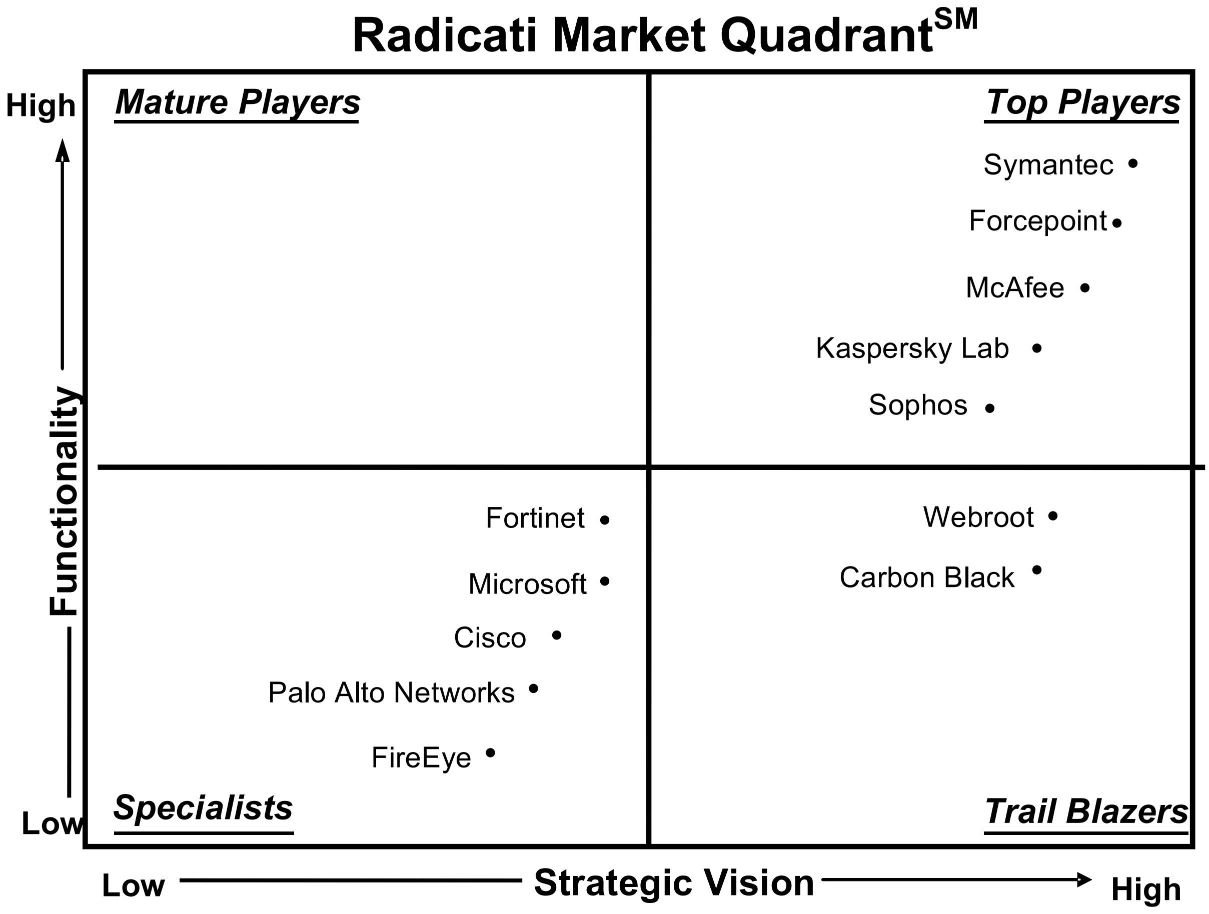

Figure 3: APT Protection Market Quadrant, 2019·

· Radicati Market Quadrant^{SM} is copyrighted March 2019 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants^{SM} should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants^{SM} are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

Key Market Quadrant Highlights

- The **Top Players** in the market are *Symantec*, *Forcepoint, McAfee, Kaspersky Lab,* and *Sophos***.**

- The **Trail Blazers** quadrant includes *Webroot*, and *Carbon Black*.

- The **Specialists** quadrant includes *Fortinet, Microsoft, Cisco, Palo Alto Networks,* and *FireEye*.

- 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. Symantec's security solutions are powered by its *Global Intelligence Network,* which offers 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:

- ***Symantec Endpoint Detection and Response (EDR)*** – exposes advanced attacks through machine learning and global threat intelligence. It utilizes advanced attack detections at the endpoint and cloud-based analytics to detect targeted attacks such as breach detection, command and control beaconing, lateral movement and suspicious power shell executions. It allows incident responders to quickly search, identify and contain all impacted endpoints while investigating threats using a choice of on-premises and cloud-based sandboxing. In addition, continuous and on-demand recording of system activity supports full endpoint visibility. Symantec EDR also provides automated investigation playbooks and user behavior analytics which make best practices accessible to any organization at lower costs. Symantec EDR 4.0 allows customers to use EDR for incident response and threat hunting across Symantec Endpoint Protection (SEP) and non-SEP endpoints. Symantec EDR Network Sensor provides inbound and outbound traffic threat prevention and detection at the network layer, and sends events to Symantec EDR for correlation with endpoint and email events.

- ***Symantec Email Threat Detection and Response (TDR)* –** 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. Email TDR sends events to Symantec EDR for correlation with endpoint and network events.

- ***Symantec Managed Endpoint Detection and Response service (MEDR)*** – is a service delivered by Symantec SOC experts who utilize Symantec EDR, Symantec SOC Technology Platform big data analytics, and Symantec Global Intelligence Network correlation to detect, investigate, and respond to advanced threats. Symantec SOC analysts are assigned to customers based on industry and region and can perform: managed threat hunting, remote investigations, and pre-authorized remediation.

- ***Symantec ProxySG appliance, Secure Web Gateway Virtual Appliance, or Cloud Service* –** are solutions that serve to block known threats, malicious sources, risky sites, 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 Web Isolation also integrates with ProxySG Appliances and Cloud Service to protect end-users from zero day, unknown and risky sites by executing code, and potential malware, from websites remotely.

- ***Symantec Content Analysis*** – analyzes and mitigates unknown content by automatically inspecting files from ProxySG, Symantec Messaging Gateway, Symantec Endpoint Protection or other sources using multiple layers of inspection technology (reputation, dual anti-malware engines, static code analysis, advanced machine learning, and more). It then brokers suspicious content to the Symantec sandbox or other sandboxes. Content Analysis is 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 Web Isolation*** – executes web sessions away from endpoints, sending only safe rendering of information to users' browsers thereby preventing any website-delivered, zero-day malware from reaching devices. When combined with Secure Web Gateways, policies allow isolating traffic from uncategorized sites or URLs with suspicious or unsafe risk profiles. Web Isolation also isolates links in email to prevent phishing threats and credential attacks.

- ***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. It can be deployed as an appliance, virtual appliance or in the cloud, providing full visibility and forensics for cloud workloads. It can also examine encrypted traffic when coupled with the Symantec SSL Visibility solution. Intelligence is used to investigate and remediate the full scope of the attack. Integrations with EDR solutions, including Symantec EDR 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 Managed Network Forensics (MNF)*** – is a service provided by Symantec Managed Security Services (MSS) for MSS Advanced Security Monitoring customers. In response to key indicators, Symantec MSS analysts remotely connect to the customer's Symantec Security Analytics to investigate suspicious activities and provide greater incident detail and context for fast incident response.

- ***Symantec Global Intelligence Network (GIN)*** – provides a centralized, cloud-based, threat indicator repository and analysis platform. It enables the discovery, analysis, and granular classification and risk-level rating 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.

STRENGTHS

- Symantec offers on-premises, cloud, and hybrid options across most of its solutions, which delivers an integrated product portfolio that defends against threats across all vectors, including endpoint, network, web, email, mobile, cloud applications, and more.

- Symantec uses a wide array of technologies 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, customized sandboxing and payload detonation technologies to uncover zero-day threats.

- 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 Web Isolation (obtained through the Fireglass acquisition) provides a safe browser experience by isolating malicious code and preventing it from executing in the end user's browser.

- Symantec Security Analytics, coupled with Symantec SSLV Visibility solution, delivers enriched packet capture for network security visibility, advanced network forensics, anomaly detection and real-time content inspection, even in encrypted traffic.

- Symantec delivers dedicated mobile device protection and analyzes 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 customer base, which provides Symantec products with on-demand real-time URL and file disposition.

- Symantec EDR provides a single pane of glass across all its modules, providing real-time visibility into attacks, as well as the ability to remediate threats across endpoints.

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 and Symantec's Managed EDR and Managed Network Forensics Services help organizations with limited in-house resources and skillsets.

- Symantec EDR customers we interviewed indicated, that while feature-rich, the product can be somewhat 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. Forcepoint offers a systems-oriented approach to insider threat detection and analytics, cloud-based user and application protection, next-gen network protection, data security and systems visibility.

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 appliance. It provides file and email URL sandboxing, detailing forensic reporting and phishing education. All Forcepoint products work together to focus 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.

- **Forcepoint Behavioral Analytics (BA)** – enables security teams to proactively monitor for high risk behavior by leveraging structured and unstructured data to provide visibility into human activity, patterns, and long-term trends that may comprise human risk.

- **Forcepoint Insider Threat** – is a user activity monitoring solution used to protect organizations from data theft, fraud, and sabotage originating from employees and other insiders. It provides deep collection capabilities including keystrokes and video of high risk activity providing security teams context and visibility into user intent.

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 Behavior Analytics (BA), enables security teams to proactively monitor for high-risk behavior inside the enterprise.

- 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.

WEAKNESSES

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

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. In 2017, McAfee acquired Skyhigh Networks, a leading CASB provider.

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:

- McAfee Network Security Platform (IPS)
- McAfee Enterprise Security Manager (SIEM)
- McAfee ePolicy Orchestrator (ePO)
- McAfee Endpoint Solutions
- McAfee Active Response (EDR)
- McAfee Web Gateway
- McAfee Threat Intelligence Exchange

These integrations operate directly or 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.

- 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 does integrate with third party email solutions to provide file attachment analysis.

- Cloud deployment is not currently available on AWS.

- 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. However, management and protection for iOS and Android devices is provided through McAfee MVISION Mobile.

- For remediation, McAfee Active Response initiates several actions (e.g. blocking, cleaning up malware, and quarantining endpoints), however, it does not rollback to a known good state. However, rollback remediation is provided through McAfee MVISION Endpoint.

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 to protect businesses, critical infrastructure, governments and consumers around the globe. 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

Kaspersky Lab’s **Threat Management and Defense** portfolio comprises of the following solutions:

- **Kaspersky Anti-Targeted Attack platform (KATA)** – is a network-level solution that helps rapidly discover threat traces and correlates multi-vector attacks into a single picture.

- **Kaspersky Endpoint Detection and Response (KEDR)** – is an agent-based solution that provides advanced endpoint detection, investigation and reaction capabilities.

- **Threat Intelligence Portal** – is a cloud-based portal providing access to Kaspersky Lab's threat knowledge base, legitimate objects and the various relationships between them.

- **Kaspersky Endpoint Security (KES)** – a multi-layered endpoint protection platform.

- **Kaspersky Secure Mail Gateway (KSMG)** – augments advanced detection scenarios with rapid prevention of email-based threats. It is due for release in Q3 2019.

- **Kaspersky Web Traffic Security (KWTS)/Secure Web Gateway (KSWB**) - augments advanced detection of web-based threats with automated prevention. It is due for release in Q3 2019.

- **Kaspersky Private Security Network (KPSN)** – is a threat intelligence database for organizations with isolated networks, strict policies of data-sharing and regulatory compliance.

- **Cybersecurity Services** – provides access to a global knowledge base of threats, training for specialists, as well as round-the-clock analysis of information security events and prompt response to incidents helping organizations quickly detect malicious acts and prevent future attacks.

The Kaspersky Anti-Targeted Attack Platform (KATA) and Kaspersky Endpoint Detection and Response (KEDR) products are designed to deliver the following functionality:

- o *Network Analysis* – multiple sensors to detect activities at multiple areas of the customer's IT environment. This provides 'near real-time' detection of complex threats and advanced persistent threats (APT).

    - ▪ 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.

- *Machine Learning engine (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, machine learning techniques and access to Global Threat Intelligence to ensure swift detection of abnormal and suspicious behavior.

- *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* – 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.

- *Web Security* – integration with Kaspersky Web Traffic Security allows to perform web-prevention based on advanced detection scenarios.

- *Endpoint Protection* – unified management of threats discovered and prevented by Kaspersky Endpoint Security and Kaspersky Endpoint Detection and Response, 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* – Kaspersky Anti Target Attack fully integrated with the Kaspersky Security Mail Gateway product, allowing it to block email threats.

- *Expertise Sharing and Knowledge Management* – provides access to a global knowledge base of threats, training for specialists, as well as round-the-clock analysis of information security events and prompt response to incidents helping organizations quickly detect malicious acts and prevent future attacks.

- *3rd party integration* – to assist with incident response and post-attack investigations Kaspersky Anti Targeted Attack Platform supporting verdicts sharing through CEF/Syslog with the customer's SIEM (Security Information and Event Management) system or OpenAPI which supports integration scenarios with Next Generation Firewall, Web Gateways and other security systems.

STRENGTHS

- Kaspersky Anti Target Attack (KATA) platform 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 Anti Targeted Attack (KATA) and Kaspersky Endpoint Detection and Response (KEDR) interface with Kaspersky Lab's traditional Endpoint Security solutions.

- Kaspersky Anti Targeted Attack (KATA) and Kaspersky Endpoint Detection and Response (KEDR) integrate with automated, updated context-based data from Kaspersky Lab experts to help better investigate and understand the nature and complexity of attacks.

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

- 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 false alerts.

- The use of the same console and server architecture in Kaspersky Anti Targeted Attack (KATA) and Kaspersky Endpoint Detection and Response (KEDR) provide security officers with seamless workflows during the incident response process.

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

WEAKNESSES

- Kaspersky Lab's Anti Targeted Attack Platform (KATA) is geared mainly for on-premises deployments. However, the current version does support installation in VMware ESXi environments for MSSP deployment scenarios.

- Kaspersky Lab's Anti Targeted Attack Platform (KATA) currently integrates with the Kaspersky Email Gateway for detection and prevention, but only integrates with the Kaspersky Secure Web Gateway for detection. Integration with the Kaspersky Secure Web gateway for network prevention is on the vendor's 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 (KATA) 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.

SOPHOS

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

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

SOLUTIONS

Sophos offers a set of complementary solutions for APT, which comprise: **Sophos SG UTM & XG Firewall,** for network protection, **Sophos Endpoint Protection** for workstations and mobile devices, and **SophosLabs** which provides unified threat intelligence across all platforms. Sophos also offers **Intercept X**, a signature-less next generation endpoint protection product which has been integrated into the existing endpoint protection solution. Sophos Intercept X can be deployed alongside competing AV products, or combined with Sophos Endpoint Protection into a single agent and product, called **Intercept X Advanced**. In addition, **Intercept X Advanced with EDR** includes Endpoint Detection and Response functionality.

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

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

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

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

Cleanup and quarantine capabilities are provided to neutralize detected threats and help return users' systems to a clean state.

- **Sophos Intercept X Advanced with EDR** – integrates intelligent endpoint detection and response (EDR) with deep learning malware detection, exploit protection, and the features included in Sophos Endpoint Protection, into a single agent.

- **SophosLabs** – 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 also offers Sophos Firewall-OS (SF-OS) that 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 UTM Advanced Threat Protection so that when it sees malicious traffic from an endpoint, it can engage Endpoint Protection to verify and clean up the infection. The SF-OS comes preinstalled on Sophos XG Firewall Series appliances.

STRENGTHS

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

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

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

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

- Sophos offers 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

- While Sophos APT solutions' forensic analysis capabilities are used within the product for automated detection and remediation, only customers of Intercept X Advanced with EDR have access to the full available forensic information.

- 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-yourself controls.

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

- Sophos does not offer CASB capabilities, or integrate with third party CASB solutions.

TRAIL BLAZERS

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. In February 2019, Webroot announced that it is being acquired by Carbonite, a provider of cloud backup and recovery solutions.

SOLUTIONS

Webroot offers business security products for endpoints, networks and user cyber-security awareness training. These cloud-based solutions offer a high degree of automation and ease of use, and are purpose designed for the MSP and SMB markets.

Webroot Endpoint Protection is a real-time, cloud-based approach to preventing malware. It is compatible with Microsoft Windows PCs, Laptops and Servers. It is also deployed on Terminal Servers and Citrix; VMware; VDI; Virtual Servers and point of sale (POS) systems. Webroot's endpoint 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 anti-malware approaches there are few local definitions or signatures deployed, and no management issues with ensuring that endpoints are properly updated.

Webroot solutions leverage real-time intelligence, based on advanced machine learning and behavior-based heuristics from Webroot BrightCloud Threat Intelligence, to detect, analyze, categorize, score, and highly accurately predict the threats each individual endpoint is experiencing.

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.

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

STRENGTHS

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

- The Webroot Platform uses machine learning, maximum entropy discrimination (MED) Big Data processing techniques, coupled with high computational scalability and actionable security intelligence to prevent, detect and protect devices from 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 secure auto-remediation using propriety monitoring, journaling, and journaling roll-back. If 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.

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.

- 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 currently provide direct integration with Active Directory services, but does offer AD mirroring in its management console. AD integration is on the vendor's roadmap.

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

- Webroot was recently acquired by Carbonite, as with any acquisition, it is yet too early to determine what effect this will have on company direction.

CARBON BLACK

1100 Winter St.
Waltham, MA 02451
www.carbonblack.com

Carbon Black is a provider of next-generation endpoint security. The company leverages its big data and analytics cloud platform, the CB Predictive Security Cloud, to enable customers to defend against advanced cyber threats, including malware, ransomware, and non-malware attacks. Carbon Black is publicly traded.

SOLUTIONS

CB Predictive Security Cloud is a next generation endpoint protection platform that consolidates security in the cloud, making it easy to prevent, investigate, remediate, and hunt for threats from a single endpoint agent, console, and data set. It offers the following modules which can be managed through the same user interface, with a single login:

- **CB Defense** – delivers next-generation antivirus (NGAV) and endpoint detection and response (EDR) functionality.

- **CB ThreatHunter** – is a threat hunting and incident response solution delivering unfiltered visibility for security operations center (SOC) and incident response (IR) teams. The CB Predictive Security Cloud captures and stores all OS events across every individual endpoint. Leveraging this unfiltered data, CB ThreatHunter provides immediate access to a complete picture of an attack at all times, reducing investigation time. CB ThreatHunter enables teams to proactively hunt for threats, as well as uncover suspicious and stealthy behavior, disrupt active attacks and address potential defense gaps. It allows organizations to respond and remediate in real-time, stopping active attacks and quickly repairing damage.

- **CB LiveOps** – is a real-time security operations solution that enables organizations to ask questions of all endpoints and take action to instantly remediate issues. It closes the gap between security analysis and IT operations by giving administrators visibility into precise details about the current state of all endpoints, enabling them to make fast decisions to reduce risk.

- **CB ThreatSight** – is a managed service for CB Defense that provides a team of Carbon

Black security experts who work side-by-side with customer organizations to help validate and prioritize alerts, uncover new threats, and accelerate investigations.

- **CB Defense for VMware** – is a cloud-delivered security solution for protecting applications deployed in virtualized data centers.

Carbon Black solutions are delivered as cloud services, however, the vendor also offers solutions for customers which may have on-premises needs. Carbon Black supports all leading OS platforms, including Windows, macOS, and Linux.

STRENGTHS

- Carbon Black offers its solution through a multi-tenant cloud platform, which makes it easier for customers to consume its services while benefiting from broad real-time threat analysis across a wide number of endpoints.

- Carbon Black offers strong prevention based on streams of activity delivered via unfiltered data collection, which enables the Predictive Security Cloud to perform well-informed analysis to detect new attack patterns and deploy new logic to stop malicious activity.

- Carbon Black Predictive Security Cloud, allows customers to choose which product modules are right for their organization. All modules are easily deployed through the same user interface and agent.

- Carbon Black offers an extensible architecture based on open APIs, which allows partners and customers to easily extend and integrate with existing security components.

WEAKNESSES

- Carbon Black Predictive Security Cloud does not currently offer some traditional endpoint protection functionality, such as firewalls, mobile security, or DLP. However, provision of a managed OS firewall is on the vendor’s roadmap, and custom integrations are possible through the platform’s open APIs.

- Carbon Black Predictive Security Cloud does not currently provide device control. This is on the vendor’s roadmap.

- The Carbon Black Predictive Security Cloud platform does not yet provide application whitelisting capabilities. Carbon Black currently offers this through its on-premises application control product, CB Protection.

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 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 empowered by global threat intelligence, 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 (AWS, Azure, GCP, and OCI**)**, 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, native public cloud (e.g. Azure, and AWS), and SaaS (hosted 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. It blocks unknown application attacks through integrated behavioral-based AI. FortiWeb is offered as a physical, virtual, and container appliance, public cloud (e.g. Azure, AWS, Google, and Oracle) and SaaS (hosted service).

- **FortiClient Endpoint Protection** – offers a centrally managed endpoint client protection for desktops, laptops, tablets and smartphones on a variety of OS such as Windows, macOS, Linux, Chromebook, iOS, and Android. It includes a standard set of EPP capabilities with next generation capabilities such as anti-exploit protection, UEBA/EDR, and sandbox integration. In addition, it integrates with FortiGate to provide seamless network-endpoint visibility, audit, one-click or automated remediation, and an end-to-end VPN solution.

- **FortiSandbox** – is a homegrown sandbox solution that sits at the core of Fortinet's ATP solution. It takes a two-step approach to analyzing suspicious files. In the first stage, known and emerging threats are identified through patented Compact Pattern Recognition Language (CRPL) anti-malware engine, global intelligence query and code emulation. Dynamic analysis is performed in the second stage where objects are executed in a simulated environment based on Windows, macOS, Linux or Android to uncover the full attack lifecycle. Organizations can choose between built-in tested VMs or upload of custom VMs for their simulated environment. There are also a number of forensic tools built-into the time-driven analysis reports, such as access to captured packets, samples, tracer logs, screenshots, and interactive sandbox mode.

  FortiSandbox can be deployed standalone to sniff all traffic, scan file repositories, allow on-demand submission, and accept blind carbon copy emails.

  Organizations who prefer a centralized zero-day intelligence hub can integrate FortiSandbox at the core of their security architecture by natively integrating with the Fortinet portfolio (i.e. FortiGate, FortiMail, FortiWeb, FortiProxy, FortiADC, and FortiClient), Fortinet Fabric partners (e.g. CarbonBlack, SentinelOne, Ziften, and more), as well as third party solutions via JSON API and ICAP. Local threat intelligence generated from FortiSandbox is shared across these integrated devices in real-time to automate protections against newly discovered threats. Optionally, intelligence packages can be manually downloaded and are STIX compatible.

Organizations can combine both FortiSandbox standalone and integrated modes to cover a wider set of use-cases. FortiSandbox is offered as a hardware and virtual appliance, SaaS (hosted) as well as natively in the public cloud (AWS and Azure).

- **FortiGuard Labs** – is Fortinet's global threat intelligence team, which leverages in-house tools and technologies, develops new services and technologies (e.g. anti-exploit, virus outbreak, content disarm and reconstruction, and more), publishes zero-day research, and plays an active role in various intelligence partnerships including the Cyber Threat Alliance, and several global and federal cyber security authorities.

STRENGTHS

- Fortinet solutions available in a wide variety of form factors, including physical and virtual appliance, SaaS (hosted service) and natively in Public Cloud (e.g. AWS, Azure, and others), 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 Fabric 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 shared in real-time with integrated Fortinet solutions, Fabric-Ready partners and third party security solutions.

- Fortinet delivers custom security processors and hardware to deliver high performance, thus enabling more scale with better price performance ratio at each inspection point.

- 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 offers separate endpoint protection platform (EPP) and EDR/UEBA solutions. However, full EDR functionality is only available through Fortinet's Fabric-Ready partnerships.

- Fortinet recently launched its own homegrown API-based CASB solution (FortiCASB), which is still a maturing solution.

- FortiSandbox integrated endpoint solutions will block and quarantine threats/endpoint automatically. However, for full reimaging, FortiSandbox sends alerts to FortiSIEM so that a ticket can be submitted to perform endpoint restoration.

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 offers the following solutions in the Advanced Persistent Threat (APT) protection space:

- **Office 365 Advanced Threat Protection (Office 365 ATP)** – is a cloud-based email filtering solution that provides protection against phishing, malware and spam attacks. It offers near real-time protection against high-volume spam campaigns, with DKIM and

DMARC support. It also adds protection against "zero-day" attachments and harmful URL links, 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 365 Enterprise E5, Office 365 Education A5, and Microsoft 365 Business 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.

- *Safe Attachments* – provides zero-day protection against unknown malware and viruses. Suspicious messages and attachments are routed to a special environment where machine learning and analysis techniques are used to detect malicious intent. If no suspicious activity is detected, the message is released for delivery to the mailbox.

- *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.

- **Windows Defender Advanced Threat Protection (Windows Defender ATP)** – is an endpoint protection platform designed to prevent, detect, investigate, and respond to advanced threats. It is available with Windows 10 Enterprise E5, Windows 10 Education E5, or Microsoft 365 E5 plans. It uses technology built into Windows 10 and Microsoft cloud services to provide:

  - *Endpoint behavioral sensors* – sensors embedded in Windows 10, collect and process behavioral signals from the operating system and send sensor data to private, cloud instances of Windows Defender ATP.

  - *Cloud security analytics* – leverages machine-learning across the across the entire Microsoft Windows ecosystem to deliver insight, detection, and recommended responses to advanced threats.

  - *Threat intelligence* – leverages threat intelligence collected by Microsoft, security teams, and augmented by threat intelligence provided by partners, to enable Windows Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are detected.

- **Azure Advanced Threat Protection (Azure ATP)** – is a hybrid solution which offers similar functionality to Advanced Threat Analytics (ATA) and serves to protect organization's on-premises networks. It parses network traffic via on-premises ATP sensors, and sends all parsed data to the Azure cloud for analysis and reporting. All information is presented in the cloud by the Azure ATP workspace portal. It is available with Enterprise + Mobility Suite E5.

- **Microsoft Advanced Threat Analytics (ATA)** – is 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.

Microsoft also offers its advanced threat protection technologies in a single package called **Microsoft 365 Identity & Threat Protection** which combines Microsoft Threat Protection (comprising Azure ATP, Windows Defender ATP, and Office 365 ATP) with Microsoft's CASB offering Cloud App Security, and Azure Active Directory. The Identity & Threat Protection package functionality is available as part of the Microsoft 365 E5 suite, or as an add-on package to other suites.

STRENGTHS

- Microsoft ATP solutions come bundled free of charge with some Microsoft Office 365 plans, or are a low-cost add-on 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.

- Microsoft ATP cloud-based solutions are easy to deploy, and manage for customers of all sizes.

- Microsoft Windows Defender ATP 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.

CISCO

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

Cisco is a leading vendor of Internet communication and security technology. Cisco has invested in a number of acquisitions over the last four years, including OpenDNS, Cloudlock, Sourcefire, Cognitive, ThreatGrid. In 2018, Cisco acquired Duo Security, a provider of unified access security and multi-factor authentication. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), made up of leading threat researchers. Cisco is publicly traded.

SOLUTIONS

Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-managed endpoint security solution designed to prevent cyberattacks, 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 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 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.

Cisco also has 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.
- 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-premises 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 does not offer sandbox support for iOS and macOS.

- Cisco AMP for Endpoints does not provide content-aware DLP functionality.
- Cisco AMP for Endpoints will appeal mostly to large and mid-size customers with complex endpoint protection needs and adequate IT management teams.

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. Palo Alto Networks is publicly traded.

SOLUTIONS

WildFire is Palo Alto Networks' sandboxing anti-APT technology. It integrates with Palo Alto Networks' on-premises or cloud Next Generation Firewall (NGFW) product line. WildFire is available as subscription cloud service, or as a private cloud through the WF-500 appliance. 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 uses a threat intelligence prioritization feature called AutoFocus, which combines automated analysis with human intelligence from its Unit42 threat research team.

WildFire 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.

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

- o *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.

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.

FIREEYE

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

FireEye, founded in 2004, offers solutions to simplify, integrate and automate 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, FireEye offers managed detection and response services, incident response services, threat intelligence and deep security forensics. FireEye is a publicly traded company.

SOLUTIONS

FireEye’s solutions portfolio comprises the following components:

- **FireEye Helix** – FireEye Helix is a security operations platform that allows organizations to take control of any incident from alert to fix. FireEye Helix integrates disparate security tools and augments them with advanced SIEM, orchestration and threat intelligence capabilities.

- **FireEye Network Security & Forensics** – 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 combines high performance network data capture and retrieval, with centralized analysis and visualization. FireEye Network Security offers several different deployment options including physical or virtual appliance, on-premises, FireEye hosted (Cloud MVX), or private cloud-based.

- **FireEye Endpoint Security** – brings front-line intelligence and experience to the endpoint, using multiple combined protection engines to block malware and exploits. The solution detects advanced attacks that bypass protection and enables response with tools and techniques developed by frontline responders. Included are four engines in one agent for protection from common and advanced threats and visibility into the threats that have breached protection with response capabilities for systems across the organization, both on and off the network.

- **FireEye Email Security** – is a secure email gateway (cloud edition) that stops email-borne threats with first-hand knowledge of attacks and attackers. Organizations can consolidate their email security stack with a comprehensive, single-vendor solution that blocks malware and suspicious URLs, as well as phishing, impersonation techniques and spam. It is also available as an on-premises solution.

- **FireEye File Protect** – enables scanning file shares (Sharepoint and One Drive currently) 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 Security suite bundles the Helix, Email Security, Endpoint Security and Network Security components into a single offering aimed to ease adoption by mid-market customers. FireEye also leverages its Mandiant and iSIGHT acquisitions to offer customized subscriptions and professional services for threat intelligence, threat prevention, detection, analysis, and response. 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-premises appliances, virtual appliances, as well as in the cloud (through Amazon AWS).

- FireEye offers 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.

- FireEye Network, Email, and File Protect 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, containment, and orchestration, but not automated remediation.

- 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 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.

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 © March 2019, 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, 2019-2023	Mar. 2019	$3,000.00
Social Networking Statistics Report, 2019-2023	Feb. 2019	$3,000.00
Instant Messaging Statistics Report, 2019-2023	Jan. 2019	$3,000.00
Mobile Statistics Report, 2019-2023	Jan. 2019	$3,000.00
Endpoint Security Market, 2018-2022	Nov. 2018	$3,000.00
Secure Email Gateway Market, 2018-2022	Nov. 2018	$3,000.00
Cloud Access Security Broker (CASB) Market, 2018-2022	Nov. 2018	$3,000.00
Enterprise DLP Market, 2018-2022	Nov. 2018	$3,000.00
Microsoft SharePoint Market Analysis, 2018-2022	Jun. 2018	$3,000.00
Corporate Web Security Market, 2018-2022	Jun. 2018	$3,000.00
Email Market, 2018-2022	Jun. 2018	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2018-2022	Jun. 2018	$3,000.00
Cloud Business Email Market, 2018-2022	Jun. 2018	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Information Archiving Market, 2019-2023	Mar. 2019	$3,000.00
Unified Endpoint Management Market, 2019-2023	Apr. 2019	$3,000.00
Advanced Threat Protection Market, 2019-2023	Apr. 2019	$3,000.00

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

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

Copyright © March 2019, The Radicati Group, Inc. Reproduction Prohibited