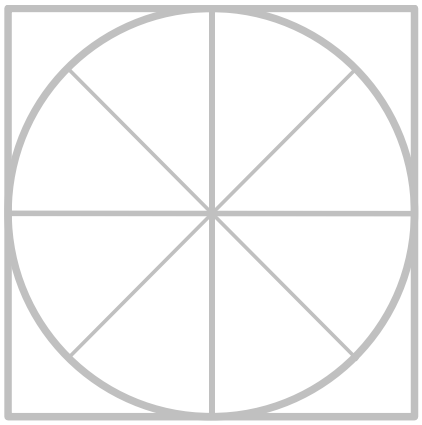
The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Advanced Persistent Threat (APT) Protection - Market Quadrant 2020 *



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

March 2020

TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED

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

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

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

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

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

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

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

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

b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.
c. Companies in this stage will either find new life, reviving their R&D efforts and move back into the Top Players segment, or else they slowly fade away as legacy technology.

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

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

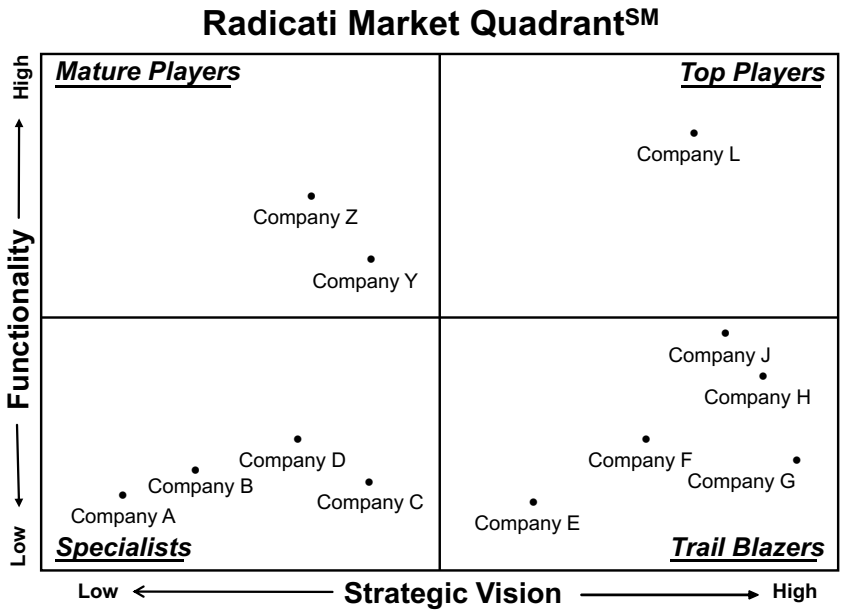


Figure 1: Sample Radicati Market Quadrant

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.

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 *Cisco, ESET, FireEye, Forcepoint, Fortinet, Kaspersky, McAfee, Microsoft, Palo Alto Networks, Sophos, Symantec,* and *VMware Carbon Black.*

- 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 nearly $5.2 billion in 2020, to over $10.5 billion by 2024.

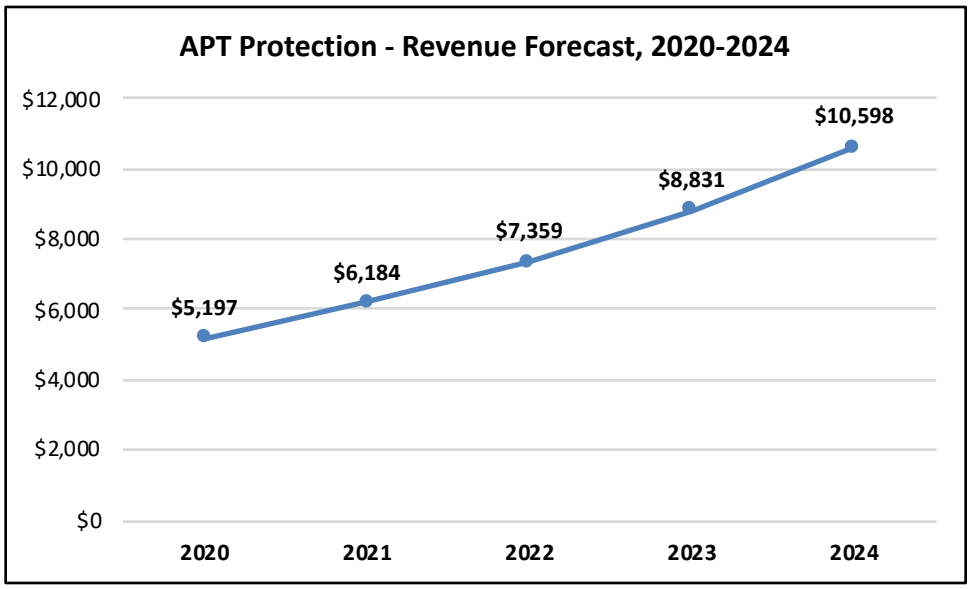


Figure 2: APT Protection Market Revenue Forecast, 2020 – 2024

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 threat sources.

- *Remediation* – refers to the ability to contain incidents, automatically remove malware, and restore endpoints and all affected resources to a pre-incident working state, as well as the

ability to issue software updates. Many vendors define remediation as just blocking and/or quarantining threats without re-imaging of compromised devices. While this is an important first step, it is not sufficient and remediation should also include re-imaging or restoring all devices to their pre-compromised state, or at least the provision of workflows and integration with tools and mechanisms to achieve that.

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

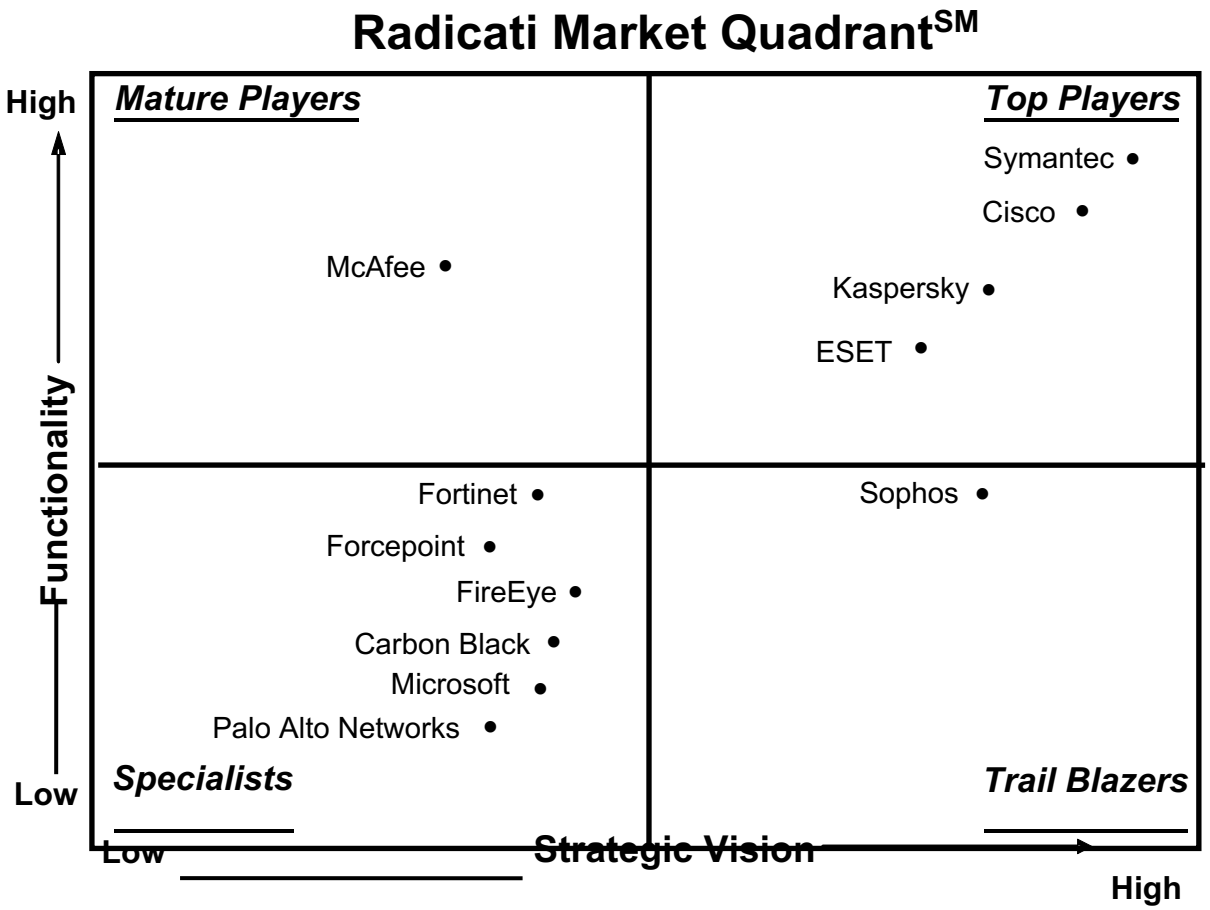


Figure 3: APT Protection Market Quadrant, 2020*

* Radicati Market Quadrant℠ is copyrighted March 2020 by The Radicati Group, Inc. This report has been licensed for distribution. Only licensee may post/distribute. 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*, *Cisco, Kaspersky,* and *ESET.*
- The **Trail Blazers** quadrant includes *Sophos*.
- The **Specialists** quadrant includes *Fortinet, Forcepoint, FireEye, VMware Carbon Black, Microsoft,* and *Palo Alto Networks*.
- The **Mature Players** quadrant includes *McAfee*.

APT PROTECTION - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC, A DIVISION OF BROADCOM

1320 Ridder Park Drive
San Jose, CA 95131
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 division of Broadcom, 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 Security Complete (SESC)*** – is Symantec's new endpoint security offering which provides full endpoint protection, including anti-malware, formerly delivered

by Symantec Endpoint Protection (SEP), plus Endpoint Detection and Response (EDR) capabilities in a single package. SESC 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. SESC also includes application control, breach detection, application isolation, breach assessment, and Active Directory defense.

- ***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 Critical Attack Discovery and Intelligence (CADI) –*** utilizes rich telemetry, cyber-attack experience, and machine learning (ML) to hunt for and discover high-fidelity incidents, alerting customers and identifying the tactics, techniques and procedures (TTPs) used by adversaries. This capability is delivered as an integral part of SESC.

- ***Symantec Threat Hunting Center (STHC)*** – automates threat hunting and uses an intelligence-driven workflow that associates indicators with threat models (actors, threat bulletins, campaigns, TTP, and vulnerabilities) using integrated threat intelligence from open source, commercial, and Symantec intelligence and matches observables with indicators. STHC is able to apply millions of indicators to billions of events and perform retrospective analysis in seconds. It connects to SIEM solutions (e.g. Splunk, Qradar, ArcSight, and others) to help automate threat hunting.

- ***Symantec ProxySG appliance, Secure Web Gateway Virtual Appliance, or Cloud delivered Web Security Service –*** are solutions that serve to block known threats, malicious sources, risky sites, unknown content 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 SSL/TLS encrypted threats across network security appliances, including 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 an on-premises, hybrid or cloud-hosted solution. 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 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 deliver 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. The acquisition of Bay Dynamics should strengthen Symantec's DLP solution with the addition of UEBA.

- Following Broadcom's acquisition of Symantec, CA's Identity and Access Management and Privileged Access Management solutions have been merged into Broadcom's Symantec Enterprise Division. This gives customers the opportunity to include identity protection and management as part of their purchase of the Symantec security portfolio. Integration of Identity Security into the Symantec Integrated Cyber Defense Platform (ICDx) also is on the roadmap.

- 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 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.

- Symantec SECS supports workflows for patch management and remediation, however, it does not currently integrate with Symantec's IMTS (Altiris) product, which is a missed opportunity. The vendor has this on its roadmap.

- Symantec is still working to add UEBA capabilities (from its Bay Dynamics acquisition) to its DLP solution.

- Symantec's recent acquisition by Broadcom has caused it to lose some mindshare among customers. However, the company is addressing this through a number of product and sales channel enhancements.

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, including Duo, OpenDNS, Cloudlock, Sourcefire, Cognitive and ThreatGrid. 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) is a cloud-based anti-malware solution that includes AMP for Endpoints and integrations to an AMP Ecosystem consisting of network/gateway security devices and other cloud-based security solutions. It works using a collective security intelligence cloud to detect, contain, and remediate advanced threats. Cisco AMP for Endpoints agents extend anti-malware capabilities with a protection lattice of next-generation endpoint security capabilities which can be deployed to protect Windows, Macs,

Linux, mobile devices and virtual systems. AMP uses global threat intelligence from Talos and AMP Threat Grid 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, NGAV malware blocking, file sandboxing and offers proactive protection by closing attack pathways before they can be exploited. An exploit prevention engine detects and blocks file-less exploitation techniques that are commonly used to exploit memory corruption vulnerabilities in common applications. Additional capabilities include system process and malicious activity protection, behavior based detection, and protection against ransomware. Using Cloud-based Collective Security Intelligence, AMP's global outbreak control capability ensures that prevention enforced on a malicious file is automatically enforced on the other policy enforcement points in the AMP Ecosystem.

- *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 Intelligence 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 and other policy enforcement points in the AMP Ecosystem without the need to wait for a content update. The Threat Response capability aggregates security telemetry across the AMP Ecosystem architecture: endpoints, network, web, email

and DNS to provide threat context enrichment for proactive threat hunting, incident investigation and response. Endpoint Isolation capability further allows an incident investigator/analyst to isolate the compromised host from network access while retaining a customer configurable list of whitelisted systems, alongside the AMP console, for access to triage or remediate the host.

- *Advanced Search* – AMP provides Threat Hunters, SOC Analysts and Incident Responders efficient information about the endpoints they manage. Security personnel have the ability to run complex queries on any or all endpoints for threat indicators. Advanced search provides deep visibility into what happened on any endpoint at any given time by taking a snapshot of its current state. For ease of use, an endpoint forensic snapshot and/or a catalog of advanced endpoint search queries is mapped to the MITRE ATT&CK framework.

- *File Sandboxing* – Threat Grid console and API access allows security teams to perform in-depth static and advanced dynamic file analysis in order to identify malware quickly in a safe and secure environment. Enhanced capabilities provide Cisco curated playbooks for sandbox runtime and a glove book feature that allows security analysts to interact with the malware in the sandbox during detonation.

- *Zero Trust Security* – AMP integrates with Cisco's DUO to deliver risk-based identity and access. AMP for Endpoints can alert DUO of device compromise. DUO can then automatically block the compromised device from being used for multi-factor authentication.

- *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 Ecosystem products via collective intelligence. If a file is determined to be malicious via AMP for Email or Web Security the information is immediately shared across all AMP-enabled platforms, both for future detection of the malicious file and retrospectively if the file was encountered by any 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 for automatic global outbreak control and trajectory.

- *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, Umbrella DNS roaming protection and Splunk for comprehensive secure mobility. AnyConnect assists with the deployment of AMP for Endpoints and expands endpoint threat protection to VPN-enabled endpoints, as well as other Cisco AnyConnect services. The Web Security and Umbrella modules prevent the endpoint from accessing and downloading content from known malicious URLs and domains. Integration with Splunk allows AnyConnect's network visibility module to send network flow telemetry for analytics and anomalous network activity detection.

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.

Cisco AMP supports open APIs, and an ecosystem of thrid party APT solution integrations.

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 provide features to help uninstall previous security software.

- Cisco AMP for Endpoints currently offers third party software patch assessment, but does not offer third party patch software remediation.

- Cisco AMP for Endpoints does not provide content-aware DLP functionality.

- Cisco AMP for Endpoints will appeal mostly to customers with adequate IT management teams and complex endpoint protection needs, who are already vested in Cisco solutions.

KASPERSKY

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

Kaspersky 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 is privately owned.

SOLUTIONS

Kaspersky's **Threat Management and Defense** portfolio comprises the following solutions:

- **Kaspersky Anti-Targeted Attack (KATA) Platform** – combines network-level advanced threat discovery and Kaspersky Endpoint Detection and Response (EDR) capabilities. It covers multiple threat entry-points (Web, Mail, endpoint, server, virtual machines) delivering fully automated data collection, centralized data storage, and detection at both network and endpoint levels. The platform is enriched through Kaspersky Threat Intelligence and is managed through a single web console.

- **Kaspersky EDR (KEDR)** – can also work as standalone technology, enabling detection of complex threats, deep investigation powered by Kaspersky Threat Intelligence and MITRE ATT&CK mapping, as well as a range of response capabilities. Kaspersky EDR can work alongside third party endpoint security solutions, and shares the same agent as Kaspersky Endpoint Security for Business.

- **Kaspersky Endpoint Security for Business (KESB**) – is a multi-layered endpoint protection platform, that provides security for mixed environments.

- **Kaspersky Secure Mail Gateway (KSMG)** – delivers email-based threat protection and provides an automated response based on in-depth KATA Platform detections.

- **Kaspersky Web Traffic Security (KWTS)** – delivers web-based threat protection and provides an automated response based on in-depth KATA Platform detections.

- **Kaspersky Threat Intelligence Portal** – offers a single access point to threat intelligence, available in both machine-readable and human-readable formats.

- **Kaspersky Private Security Network (KPSN)** – a private threat intelligence database for organizations with isolated networks, or stringent requirements regarding data-sharing and regulatory compliance.

- **Cybersecurity Services** – provide access to global threat intelligence, training programs for specialists, managed detection and response services as well as security and compromise assessments to close security gaps before their exploitation.

The Kaspersky Anti-Targeted Attack (KATA) Platform and Kaspersky EDR (KEDR) products deliver the following functionality:

- *Network traffic analysis (NTA)* – uses network sensors to detect activities in multiple segments of the IT infrastructure, enabling the 'near real-time' detection of complex threats in web and email environments. SMTP, POP3, POP3S, HTTP, HTTPS, ICAP, FTP and DNS protocols are supported. The NTA module features behavior detection capabilities, and analyzes traffic and objects through Intrusion Detection and URL reputation analysis.

- *Sandboxing* – KATA Platform Advanced Sandbox technology provides a safe environment for the analysis of threat activity, helping identify unknown or tailored malware. Results are mapped to the MITRE ATT&CK knowledgebase. The sandbox also provides techniques for OS environment randomization, time acceleration in virtual machines, anti-evasion techniques, user activity simulation, and others, which contribute to behavior-based detection.

- *Kaspersky Security Network (KSN)* – is a global cloud infrastructure holding reputation verdicts and other information about objects processed by the KATA Platform (files, domains, URLs, IP addresses and more). A private cloud based solution, *Kaspersky Private Security Network (KPSN*), is available for organizations unable to send their data to the global KSN cloud but still wishing to benefit a global reputation database.

- *Targeted Attack Analyzer (TAA)* – discovers suspicious actions based on anomaly heuristics, provisioning real-time automated threat hunting capabilities. It supports the automatic analysis of events, and their correlation with a unique set of Indicators of Attack (IoAs) generated by Kaspersky's Threat Hunters. All IoAs are mapped to MITRE ATT&CK to provide detailed information including the ATT&CK-defined technique used, a description and mitigation strategies. Databases of custom IoAs appropriate to the specific infrastructure or the industry sector, can also be created.

- *Anti-malware engine* – working on a central node, with more aggressive settings than are enabled on endpoint configuration, the engine scans objects for malicious or potentially dangerous code, as well as sends objects with potentially malicious contents to the sandbox.

- *Indicators of Compromise (IoCs) scanning* – the KATA Platform allows centralized IoCs loading from threat data sources and supports automatic scheduled IoCs scanning, streamlining the analysts' work.

- *Detection with YARA rules* – supports complex matching rules to search files with specific characteristics and metadata. It also allows the creation and uploading of customized YARA rules in order to analyze objects for threats specific to the organization.

- *Retrospective analysis* – allows retrospective analysis to be conducted while investigating multi-stage attacks, even in situations where compromised endpoints are inaccessible or when data has been encrypted. In addition, saved files from mail and web traffic can be automatically rescanned periodically, applying updated detection rules.

- *Query builder for proactive threat hunting* – Analysts can build complex queries in searching for atypical behavior, suspicious events and threats specific to the infrastructure.

- *Kaspersky Threat Intelligence Portal* – supports manual threat queries to the Threat Intelligence knowledgebase to give IT security analysts' additional context for threat hunting and effective investigation.

- *Third party integration* – KATA Platform supports verdict sharing through CEF/Syslog with the customer's SIEM (Security Information and Event Management) system, or OpenAPI for integration scenarios with Next Generation Firewall, Web Gateways and other security systems.

STRENGTHS

- The Kaspersky Anti Targeted Attack (KATA) Platform incorporates Kaspersky EDR to offer an all-in-one APT Protection Platform based on a unified server architecture and centralized management.

- The use of a single console and server architecture in the Kaspersky Anti Targeted Attack (KATA) Platform and Kaspersky EDR (KEDR) provides security officers with efficient workflows for improved incident response.

- Kaspersky offers flexible implementation (hardware-independent software appliances) with separate network sensors and lightweight endpoint agents.

- The KATA Platform supports the automated comparison of internal investigation results with global reputation data (i.e. through the Kaspersky Security Network), which automatically checks files, URLs, domains, and more, to accelerate the incident investigation process.

- For organizations with strict privacy policies, such as financial services or government agencies, the KATA platform can work in a completely isolated mode, without transferring any data outside the organization's perimeter.

- Kaspersky Managed Detection and Response delivers protection from evasive threats that tend to circumvent existing automatic prevention and detection technologies.

- Kaspersky provides MSSP deployment scenarios with the ability to manage network sensors and thousands of endpoints within a single unified console, supporting both on-premises and hybrid cloud scenarios.

WEAKNESSES

- The Kaspersky Anti Targeted Attack (KATA) Platform is geared mainly to on-premises deployment.

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

- An EDR agent for mobile platforms is not yet available.

- Kaspersky does not offer yet a CASB solution. However, it provides APIs for integration with third party CASB solutions, and is developing a CASB solution aimed at mid-size organizations.

ESET, SPOL. S.R.O.

Einsteinova 24
851 01 Bratislava
Slovak Republic
www.eset.com

ESET, founded in 1992, offers cybersecurity products and services for enterprises, small and medium businesses and consumers. Headquartered in the Slovak Republic, ESET has research, sales and distribution centers worldwide and a presence in over 200 countries. The company is privately held.

SOLUTIONS

ESET's anti-APT product portfolio includes the following solutions:

- **ESET Enterprise Inspector (EEI)** – is ESET's EDR solution. It combines ESET's detection and prevention technologies, threat intelligence and cloud malware protection system with other advanced techniques to monitor and evaluate suspicious processes and behaviors. It can detect policy violations, anomalies, and can provide detailed information and response options in the event of security incidents. It provides multiple options to respond to incidents or suspicious activities.

- **ESET Dynamic Threat Defense (EDTD)** – is ESET's managed cloud sandboxing solution, which provides another layer of protection for ESET Endpoint and Server security solutions. It provides static and dynamic analysis and reputation data, to detect zero-day threats. It is managed by the ESET Security Management Center and integrates directly with ESET Enterprise Inspector, ESET Mail Security solutions and ESET Endpoint solutions.

- **ESET's Threat Intelligence Service** – is ESET's threat reputation network. It uses information gathered from over 110 million sensors that is sent to ESET's Cloud Malware Protection System via ESET LiveGrid®. It shares actionable threat intelligence with customers. Additionally, it provides IOCs (IP, URL, file hash) and serves as an automated malware analysis portal.

- **ESET Threat Hunting** – is a security service delivered by ESET cybersecurity experts who perform an on-demand investigation of data, events and alarms generated by the ESET Enterprise Inspector. This may include root cause analysis, forensic investigations, as well as actionable mitigation advice.

- **ESET Threat Monitoring** – is a security service delivered by ESET cybersecurity experts who continuously monitor customer network and endpoint security data to provide alerts in real time if suspicious activity requires attention. It also provides actionable advice on risk mitigation.

- **ESET Manual Malware Analysis** – is an ESET security service which provides full examination and reverse engineering of submitted files. It also provides detailed reports on malicious code behavior with recommendations for prevention, removal and mitigation of attack impact.

- **Forensic Analysis & Consulting** – is a service which provides manual examination of submitted hardware and investigation by ESET Malware Research experts to provide mitigation suggestions and minimize breach aftermath.

- **ESET Initial Assessment and Optimization** – is a service designed for customers utilizing ESET's Enterprise Inspector (EEI) EDR solution, which further improves protection and detection capabilities based on an initial assessment which results in the optimization of settings, rules and exclusions specifically tailored to a customer's environment.

STRENGTHS

- ESET EEI is a natively on-premise solution, which can be alternatively deployed in AWS and MS Azure instances.

- ESET EEI solution offers strong EDR capabilities which include collection of real time data, including process execution, loading of DLLs, script execution, manipulation of files, registry, network communication, process injections, and more.

- ESET solutions offer multi-language support and a large set of localized versions.

- ESET solutions are well known for ease of deployment and on-going use.

- ESET offers single pane of glass administration of all ESET solutions deployed in the network and controls endpoint prevention, detection and response layers across desptops, servers, agentless virtual machines, and mobile devices.

- ESMC offers remediation/response capabilities through command tasks which include: network isolation, restoring files from backup, file quarantining, file removal, process termination and behavior blocking.

WEAKNESSES

- Currently, some remediation actions require moving from the separate Enterprise Inspector (EEI) console back to the Security Management Center.

- ESET does not currently support macOS or Linux platforms. However, macOS EDR agent integration is on the vendor's roadmap for 2020, whereas Linux agent integration is on a long-term roadmap.

- ESET does not provide its own DLP solution. However, it offers DLP through the ESET Technology Alliance, its partner program.

- ESET does not offer a CASB solution or integrate with third party CASB providers.

- ESET lacks visibility in North America, however the vendor is working on to address this.

TRAIL BLAZERS

SOPHOS

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

Sophos offers IT security solutions for businesses, which include encryption, endpoint, email, Web, next-generation firewall (NGFW), and more. All solutions integrate with Sophos Central, Sophos's cloud-based management platform, and backed by SophosLabs, its global network of threat intelligence centers. The company is headquartered in Oxford, U.K. In March 2020, Sophos was acquired by private equity firm Thoma Bravo, in a move that takes the company private.

SOLUTIONS

Sophos offers a set of complementary solutions for APT, which comprise: **Sophos SG UTM & XG Firewall,** for network protection; **Sophos Intercept X for next-gen Endpoint Protection** for workstations, servers and mobile devices; and **SophosLabs** which provides unified threat intelligence across all platforms. **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 Intercept X Endpoint Protection** – Sophos Intercept X employs a layered approach to endpoint protection, rather than simply relying on one primary security technique. It combines foundational and modern techniques. Modern techniques include deep learning malware detection, exploit prevention, and anti-ransomware specific features. Foundational techniques include signature-based malware detection, behavior analysis, malicious traffic detection, device control, application control, web filtering, data loss prevention, and more.

- **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 Intercept X 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' 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 offers only basic CASB capabilities.

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. 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 can integrate FortiSandbox with the Fortinet portfolio (i.e. FortiGate, FortiMail, FortiWeb, FortiProxy, FortiADC, and FortiClient), Fortinet Fabric partners (e.g. VMware/CarbonBlack, SentinelOne, Ziften, and others), 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 only basic API-based CASB functionality, through its own homegrown FortiCASB 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.

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.

There are currently two types of AMD offerings:

- **AMD Cloud** – is a SaaS solution that integrates out of the box with Forcepoint Web Security, Email Security, CASB, and NGFW products.

- **AMD On Premises** – 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 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.

WEAKNESSES

- 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. Forcepoint AMD can tie into third party EDR solutions only through custom integrations.

- Forcepoint does not offer its own sandboxing technology, but delivers sandboxing through a partnership with Lastline, for best-in-class sandboxing technology.

- Forcepoint has lost market visibility, and is primarily focused on the North American government market.

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 (e.g. Sharepoint and One Drive) 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 offer customized subscriptions and professional services (through its Mandiant and iSIGHT acquisitions) 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 threat 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.

VMWARE 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. In 2019, Carbon Black was acquired by VMware.

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 mobile security, or DLP. However, 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.

MICROSOFT

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

Microsoft provides a broad range of products and services for businesses and consumers, through a 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.

- *ATP for SharePoint, OneDrive and Microsoft Teams* – can be turned on to help detect and block malicious files in team sites and document libraries.

- **Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP)** – is a cloud-based EDR analytics protection and response service designed to help detect, block and remediate zero-day threats. It provides protection against phishing, malware and spam attacks. It can offer 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 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.

- *Managed Detection and Response* – as part of Microsoft Defender ATP, Microsoft also offers **Microsoft Threat Experts**, a managed detection and response (MDR) service which combines targeted attack notification with on-demand SOC expert services. It is available as part of the Microsoft 365 E5 subscription plan.

Microsoft Defender ATP is also available for Mac platforms, while support for Linux platforms is currently available only through partners.

- **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 Defender ATP is a good first step for organizations looking for an entry-level EDR solution.

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 often 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 are included with what plans.

- Microsoft Office 365 customers we spoke to as part of this research, continue to report 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. 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 a subscription cloud service, or as a private cloud solution 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.

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

- *Bare metal analysis* – 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, cloud, or as a private cloud solution. Hybrid deployments are also supported where sensitive files may be processed in the private cloud, whereas other content is analyzed in the cloud.

- 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.

MATURE PLAYERS

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 endpoints, networks, servers, the Cloud and more.

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.

- *Detailed reporting* – provides critical information for investigation including MITRE ATT&CK mapping, disassembly output, memory dumps, graphical function call diagrams, embedded or dropped file information, user API logs, and PCAP information. Threat time lines help visualize attack execution steps

- *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.

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

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

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

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

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

Consulting Services:

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

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

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

MARKET RESEARCH PUBLICATIONS

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

Currently Released:

Title	Released	Price*
Email Statistics Report, 2020-2024	Mar. 2020	$3,000.00
Instant Messaging Statistics Report, 2020-2024	Feb. 2020	$3,000.00
Social Networking Statistics Report, 2020-2024	Jan. 2020	$3,000.00
Mobile Statistics Report, 2020-2024	Jan. 2020	$3,000.00
Endpoint Security Market, 2019-2023	Nov. 2019	$3,000.00
Secure Email Gateway Market, 2019-2023	Nov. 2019	$3,000.00
Cloud Access Security Broker (CASB) Market, 2019-2023	Nov. 2019	$3,000.00
Enterprise DLP Market, 2019-2023	Nov. 2019	$3,000.00
Microsoft SharePoint Market Analysis, 2019-2023	Apr. 2019	$3,000.00
Email Market, 2019-20223	Apr. 2019	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2019-2023	Apr. 2019	$3,000.00
Cloud Business Email Market, 2019-2023	Mar. 2019	$3,000.00
Corporate Web Security Market, 2019-2023	Mar. 2019	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Information Archiving Market, 2020-2024	Mar. 2020	$3,000.00
Advanced Threat Protection Market, 2020-2024	Mar. 2020	$3,000.00
Unified Endpoint Management Market, 2020-2024	Mar. 2020	$3,000.00

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

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

