The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Advanced Persistent Threat (APT) Protection - Market Quadrant 2021 *

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

March 2021

* Radicati Market Quadrant^{SM} is copyrighted March 2021 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^{SM} should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants^{SM} are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED

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

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

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

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

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

    b. Established vendors that offer 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.

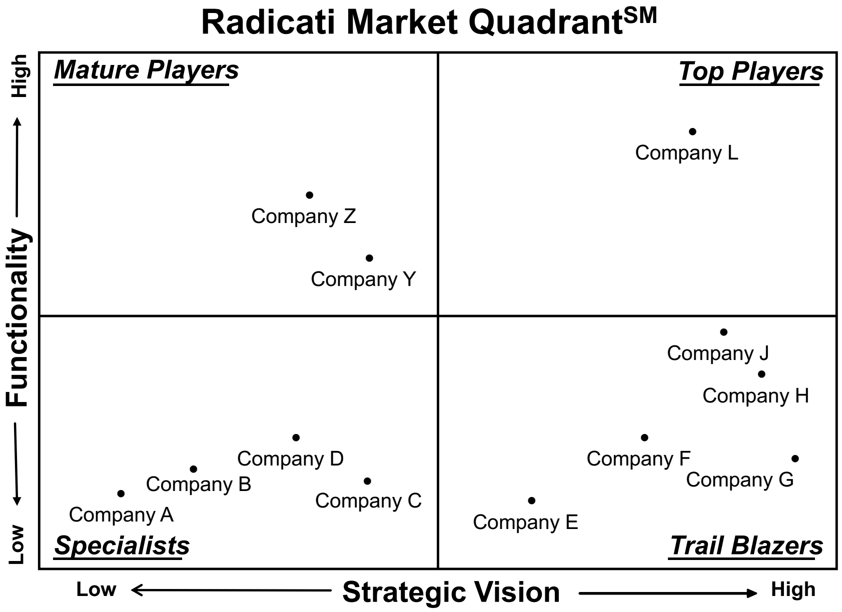

Figure 1: Sample Radicati Market Quadrant

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 *Bitdefender, Cisco, ESET, FireEye, Forcepoint, 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 over $5.9 billion in 2021, to over $12.4 billion by 2025.

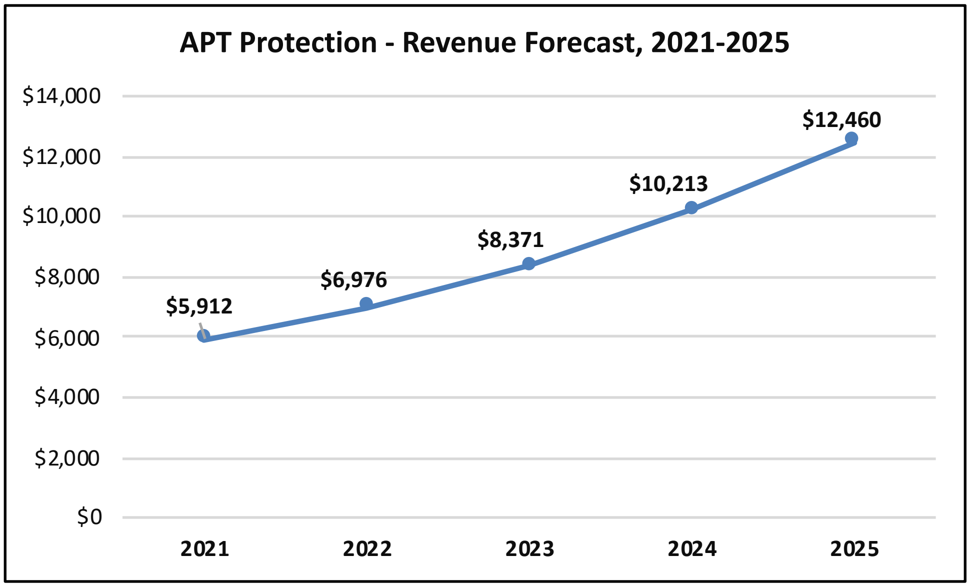

Figure 2: APT Protection Market Revenue Forecast, 2021 – 2025

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

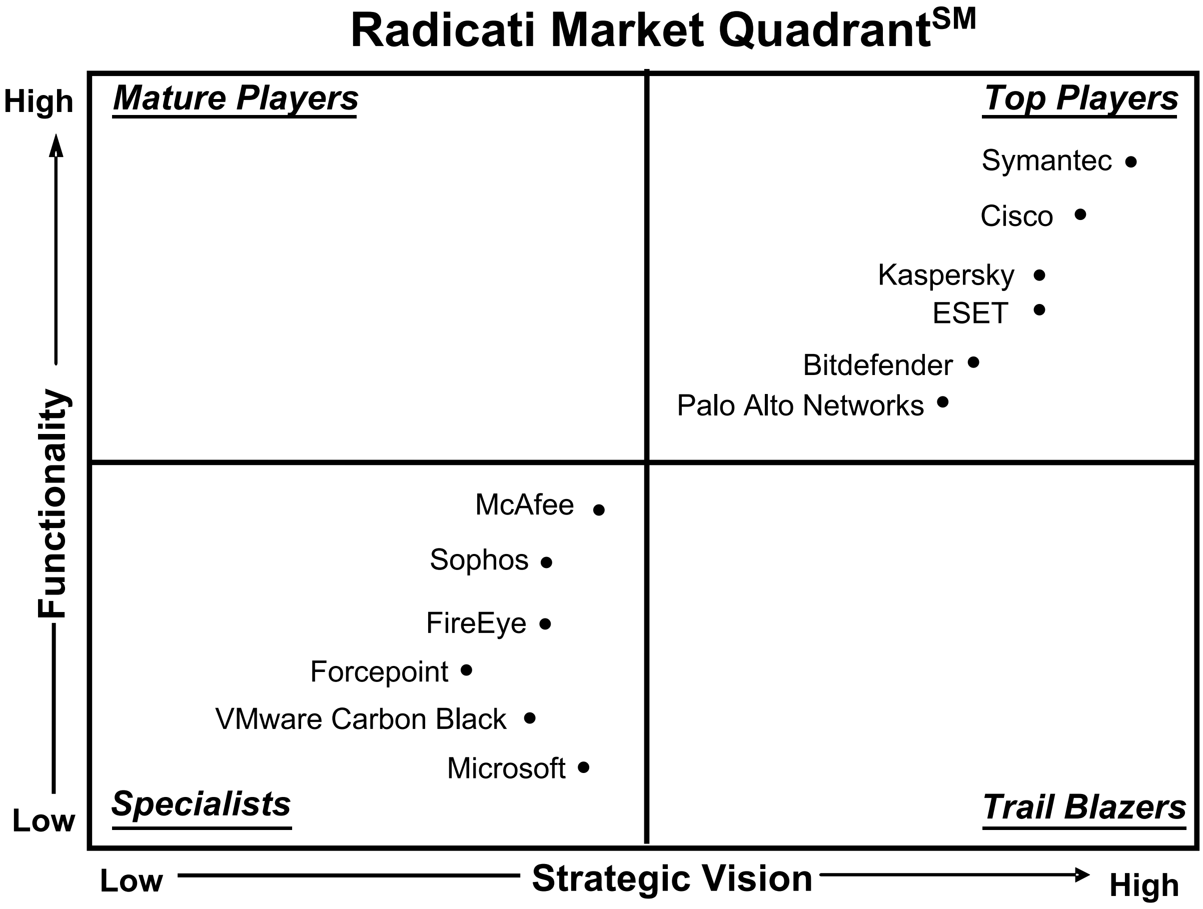

Figure 3: APT Protection Market Quadrant, 2021*

* Radicati Market Quadrant^{SM} is copyrighted March 2021 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^{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*, *Cisco, Kaspersky, ESET, Bitdefender, and Palo Alto Networks***.**

- There are no **Trail Blazers** in this market at this time.

- The **Specialists** quadrant includes *McAfee, Sophos, FireEye, Forcepoint, VMware Carbon Black,* and *Microsoft*.

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

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 network, endpoint and email security 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. Solutions can be delivered on-premises, cloud-based or as hybrid solutions. Symantec's security portfolio comprises the following components:

- ***Symantec Web Protection Suite (enterprise-grade Secure Web Gateway appliances, virtual appliances, or cloud-delivered SaaS service)*** **–** blocks 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 Symantec Proxy to orchestrate malware scanning and application blocking, while Symantec SSL Visibility provides additional visibility into SSL/TLS encrypted threats. Symantec Web Isolation also integrates with Proxy Appliances and the Cloud SWG Service to protect end-users from zero-day, unknown and risky sites by executing code and potential malware remotely and away from the user's browser. SWG appliances along with simplified software subscription licensing, allow customers to support on-premises, in the cloud, or hybrid deployments. Symantec also moved its SaaS SWG solution, Web Security Services, to the Google Cloud Platform, to improve performance, stability and scalability.

- ***Symantec Content Analysis*** **–** analyzes and mitigates unknown content by automatically inspecting files from Symantec Proxy, Symantec Messaging Gateway, Symantec Endpoint Protection or other sources using multiple layers of inspection technology (e.g. reputation, dual anti-malware engines, static code analysis, advanced machine learning, and more). It then brokers suspicious content to the Symantec sandbox, or third party 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 network traffic analysis and full-packet capture, indexing, deep packet inspection (DPI) and anomaly detection to enable incident response and eradicate threats that may have penetrated the network, including 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.

- ***Symantec Endpoint Security Complete (SESC)*** – is Symantec's full-feature endpoint security offering which combines Symantec Endpoint Protection (SEP), Symantec Endpoint Detection and Response (SEDR), Active Directory Defense, and Application Control and Isolation to provide an integrated offering with coverage across all devices, including mobile. SEP upgrades do not require the installation of a new agent. The SEP Agent works with SESC, and can be deployed as cloud managed, on-premises, or a hybrid. 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 breaches, command and control beaconing, lateral movement and suspicious power shell executions. It allows incident responders to quickly search, identify and contain 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 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 Threat Hunter* –** utilizes rich telemetry, cyber-attack experience, and machine learning (ML) to hunt for and discover high-fidelity incidents. Symantec analysts review ML outputs and provide vital insights about potential breaches directly into the SES Complete product console. This information, allows SOC teams to understand the full context of attacks and deploy the specific tactics, techniques and procedures (TTPs) needed to quickly respond to incidents. This capability is delivered as an integral part of SESC.

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 and UEBA solutions that integrate with endpoints, gateways, and cloud applications to prevent data leaks and help achieve industry and regulatory compliance. Symantec owns its own technology for CASB and Web Isolation solutions.

- Following Broadcom's acquisition of Symantec, CA's Identity and Access Management and Privileged Access Management solutions were 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. Symantec continues to integrate CA's Identity Security products into ICDx.

- Symantec Security Analytics, coupled with Symantec SSLV Visibility solution, delivers network traffic analysis and 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 real-time visibility into attacks, as well as the ability to remediate threats across both on-premises or cloud based 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.

- SESC supports workflows for patch management and remediation, however, it does not currently integrate with Symantec's ITMS (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.

- Although the Symantec acquisition by Broadcom initially affected customer mindshare, the company has addressed this in a number of product, service 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 security 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 SecureX – is a cloud-native platform within the Cisco Secure portfolio which combines multiple sensor and detection technologies into a unified location for visibility and provides automation and orchestration capabilities to maximize operational efficiency across network, users, endpoints, cloud, and applications. Cisco Secure customers are entitled to Cisco SecureX at no additional charge with purchase of any SecureX-capable product.

Cisco Secure Endpoint (formerly AMP for Endpoints) – is a core element of the Cisco Secure solution to address APT attacks. It is a SaaS-based APT solution that includes a next generation endpoint security product where deployments are managed from a cloud based management console. There is also an option for on-premise deployment using either a virtual appliance or physical appliance based on Cisco UCS hardware. Cisco Secure Endpoint supports Windows, macOS, Linux, Apple iOS and Google Android.

Secure Endpoint delivers the following functionality:

- *Prevention* – Secure Endpoint combines Global Threat Intelligence, NGAV, exploit prevention, heuristic and behavior analysis to offer proactive protection by closing attack pathways before they can be exploited.

- *Detection* – Secure Endpoint continually monitors all activity on endpoints to identify malicious behavior and detect indicators of compromise. Secure Endpoint offers agentless detection when deployed alongside compatible web proxies (e.g. Cisco Secure Web Appliance, Symantec ProxySG, or other third parties). It helps uncover file-less or memory-only attacks, abuse of LoLBins, web browser only infections, and stop threats before it compromises the OS-level. The built-in SecureX platform extends detection across the security infrastructure for enhanced threat detection context and correlation across multiple threat vectors.

- *Response* – Secure Endpoint offers automated remediation across all endpoints and other policy enforcement points in the Cisco Secure portfolio without the need to wait for a content update. The Threat Response capability aggregates security telemetry across the Cisco Secure architecture: endpoints, network, web, email and DNS to provide threat context enrichment for proactive threat hunting, incident investigation and response. Response actions can range from automatic triage and forensic capture to endpoint isolation.

- *Threat Hunting* – Secure Endpoint provides Threat Hunters, SOC Analysts and Incident Responders efficient information about the endpoints they manage. 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. A managed threat hunting option is also available.

- *Zero Trust Security* – Secure Endpoint's integration with Cisco Secure Access by Duo and Identity Services Engine (ISE) delivers risk-based identity and access controls. Secure

Endpoint can alert Duo and ISE of device compromise. Duo can then automatically block the compromised device from being used for multi-factor authentication to secure applications and systems. ISE can automatically trigger change of authorization policy to network segment compromised endpoints for threat centric network admission control.

- *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. The global outbreak control capability leverages collective intelligence cloud block across all Cisco Secure policy enforcement points, from edge to endpoint.

- *Patch Assessment* – Secure Endpoint identifies vulnerable software on the endpoint and provides a catalog of endpoint posture assessment advanced search queries to rapidly assess patch levels and attack surface.

The **Cisco AnyConnect Secure Mobility Client** offers secured VPN access , endpoint posture enforcement and integration with Cisco Web Security, Umbrella DNS roaming protection and Splunk for comprehensive secure mobility.

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 supports open APIs, and an ecosystem of 3rd party APT solution integrations.

Cisco security portfolio also includes the following capabilities:

Secure Network Analytics (Stealthwatch) – provides enterprise-wide network visibility and applies advanced security analytics to detect and respond to threats in real time. It uses a combination of behavioral modeling, machine learning, and global threat intelligence, to detect threats such as command-and-control (C&C) attacks, ransomware, Distributed-Denial-of-Service (DDoS) attacks, illicit cryptomining, unknown malware, and insider threats.

Cisco Secure Email – provides comprehensive protection for on-premises or cloud-based email by stopping phishing, spoofing, business email compromise, malware and other common cyber threats.

Cisco Secure Cloud Analytics (Stealthwatch Cloud) – provides the visibility and threat detection capabilities you need to keep workloads secure in all major cloud environments like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Cisco Secure Firewall – is available is a variety of form factors (both appliances and virtual appliances) with both on-premise and cloud-based centralized management.

Cisco Umbrella – is a cloud-native, multi-function security service at the core of Cisco's Secure Access Service Edge (SASE) architecture. It unifies firewall, secure web gateway, DNS-layer security, cloud access security broker (CASB), and threat intelligence solutions into a single cloud service to help secure networks.

Cisco Secure Malware Analytics – combines static and dynamic malware analysis with threat intelligence into a single solution delivered through the cloud, as an on-premises solution, or integrated into Cisco security technologies.

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.

- Cisco offers a rich, highly integrated portfolio which combined with its built-in SecureX platform simplifies the security experience and allows organization to unify visibility, detection and response in order to defend against advanced APT attacks.

- Secure Endpoint 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.

- Secure Endpoint has the ability to roll back time on attacks to detect, alert, and quarantine files that become malicious after the initial point of entry.

- Secure Endpoint offers protection, detection and response in a single agent across PCs, Macs, mobile devices, Linux, virtual environments, as well as an on-premises private cloud option.

- Secure Endpoint is fully integrated with the Cisco Secure solutions to further increase visibility and control across an organization.

WEAKNESSES

- While Cisco Secure Endpoint can register with Windows Security Center to disable Defender, it does not currently provide features to help uninstall other third-party security software.

- Cisco Secure Endpoint currently offers patch assessment, but does not offer software patch remediation of third party software. However, a Cyber Hygiene capability is on the SecureX roadmap.

- Cisco does not offer its own native, content-aware DLP solution. However, Cisco supports ICAP integration and has a partnership with Digital Guardian.

- Cisco Secure Endpoint will appeal most 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 Expert Security offers capabilities to defend against APTs and targeted cyberattacks with advanced technologies, actionable threat intelligence, knowledge transfer and expert guidance from Kaspersky.

Kaspersky Expert Security comprises the following products and services:

- **Kaspersky Anti Targeted Attack (KATA) Platform** – acts as an Extended Detection and Response (XDR) solution, combining network-level threat discovery and Kaspersky EDR capabilities to deliver fully automated data collection and storage, threat detection, proactive threat hunting, deep investigation and a centralized response. All potential threat entry points, network, web, mail, PCs, laptops, servers, and cloud workloads, are under control offering complete visibility and a centralized defense.

- **Kaspersky EDR –** also offered as a standalone technology, Kaspersky EDR is a powerful EDR tool for security experts, SOCs & Incident Response teams, enabling effective advanced detection, investigation with MITRE ATT&CK mapping and Kaspersky Threat Intelligence enrichment and response to multi-staged complex attacks targeting endpoint infrastructures.

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

- **Kaspersky Hybrid Cloud Security –** multi-layer protection for virtual servers and desktops in hybrid environments, simplifying security and ensuring visibility and control across a wide range of virtualization and public cloud platforms.

- **Kaspersky Security for Mail Sever** and **Kaspersky Security for Internet Gateways** – delivers email- and web-based threat protection and provides an automated response based on in-depth KATA Platform detections.

- **Kaspersky Threat Intelligence** – provides instant access to technical, tactical, operational and strategic Threat Intelligence.

- **Kaspersky Cybersecurity Training** – develops practical skills for in-house teams, including working with digital evidence, analyzing and detecting malicious software, working with Yara, and adopting best practices for incident response.

- **Kaspersky Incident Response** – covers the entire incident investigation cycle to completely eliminate the threat to the organization.

- **Kaspersky Managed Detection and Response** – an individually tailored ongoing threat hunting, investigation and response solution powered by AI and fully managed by Kaspersky experts.

- **Kaspersky Security Assessment** – are a set of services that provide a clear understanding of a company's security posture to close existing security gaps before they can be exploited.

The KATA Platform with Kaspersky EDR at its core delivers the following functionality:

- *Network traffic analysis (NTA)* – uses network sensors to detect activities in multiple segments of the IT infrastructure, enabling ‘near real-time’ detection of complex threats in web and email environments. It supports SMTP, POP3, POP3S, HTTP, HTTPS, ICAP, FTP and DNS protocols.

- *Sandboxing* –Advanced Sandbox technology provides capabilities for OS environment randomization, time acceleration in virtual machines, anti-evasion, user activity simulation, MITRE ATT&CK mapping and more, to 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, etc.). *Kaspersky Private Security Network (KPSN*), is available for organizations unable to send their data to the global KSN cloud but still wanting to benefit from 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 matching with a unique set of Indicators of Attack (IoAs) generated by Kaspersky’s threat hunters. All IoAs are mapped to MITRE ATT&CK information. Databases of custom IoAs appropriate to the specific infrastructure, or industry sector can also be created.

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

- *Detection with YARA rules* – supports complex matching rules to search files with specific characteristics and metadata. It also allows 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.

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

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

- *Third-party integration* – the KATA Platform supports verdict sharing through CEF/Syslog with the customer's SIEM system, or OpenAPI for integration scenarios with next-generation firewall, web gateways and other security systems.

STRENGTHS

- The Kaspersky Anti Targeted Attack (KATA) Platform with Kaspersky EDR at its core acts as an Extended Detection and Response (XDR) solution delivering all-in-one APT protection powered by Threat Intelligence and mapped to the MITRE ATT&CK framework.

- Kaspersky's Enterprise Portfolio effectively combines different layers of protection against complex cyberthreats. It is available as on-premise, cloud, hybrid, or air-gapped deployment and management approaches.

- The use of a single console and server architecture in the Kaspersky Anti Targeted Attack (KATA) Platform and Kaspersky EDR 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.

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

WEAKNESSES

- Kaspersky EDR does not currently support macOS. However, this is on the vendor's nearest roadmap.

- Kaspersky does not offer full-featured Data Loss Prevention (DLP). Customers who require this functionality will need to source it elsewhere.

- Kaspersky does not offer a full-featured CASB solution. However, it supports APIs for integration with third-party CASB solutions, and is working to offer basic CASB functionality aimed at small 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, cross-referencing MITRE ATT&CK® techniques. It combines ESET's detection and prevention technologies, threat intelligence and cloud malware protection system with other advanced detection 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 and emerging threats. It is managed by ESET Protect (previously ESET Security Management Center) and ESET Protect Cloud (previously ESET Cloud Administrator) 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 through ESET proprietary targeted early warning reports (e.g. Targeted malware report, Botnet activity report, Forged SSL certificate report, Targeted phishing report, and more). 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, network isolation, 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 ease of use.

- ESET offers single pane of glass remote management (available as cloud or on-premises) for computers, servers, mobile devices and virtual environments for increased visibility of threats, users and quarantined items.

- ESET offers extensive remediation/response capabilities through command tasks which include: network isolation of endpoints, the ability to terminate processes, restore files from backup, reboot endpoints, behavior blocking, and more.

WEAKNESSES

- ESET Enterprise Inspector does not currently support Linux platforms. However, Linux agent integration is on the vendor's roadmap.

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

- ESET does not currently 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.

BITDEFENDER

15A Orhideelor St.
Orhideea Towers, district 6
Bucharest, 060071
Romania
www.bitdefender.com

Bitdefender, founded in 2001, is a cybersecurity company delivering threat prevention, detection, and response solutions worldwide. The company has customers in 170 countries and offices around the world. The company is privately held.

SOLUTIONS

Bitdefender's **GravityZone**, is a hosted enterprise security platform that provides security controls and security posture management across endpoints, cloud workloads, network and users. For customers with restricted cloud usage, GravityZone can also be deployed on-premises. Bitdefender security agents can be installed on all leading platforms including Windows, Linux, Mac, Android, iOS and Microsoft Exchange.

Bitdefender delivers a number of GravityZone security packages, as follows:

- **GravityZone Ultra** – offers an integrated endpoint protection and EDR solution, which offers prevention, automated detection, investigation and response tools in a single agent, which can be managed through a single console. It provides real-time visibility into endpoints, insight into suspicious activity, alert triage and incident analysis visualization, one-click investigation, IOC lookup, helps track live attacks and lateral movements and enables rapid response for containment and remediation. It is available only as a cloud solution and can protect desktops, servers and Microsoft Exchange mailboxes.

- **GravityZone Elite** – is an integrated endpoint protection, risk management, and attack forensics platform which includes all the APT protection capabilities of GravityZone Ultra, except for the highly interactive EDR elements. It safeguards organizations with high-risk profiles from the full spectrum of advanced threats, in a fully automatic manner. It provides advanced protection and automatic detection/response for physical, virtual, mobile, cloud-based workloads, and email services.

- **GravityZone Business Security / Advanced Business Security** – are entry level bundles which deliver Machine Learning capabilities, behavioral analysis and processes monitoring, Fileless Attack Defense and Network Attack Defense are part of their core technology stack.

Bitdefender also offers the following product add-ons for APT defense:

Bitdefender Sandbox Analyzer On-Premises – is a next-generation AI-powered sandbox delivered as an on-premises virtual appliance, it delivers advanced detection, reporting & attack visibility. It helps enhance an organization’s posture against sophisticated or targeted attacks, through advanced detection and reporting capabilities of elusive, persistent threats.

Hypervisor Introspection (HVI) – is a solution designed to protect against sophisticated attacks on virtualized infrastructures. It introspects the memory of running virtual machines using Virtual Machine Introspection APIs in Xen and KVM hypervisors. HVI searches for attack techniques, such as buffer overflows, heap spray and code injection, to detect and block malicious activity before an attacker gains access and persistence on the targeted systems. In leveraging the hypervisor, the solution requires no software within protected virtual machines, allowing full insight without sacrificing isolation.

Bitdefender Network Traffic Security Analytics (NTSA) – applies Cloud threat intelligence, Machine Learning and behavior analytics to network traffic to detect advanced attacks early and enable effective threat response. It detects advanced attacks in real-time, provides threat context and triggers autonomous incident response through the integration with GravityZone. NTSA uses a combination of technologies built to detect advanced persistent threats for all entities, managed or unmanaged, for encrypted or un-encrypted network traffic.

Bitdefender (Hosted) Email Security – provides business email protection beyond malware and other traditional threats such as spam, viruses, large-scale phishing attacks and malicious URLs. It provides protection from known, unknown and emerging email security threats. It also protects against advanced attack scenarios that involve impersonation, credential phishing and impostor email.

Bitdefender Managed Detection and Response (MDR) provides customers with outsourced cybersecurity operations 24x7. It combines Bitdefender security technologies for endpoints, network, and security analytics, with the threat-hunting expertise of a fully staffed SOC.

STRENGTHS

- Bitdefender relies on various non signature-based techniques including heuristics, machine learning models, anti-exploit, fileless protection, cloud-based sandbox analyzer, network attack defense and process inspector to guard against advanced threats.

- Bitdefender GravityZone effectively combines an array of solutions including, endpoint security, EDR, XDR, MDR as well as patch management, encryption, and email security, at an attractive price point.

- Gravity Zone provides highly flexible multi-tenancy management options, APIs and advanced integrations with many IT management tools and platforms, to enable security teams to easily automate security workflows and scale operations.

- The integration of Network Traffic Analytics in GravityZone Ultra Plus extends the detection capabilities EDR to incorporate events information from other sensors thus improving detection and reducing attack dwell time.

WEAKNESSES

- Bitdefender's Mobile Security (MDM) solution for Android and iOS is currently available only for its GravityZone on-premises solutions. A cloud version is on the vendor's near term roadmap.

- GravityZone Endpoint Security currently provides only basic DLP-like functionality that allows Administrators to define patterns to be checked against scanned SMTP and HTTP traffic.

- Bitdefender does not currently offer a CASB solution. The vendor has this on its roadmap.

- While offering highly accurate malware and threat detection solutions, Bitdefender lacks pre-built integration with SOAR tools. However, Bitdefender offers APIs for 3rd party integration, with pre-built integrations as a roadmap item.

- Bitdefender is still best known for its consumer products and lacks greater visibility in the enterprise market. The vendor is working to address this.

PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

Palo Alto Networks, founded in 2005, delivers a comprehensive security portfolio, protecting organizations across clouds, networks, endpoints, and mobile devices. 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-deployed next-generation firewalls (NGFW). WildFire is sold on a subscription basis, and deploys as a cloud service, on-premises as a private cloud, or as a hybrid cloud model. WildFire provides complete visibility into all traffic, including advanced threats, across hundreds of applications, including Web traffic, email protocols , and FTP, regardless of ports or encryption (SSL). WildFire leverages threat intelligence prioritization features that combine automated analysis with human intelligence from the Palo Alto Networks Unit 42 threat research team.

WildFire leverages the following detection techniques:

- *Static analysis* – combines memory analysis, machine learning, analysis of file anomalies, malicious patterns and known malicious code.
- *Dynamic analysis* – leverages evasion-resistant custom hypervisor that performs behavioral scoring, network profiling, and multi-application version analysis.
- *Multi-stage analysis and prevention* – analyzes multi-stage threats creating prevention protections for each stage.
- *Bare metal analysis* – enables full dynamic analysis on real hardware, with no virtual environment and no hypervisor, to identify virtual machine evasion techniques.
- *Inline ML-based prevention* – provides real time prevention capabilities to immediately block APTs without relying on legacy signatures.

WildFire executes suspicious content in Linux, macOS, Android, and Windows 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, among others.

WildFire is natively integrated with the Palo Alto Networks product portfolio. Preventions generated by WildFire are automatically distributed to all WildFire subscribers globally within seconds. WildFire offers integrated logging, reporting and forensics through the management interfaces (including NGFW, VM-Series, Prisma Access, Panorama, Prisma Cloud, Cortex XDR, Cortex XSOAR, Prisma SaaS) and the WildFire portal. An open API is available for all integrations with any third-party security tools, such as SIEM (Security Information and Event Management) solutions and third-party email security 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 hybrid cloud solution. Hybrid deployments allow for sensitive files to be analyzed privately, whereas other content is analyzed in the cloud.

- WildFire integrates across Palo Alto Networks' entire product portfolio to offer full, rapid, up to date prevention and threat intelligence.

WEAKNESSES

- Palo Alto Networks' on-premise solution is not available in a virtual form factor.

- Palo Alto Networks solutions tend to be somewhat more costly when compared with other vendors in the space.

- Palo Alto Networks is still working to integrate capabilities from its recent Expanse (attack surface management) and Crypsis (incident response expert services) acquisitions.

SPECIALISTS

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. In late 2020, McAfee filed an initial public offering.

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 Active Response (EDR)
- McAfee Advanced Threat Defense Email Connector
- McAfee Enterprise Security Manager (SIEM)
- McAfee ePolicy Orchestrator (ePO)
- McAfee Network Security Platform (IPS)
- McAfee Threat Intelligence Exchange: including Application Control, Endpoint protection, Security for Email Servers, and Server Security.
- McAfee Web Gateway

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), it does not rollback to a known good state. However, rollback remediation is provided through McAfee MVISION Endpoint.

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 are connected 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 February 2020, the company was acquired by private equity firm Thoma Bravo, in a move that takes the company private.

SOLUTIONS

Sophos offers several solutions for APT, which comprise: next-gen **XG Firewall,** for network protection; **Intercept X Advanced**, **Intercept X Advanced with EDR**, and **Managed Threat Response**, for endpoint protection. The EDR version contains all the traditional and modern protection of Intercept X Advanced, but also includes additional endpoint detection and response (EDR) functionality on the same agent. The Sophos Managed Threat Response (MTR) Service adds a 24/7 managed detection and response service in addition to the features in Intercept X Advanced with EDR.

- **Sophos XG Firewall** – is Sophos's flagship next-generation firewall which provides comprehensive Web Gateway functionality. The version 18 (v18) release introduces a new high-performance SSL/TLS decryption engine and inline web filter that inspects encrypted and non-encrypted web traffic on any port. It integrates with Sophos's cloud-based Intelix platform to protect against emerging threats with sandboxing and deep learning analysis. It also offers cloud app visibility and shadow IT detection, leveraging a heartbeat connection between gateway and endpoint to identify unrecognized application traffic.

- **Sophos Intercept X Advanced** – combines traditional protection and next-generation endpoint protection in a single solution, with a single agent. It provides signature-less exploit prevention, antivirus, deep learning malware detection, anti-ransomware, active adversary protection, HIPS, whitelisting, web security, application control, DLP and more. Sophos's Synchronized Security automates incident response and application visibility, via on-going direct sharing of threat, security, and health information between endpoints and the network. Additional features include root cause analysis, and advanced system cleaning technology.

- **Sophos Intercept X Advanced with EDR** – also includes integrated endpoint detection and response capabilities using the same agent. EDR functionality is available for Windows, macOS and Linux devices. **Intercept X for Server** includes all Intercept X functionality with the addition of Application Lockdown, File Integrity Monitoring and visibility into organizations' wider cloud environments (e.g. serverless functions, S3 buckets and databases).

The following solutions are also available as separate add-ons:

  - *Sophos Mobile* – handles all mobile devices, from the initial setup and enrollment, through device decommissioning. It includes a fully featured web-based console allowing administration from any location on any device.

  - *Intercept X for Mobile* – protects mobile devices using up-to-the-minute intelligence from Sophos Labs, deep learning malware detection, and more. Apps can be scanned on installation, on demand or on a schedule.

All Sophos solutions are managed via **Sophos Central**, a cloud-based platform for all Sophos solutions. In addition, Sophos offers the following services:

Sophos Managed Threat Response (MTR) – a 24/7 threat hunting, detection, and response delivered by an expert team as a fully-managed service.

Sophos Rapid Response – an emergency incident response service for organizations experiencing an active cyberattack. It is available to existing Sophos customers, as well as non-customers (included in Sophos MTR service).

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 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 solutions are attractively priced for SMBs and 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.

- Sophos offers limited support for patch assessment and remediation of third party software running on the endpoint.

- In pursuit of simplicity, Sophos solutions do not always provide administrators with granular, customizable controls typically found in competing solutions.

- Sophos offers only basic CASB and DLP capabilities.

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 threat intelligence, security orchestration, workflow management, next-generation SIEM, investigation capabilities and compliance reporting. It is available with any FireEye subscription-based solution, and integrates across all FireEye technologies and non-FireEye security products.

- **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 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 available as a cloud solution, as well 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 Cloudvisory** – offers visibility into a multi-cloud infrastructure through a single console. It offers security analytics, network flow visualization, compliance assurance, and machine learning driven governance management.

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 offers 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.

FORCEPOINT

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

Forcepoint offers a systems-oriented approach to insider threat detection and analytics, cloud-based user and application protection, next-generation network protection, data security and systems visibility. Forcepoint, a Raytheon Company and Vista Equity Partners joint venture, was acquired by Francisco Partners in early 2021.

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. AMD is available as a cloud solution and as an on-premises appliance, as follows:

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

- **AMD On Premises** – is an 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** – provides visibility and control for cloud applications such as Office 365, Google G Suite, Salesforce and others. It enforces security policies for all endpoint devices including BYOD and access points (mobile apps and browsers). It helps protect data stored in cloud storage services through DLP and Forcepoint Advanced Malware Detection.

- **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

- Forcepoint solutions tend to be more expensive than competing solutions, and are a best fit for mid-size and large enterprises with advanced needs.

- 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.

VMWARE CARBON BLACK

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

VMware Carbon Black is a provider of next-generation Endpoint and Workload Security. The company leverages its big data and analytics cloud platform, the VMware Carbon Black Cloud, to enable customers to identify risk, protect, detect and respond against advanced cyber threats, including malware, ransomware, and non-malware attacks. VMware is publicly traded.

SOLUTIONS

VMware Carbon Black Cloud is a next generation protection platform that consolidates security in the cloud, making it easy to prevent, investigate, remediate, and hunt for threats. VMware Carbon Black supports all leading OS platforms, including Windows, macOS, and Linux. It offers the following modules which can be managed through the same user interface, with a single login:

- **VMware Carbon Black Endpoint –** Delivers next generation delivers next-generation antivirus (NGAV), IT hygiene, endpoint detection and response (EDR) and managed detection functionality. It analyzes attacker behavior patterns to detect malware, fileless, or living-off-the-land zero-day attacks, offers real-time device assessment and remediation. It serves to audit the current system state and track and harden the security posture across protected devices. Combines this with offering threat hunting and containment capabilities. It serves to proactively hunt for abnormal activity using threat intelligence and customizable detections. In addition, VMware Carbon Black offers managed detection which is a real-time security operations solution that provides managed alert monitoring and triage. It delivers visibility for security operations center (SOC) and incident response (IR) teams. Leveraging this data, enables teams to proactively hunt for threats, as well as uncover suspicious and stealthy behavior, disrupt active attacks and address potential defense gaps

- **VMware Carbon Black Workload –** Delivers Visibility to identify risk and harden workloads, Prevention, detection and response to advanced attacks Simplified operations for IT and security teams. VMware Carbon Black Cloud Workload helps security and infrastructure teams focus on the most high-risk vulnerabilities by finding, prioritizing and delivering them in an automated fashion to the right dashboard. Combining this with NGAV to analyzes attacker behavior patterns to detect malware, fileless, or living-off-the-land zero-day attacks and offering real-time workload assessment and remediation to maintain a hardened posture. Combining that with EDR to detect and respond to the most complex attacks across the data center and maintain a strong security posture.

STRENGTHS

- VMware 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.

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

- VMware Carbon Black 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.

- VMware 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

- VMware Carbon Black Cloud does not offer some traditional endpoint protection functionality, such as firewalls, mobile security, or DLP. However, custom integrations are possible through the platform's open APIs.

- VMware Carbon Black Cloud does not provide application control capabilities. VMware Carbon Black currently offers this through an on-premises application control product.

- VMware Carbon Black has lost some mindshare following the VMware acquisition.

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:

- **Microsoft Defender for Office 365 (formerly 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 available in 2 plans.

  Microsoft Defender for Office 365 Plan 1 provides the following capabilities:

  - *Safe Links* – provides time-of-click verification of URLs in email messages and Office files.

  - *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.

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

  - *Anti-phishing protection* – detects attempts to impersonate user and internal or custom domains. It applies machine learning to block phishing attacks.

- *Advanced reporting dashboard* – provides real time threat detection reports with recommendations and alerts to imminent threats.

Plan 2 adds the following capabilities:

- *Threat investigation and response tools* – which include Threat Trackers to deliver intelligence on prevailing cybersecurity issues; Threat Explorer for real-time reporting detection; Automated Investigation and Response (AIR) to support automated investigation and response to well-known threats; Attack Simulation to help identify vulnerabilities; and Campaign Views to identify and categorize phishing attacks.

Microsoft Defender for Office 365 Plan 1 is included in Microsoft 365 Business Premium. Microsoft Defender for Office 365 Plan 2 is included in Office 365 E5, Office 365 A5, Microsoft 365 E5 Security, and Microsoft 365 E5. A *Safe Documents* feature is only available with the Microsoft 365 E5 plan, or users with the Microsoft 365 E5 Security license.

- **Microsoft Defender for Endpoint (formerly Microsoft Defender ATP)** – is a cloud-based endpoint security solution that includes risk-based vulnerability assessment and management, attack surface reduction, behavior-based next generation protection, EDR, automatic investigation and remediation, managed hunting, and unified security management. 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 for Endpoint, 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 for Endpoint is also available for macOS, Linux, Android and iOS platforms, although feature parity is not available across all platforms.

- **Azure Defender for Identity (formerly 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. It is available with Microsoft 365 plans.

- **Microsoft Cloud App Security** – is Microsoft's cloud access security broker (CASB) solution which integrates natively with Microsoft's security and identity solutions, including Azure Active Directory, Intune, and Azure Information Protection.

- **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.

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 for Endpoint is a good first step for organizations looking for an entry-level EDR solution.

WEAKNESSES

- 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. In order to obtain Microsoft's full range of security capabilities, customers must upgrade to the high-end Microsoft 365 E5 enterprise license.

- 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 customers deploy Microsoft technologies as a baseline, while also deploying additional security solutions from other vendors for advanced protection.

- 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 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.

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, 2021-2025	Feb. 2021	$3,000.00
Instant Messaging Statistics Report, 2021-2025	Feb. 2021	$3,000.00
Social Networking Statistics Report, 2021-2025	Jan. 2021	$3,000.00
Mobile Statistics Report, 2021-2025	Jan. 2021	$3,000.00
Endpoint Security Market, 2020-2024	Nov. 2020	$3,000.00
Secure Email Gateway Market, 2020-2024	Nov. 2020	$3,000.00
Microsoft SharePoint Market Analysis, 2020-2024	May 2020	$3,000.00
Email Market, 2020-2024	Apr. 2020	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2019-2023	Apr. 2020	$3,000.00
Cloud Business Email Market, 2020-2024	Apr. 2020	$3,000.00
Corporate Web Security Market, 2020-2024	Apr. 2020	$3,000.00
Unified Endpoint Management Market, 2020-2024	Apr. 2020	$3,000.00
Advanced Threat Protection Market, 2020-2024	Apr. 2020	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Information Archiving Market, 2021-2025	Apr. 2021	$3,000.00
Advanced Threat Protection Market, 2021-2025	Apr. 2021	$3,000.00
Corporate Web Security Market, 2021-2025	Apr. 2021	$3,000.00

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

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