The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Advanced Persistent Threat (APT) Protection - Market Quadrant 2022 *

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

March 2022

* Radicati Market Quadrant^{SM} is copyrighted March 2022 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 possess a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don't become Top Players overnight. Most of the companies in this quadrant were first Specialists or Trail Blazers (some were both). As companies reach this stage, they must fight complacency and continue to innovate.

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

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

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

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

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

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

b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.

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

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

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

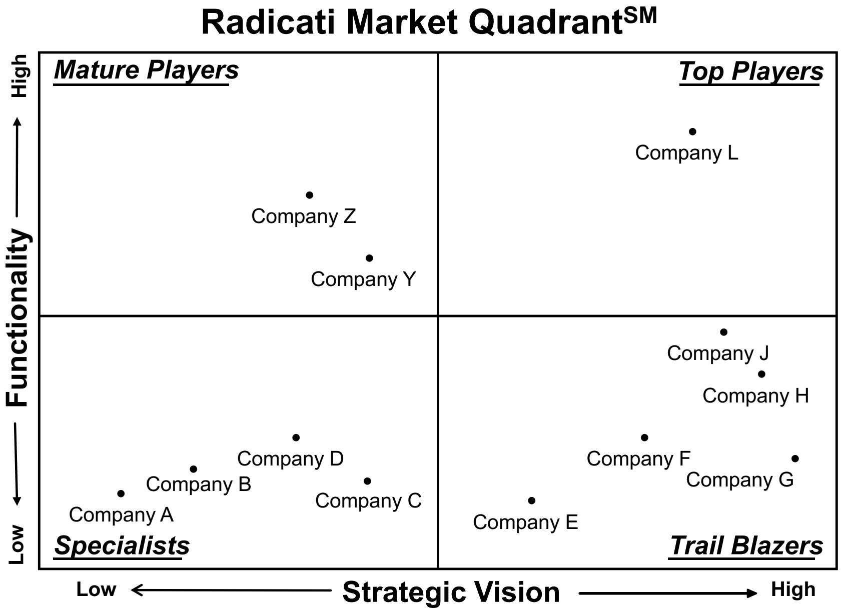

Figure 1: Sample Radicati Market Quadrant

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/XDR, CASB, reputation networks, threat intelligence management and reporting, forensic analysis and more. Some of the leading players in this market are *Bitdefender, Broadcom, Cisco, ESET, Kaspersky, Microsoft, Palo Alto Networks, Sophos, Trellix,* 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 $6.9 billion in 2022, to nearly $15.2 billion by 2026.

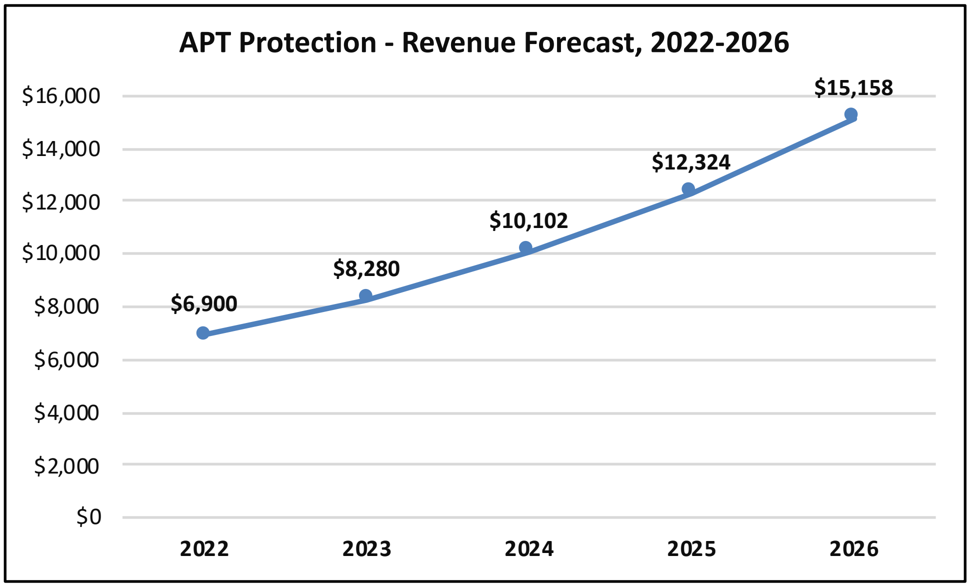

Figure 2: APT Protection Market Revenue Forecast, 2022 – 2026

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)/Extended Detection and Response (XDR)* – 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. XDR is the extension of EDR beyond endpoints, to correlate attack detection and response across endpoints, networks, servers, cloud workloads, SIEM, and more.

- *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

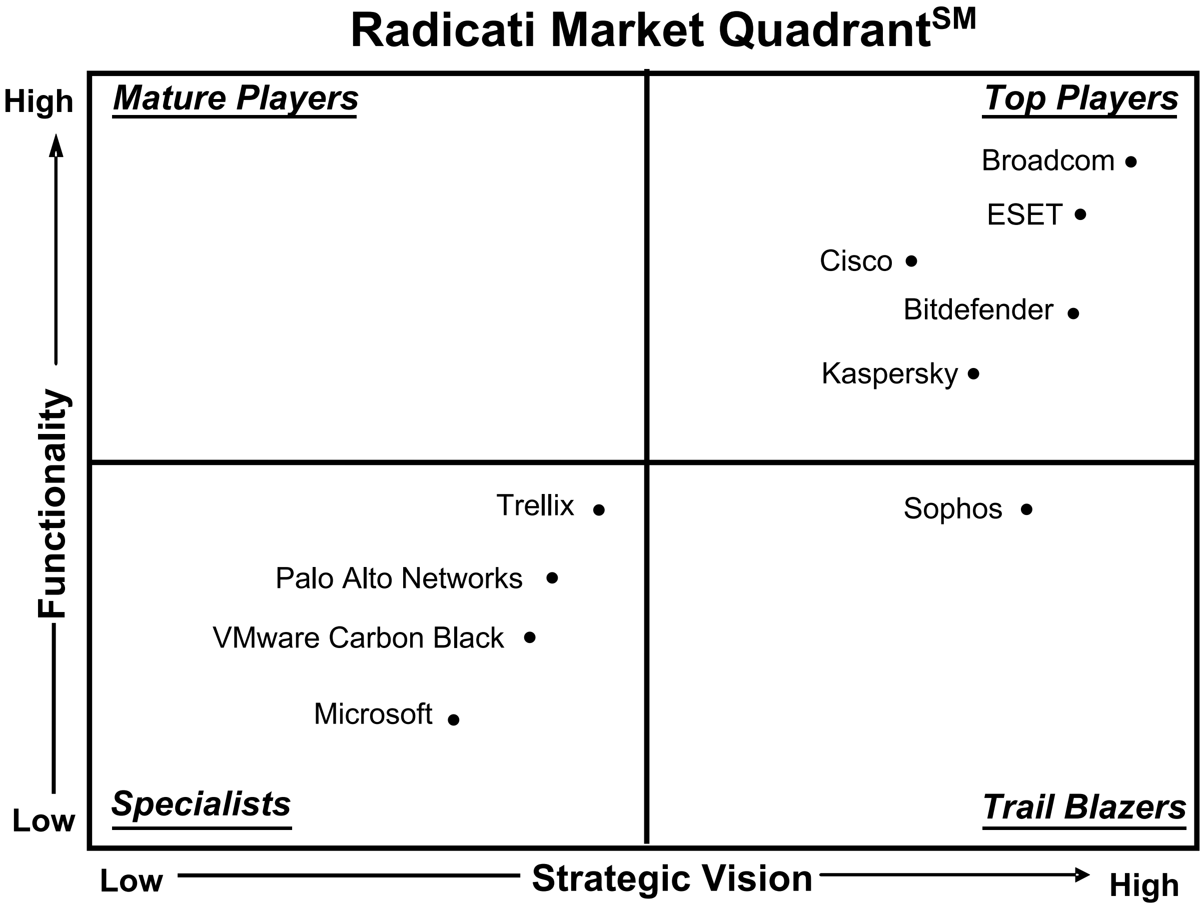

Figure 3: APT Protection Market Quadrant, 2022*

* Radicati Market Quadrant^{SM} is copyrighted March 2022 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 *Broadcom*, *ESET*, *Cisco, Bitdefender,* and *Kaspersky***.**

- The **Trail Blazers** quadrant includes *Sophos*.

- The **Specialists** quadrant includes *Trellix, Palo Alto Networks, VMware Carbon Black,* and *Microsoft*.

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

APT PROTECTION - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC, BY BROADCOM SOFTWARE

1320 Ridder Park Drive
San Jose, CA 95131
www.broadcom.com

Founded in 1982, Symantec, by Broadcom Software is one of the largest providers of enterprise security technology. Symantec 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 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 Web Protection Suite (WPS)*** **–** available as enterprise-grade Secure Web Gateway appliances, virtual appliances, or cloud-delivered SaaS services, block known threats, malicious sources, risky sites, unknown content categories, and malware delivery networks at the gateway in real-time. WPS provides these capabilities through an integrated collection of threat protection technologies with a user-based license that allows customers to support on-premises, in the cloud, or hybrid deployments. Key capabilities include:

    - *Symantec proxy-based SWG* – can be deployed either on-premises as an appliance or VM, or through cloud-hosted SWG and powered by Symantec Intelligence Services, it categories, classifies, applies policy and assigns risk scores to all web traffic to block the majority of threats.

    - *Content Analysis and sandboxing* – integrates with the Symantec Proxy to orchestrate malware scanning, dynamic sandboxing and application blocking, while Symantec SSL Visibility provides additional visibility into SSL/TLS encrypted threats.

    - *Symantec Web Isolation* – also integrates with on-premises or 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.

    - *Management Center and Reporting* – offers centralized management and reporting capabilities for Web Protection Suite and enables consistently applied security policies and protections to enhance threat protection.

- ***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 XDR solutions, including Symantec XDR, 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 Endpoint Security Complete (SESC)*** – is Symantec's full-feature endpoint security offering which combines Symantec Endpoint Protection (SEP), Symantec Endpoint Detection and Response (SEDR), Adaptive Protection, Active Directory defense, and Threat Hunter to provide an integrated offering with coverage across all devices, including mobile. Functionality includes:

  - *Adaptive Protection* – automates custom hardening by blocking unused and potentially malicious processes and behaviors to stop attackers without affecting employee productivity.

  - *Active Directory defense* – helps stop lateral movement of attackers to prevent infiltration of network assets.

  - *Threat Hunter* – assists SOCs by combining Symantec's expert analyst research with advanced machine learning and threat intelligence of internal and global data to provide alerts and insights onto unfolding attacks.

  - *Upgrading from SEP to SESC* – does not require installation of a new agent, as both use the same agent. SESC can be deployed as cloud managed, on-premises, or a hybrid. SESC exposes advanced attacks through advanced 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 search, identify and contain impacted endpoints while investigating threats using a choice of on-premises and cloud-based sandboxing. In addition, SESC offers continuous, on-demand recording of system activity to support 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.

STRENGTHS

- Symantec offers on-premises, cloud, and hybrid options across its threat protection 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, deny lists, machine learning, exploit prevention, web isolation, mobile protection, ZTNA, 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 ZTNA, CASB and Web Isolation.

- Broadcom’s Software Division which brings together multiple acquisitions (Symantec, CA, and others) into a single business unit, which gives customers access to identity protection and management as part of their purchase of the Symantec security portfolio. Symantec continues to integrate CA’s Identity Security products into their security platform

- 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, with simplified licensing, offer streamlined protection for smaller customers.

- SESC supports workflows for patch management and remediation. Although customers use both products together, SESC and Symantec's ITMS (Altiris) product are currently on two separate consoles.

- Symantec Endpoint Security offers encryption as a separate option, available for separate purchase.

- Symantec offers strong content aware DLP capabilities, however these require a separate add-on.

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 PROTECT** – is ESET's unified single-click security management platform with XDR-enabling and threat hunting capabilities. It is available as a cloud or on-premises deployment and offers extensive remediation/response capabilities through command tasks which include: network isolation of endpoints, the ability to terminate processes, restore files from backup, Open Terminal (remote PowerShell), reboot endpoints, behavior blocking, and more. The ESET PROTECT platform provides over 170 built-in reports and allows organizations to create custom reports from over 1000 data points.

- **ESET Inspect (EI)** (*previously ESET Enterprise Inspector*) – is ESET's XDR-enabling component of the ESET PROTECT platform. It delivers breach prevention, enhanced visibility and remediation. It references its detections to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework. ESET Inspect features an API that allows effective integration with tools such as SIEM, SOAR, ticketing tools and many others. Paired with ESET Endpoint Protection products, ESET Inspect is a cloud-delivered, XDR-enabling solution which detects advanced persistent threats, stops fileless attacks, blocks zero-day threats, protects against ransomware, and helps prevent company policy violations.

- **ESET LiveGuard Advanced** *(previously ESET Dynamic Threat Defense)* – is ESET's cloud managed advanced threat defense which provides an additional layer of protection for ESET Endpoint and Server security solutions. It provides an isolated test environment in which suspicious programs can be executed, and their behavior observed, analyzed and reported in an automated manner. This is particularly effective against zero-day threats, including ransomware.

- **ESET Endpoint Security** – leverages a multilayered approach that utilizes multiple technologies to enable organizations to: protect against ransomware, block targeted attacks, prevent data breaches, stop fileless attacks, detect advanced persistent threats, and offer mobile protection (MDM).

- **ESET's Managed Detection and Response service** – is a customized, integrated security services package designed to complement ESET Inspect, ESET's XDR-enabling component of the ESET PROTECT platform. It is delivered by ESET's security experts to offer investigation of incidents and proactive threat hunting, it also provides response and remediation steps to eliminate threats and ensure business continuity.

- **ESET's Threat Intelligence Reports & Feeds** – is ESET's threat intelligence for detection of Advanced Persistent Threats (APTs), blocking of suspicious domains and IOCs (Indicators of Compromise), prevention of botnet or phishing attacks. Tactical threat intelligence is distributed through ESET proprietary targeted early warning reports (e.g. Targeted malware report, Botnet activity report, Forged SSL certificate report, Targeted phishing report, and more). It also provides IOCs (IP, URL, file hash) and serves as an automated malware analysis portal. ESET also offers strategic, private APT reports for specialized SOCs and CERTs with detailed contextual information on diverse APT actors.

STRENGTHS

- ESET Inspect is available as a cloud or on-premises solution, and can be alternatively deployed in AWS and MS Azure instances.

- ESET Inspect, the cloud-delivered XDR-enabling component of the ESET PROTECT platform, supports all major operating systems (i.e. Windows, macOS, and Linux), and is available as a cloud or on-premises solution, as well as can be deployed in AWS and MS Azure instances.

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

- Customers appreciate ESET solutions for their ease of deployment and ease of use.

- ESET PROTECT offers a unified single-click security management platform with XDR-enabling and threat hunting capabilities.

WEAKNESSES

- 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.

CISCO

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

Cisco is a leading vendor of Internet communication and security technology. Cisco's security solutions are powered by the Cisco Talos Intelligence 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 that combines multiple sensor and detection technologies into a unified location for visibility and provides automation and orchestration capabilities to maximize operational efficiency across the network, users, endpoints, cloud, and applications. Cisco Secure customers are entitled to Cisco SecureX at no additional charge with the 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-premises deployment using either a virtual appliance or a 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, Vulnerability 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 they compromise the OS-level. The built-in SecureX platform extends detection and response 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 with efficient information about the endpoints they manage. For ease of use, an endpoint forensic snapshot and/or a catalog of advanced endpoint search queries are mapped to the MITRE ATT&CK framework. Options for managed threat hunting or full managed endpoint detection and response services are 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 a 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 integration with Kenna Security enables risk-based endpoint security by inferring a vulnerability risk score for each endpoint as well as identifying applicable common vulnerabilities and exposures (CVEs) to help organizations proactively reduce attack surface and to correlate vulnerability impact during endpoint incident investigations. It also provides a catalog of endpoint posture assessment advanced search queries to rapidly assess patch levels and hunt for indicators of compromise.

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's security portfolio also includes the following capabilities:

Secure Network Analytics – 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 – provides the visibility and threat detection capabilities needed 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 in a variety of form factors (both appliances and virtual appliances) with both on-premises 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.

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 an organization to unify visibility, detection, and response 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 can 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.

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** – entry level bundle which delivers Machine Learning capabilities, behavioral analysis and processes monitoring, Fileless Attack Defense and Network Attack Defense are part of the 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 (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 endpoint-to-endpoint correction and network visibility 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 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.

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 delivers an Extended Detection and Response (XDR) platform together with expert guidance, assessment, threat intelligence, and skills training.

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 Expert 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 Expert –** also offered as a standalone technology, Kaspersky EDR is an 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 Expert 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 Expert 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 Expert 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 Expert does not currently support macOS. However, this is on the vendor's 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.

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 are connected with Sophos Central, Sophos's integrated cloud-based management console, and backed by SophosLabs, its global network of threat intelligence centers. The company is headquartered in Oxford, U.K. In 2020, Sophos was acquired by private equity firm Thoma Bravo.

SOLUTIONS

Sophos offers several solutions for APT, which comprise: next-gen **Sophos Firewall,** for network protection; **Intercept X Advanced**, **Intercept X Advanced with XDR**, **Intercept X with MTR Standard,** and **Intercept X with MTR Advanced**, for endpoint protection. The XDR version contains all the traditional and modern protection of Intercept X Advanced, but also includes extended detection and response (XDR) functionality across endpoint, server, network, email, cloud and mobile data. 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 XDR.

- **Sophos Firewall** – is Sophos's flagship next-generation firewall which provides comprehensive Web Gateway functionality. It includes a 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, active adversary protection, deep learning malware detection, anti-ransomware, AV, HIPS, whitelisting, web security, application and device 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. Intercept X Advanced includes the following key capabilities:

    - *Anti-exploit and active adversary technology* – looks at the tools and techniques used by attackers to distribute malware, steal credentials, and escape detection.

    - *Deep learning malware detection* – uses advanced machine learning to examine the "DNA" of files and a determine if they are malicious without ever having seen them before.

    - *CryptoGuard* – behavior-based ransomware protection that detects malicious encryption and rolls back any affected files.

    - *Host Intrusion Prevention System (HIPS)* – is integrated into the endpoint agent and console, to identify and block previously unknown malware before damage occurs.

    - *Web security* – is integrated into the endpoint agent platform and provides live URL filtering. Multiple browsers are supported, such as IE, Firefox, Safari, Chrome, and Opera.

    - *Web content filtering and policy enforcement* – is included to block Web content based on categories. For Sophos customers that also have the Sophos UTM or secure web gateway appliance, these appliances leverage the endpoint to enforce web filtering policies, even when the endpoints are off the corporate network.

    - *Application control* – is available for thousands of applications across dozens of application categories. P2P, IM, and more can be blocked for all users or some users. Web browsers can also be blocked to force users to use only a company-sanctioned browser.

- *Device control* – can be used to block the use of storage devices, optical drives, wireless devices (e.g. Bluetooth), and mobile devices.

- *DLP* – is available for content in motion. Pre-built and custom filters can be enabled that scan content for infringing data. DLP features are also extended to email appliances.

- *Firewall* – protect endpoints from malicious inbound and outbound traffic. Location-aware policies are available to add security when protected endpoints are out of the office.

Sophos Intercept X Advanced for Server (available as *Intercept X Advanced for Server*, *Intercept X Advanced for Server with XDR*, and *Intercept X Advanced for Server with MTR*) includes all Intercept X Advanced 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). It offers:

- *Server Lockdown* – ensures that only approved applications can run on a server.

- *File Integrity Monitoring* – will notify if there are unauthorized attempts to change critical files.

- *Cloud Workload Protection* – detect cloud workloads as well as critical cloud services including S3 buckets, databases and serverless functions, identify suspicious activity, spot insecure deployments and close security gaps.

- *Agentless scanning* – managed through the same console used by Sophos endpoint clients, ensures that every virtual machine on a VMware host is protected.

Sophos Intercept X Advanced with XDR (available as *Intercept X Advanced with XDR*, *Intercept X Advanced for Server with XDR*) includes integrated endpoint detection and response capabilities using the same agent. XDR functionality is available for Windows, macOS and Linux devices. Includes all features of Intercept X Advanced plus:

- *EDR/XDR* – designed for IT administrators and cybersecurity specialists to handle critical IT operations and threat hunting questions.

- *LiveDiscover* – Uses pre-defined or custom queries to hunt through live and historical data on an endpoint plus the data from Sophos products in the Data Lake.

- *LiveResponse* – Instantly act on an endpoint to resolve issues or carry out additional tasks after an automatic remediation.

Sophos also offers **Sophos Mobile** and **Intercept X for Mobile** as separate add-ons. All Sophos solutions are managed via **Sophos Central**, an integrated cloud-based management console for all Sophos solutions. **Sophos Rapid Response** is 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 strong XDR capabilities, in an easy to consume format that is easily accessible for security teams across a wide expertise range.

- 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 XDR 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 Intercept X endpoint solutions do not have direct access to Sophos's Sandstorm sandboxing functionality.

- Sophos no longer supports network access control, which prevents administrators from blocking network access to certain endpoints (e.g. new endpoints that have not yet deployed the organization's security policies).

- Sophos offers only basic CASB and DLP capabilities.

SPECIALISTS

TRELLIX

300 Baker Ave
Concord, MA 01742
www.mcafee.com

Trellix, is a new company launched in January 2022 by Symphony Technology Group (STG), with combined assets from McAfee Enterprise and FireEye Products to focus on extended detection and response (XDR). Trellix is privately held.

SOLUTIONS

McAfee Advanced Threat Defense (ATD) enables organizations to detect advanced targeted attacks and convert threat information into immediate action and protection. It 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.

ATD delivers the following functionality:

- *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* – offers integrated solutions to easily move organizations from analysis and conviction to protection and resolution. At the data level, ATD 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.

ATD 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. Support is also provided for 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. ATD also supports third party email gateways, and integration with BRO-IDS, an open source network security monitor.

STRENGTHS

- ATD is available through flexible deployment options, which include appliance, virtual appliance and cloud form factors with CapEx and OpEx purchase options. ATD 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 ATD 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 can also integrate to publish and subscribe to DXL threat intelligence.

- ATD 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.

WEAKNESSES

- Trellix does not offer its own email gateway solution. However, ATD does integrate with third party email solutions to provide file attachment analysis.

- Cloud deployment is not currently available on AWS.

- ATD does not support Apple macOS, or Linux platforms.

- ATD 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.

- Trellix is a new company recently formed by the merger of assets from McAfee Enterprise and FireEye Products into a combined company focused on extended detection and response (XDR). At the time of this writing, it is too early to assess the company’s future direction.

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.

A WildFire WF-500-B appliance can conduct threat analysis and generate protections entirely on-premises. This helps address the needs of customers with air-gapped networks.

STRENGTHS

- Palo Alto Networks was one of the early developers of anti-APT technology, and benefits from its long term expertise in threat detection.

- 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 has been working to integrate capabilities from its recent Expanse (attack surface management) and Crypsis (incident response expert services) acquisitions, however, customers should check carefully on available features and functionality.

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 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 can audit the current system state and track and harden the security posture across protected devices. This combines 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 through 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. It offers 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. It combines this with

NGAV to analyze attacker behavior patterns in order to detect malware, fileless, or living-off-the-land zero-day attacks and offer real-time workload assessment and remediation to maintain a hardened posture. This combines 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 Endpoint (MDE)** – 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 in two plans: Plan 1 (currently in preview) aimed at E3 license customers, or as Plan 2 (generally available) for E5 license customers or E3 customers with a E5 security extension. 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 MDE.

    - *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.

- **Microsoft Defender for Office 365** – 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, and Microsoft 365 E5. Both Plan 1 and Plan 2 are also each available as an add-on to certain subscriptions. A *Safe Documents* feature, which allows viewing of documents in a protected state, is only available with the Microsoft 365 E5 plan, or Microsoft 365 E5 Security licenses.

- **Azure Defender for Identity** – is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider threats. 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 Defender for Cloud Apps (formerly 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 ATP cloud-based solutions are easy to deploy, and manage for customers of all sizes.

- 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 is investing heavily in its security solutions portfolio, to deliver an impressive ecosystem of solutions that encompass the OS, applications, and services.

- 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.

- As a purely cloud-based solution, Microsoft Defender for Office 365, is not applicable to customers with purely on-premises deployments or air-gapped networks.

- 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*
Secure Email Gateway Market, 2021-2025	Dec. 2021	$3,000.00
Endpoint Security Market, 2021-2025	Dec. 2021	$3,000.00
Microsoft SharePoint Market Analysis, 2021-2025	May 2021	$3,000.00
Email Market, 2021-2025	Apr. 2021	$3,000.00
Microsoft Office 365, Exchange and Outlook Market Analysis, 2021-2025	Apr. 2021	$3,000.00
Cloud Business Email Market, 2021-2025	Apr. 2021	$3,000.00
Corporate Web Security Market, 2021-2025	Apr. 2021	$3,000.00
APT Protection Market, 2021-2025	Apr. 2021	$3,000.00
Information Archiving Market, 2021-2025	Mar. 2021	$3,000.00
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

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

Upcoming Publications:

Title	To Be Released	Price*
Information Archiving Market, 2022-2026	May 2022	$3,000.00
APT Protection Market, 2022-2026	May 2022	$3,000.00
Corporate Web Security Market, 2022-2026	May 2022	$3,000.00

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

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