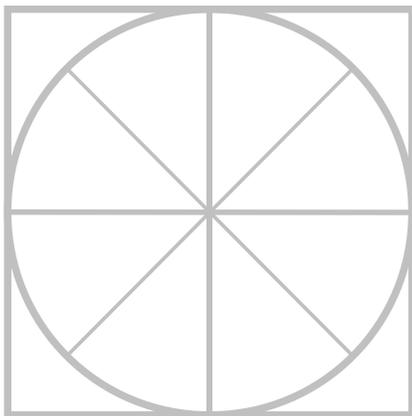




THE RADICATI GROUP, INC.

Advanced Persistent Threat (APT) Protection - Market Quadrant 2023 *



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

March 2023

* Radicati Market QuadrantSM is copyrighted March 2023 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market QuadrantsSM 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 QuadrantsSM 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	3
MARKET SEGMENTATION – ADVANCED PERSISTENT THREAT (APT) PROTECTION.....	5
EVALUATION CRITERIA	7
MARKET QUADRANT – APT PROTECTION	10
<i>KEY MARKET QUADRANT HIGHLIGHTS</i>	11
APT PROTECTION - VENDOR ANALYSIS	11
<i>TOP PLAYERS</i>	11
<i>TRAIL BLAZERS</i>	25
<i>SPECIALISTS</i>	28

Please note that this report comes with a 1-5 user license. If you wish to distribute the report to more than 5 individuals, you will need to purchase an internal site license for an additional fee. Please contact us at admin@radicati.com if you wish to purchase a site license.

Companies are never permitted to post reports on their external web sites or distribute by other means outside of their organization without explicit written prior consent from The Radicati Group, Inc. If you post this report on your external website or release it to anyone outside of your company without permission, you and your company will be liable for damages. Please contact us with any questions about our policies.

RADICATI MARKET QUADRANTS EXPLAINED

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

1. **Top Players** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as 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.

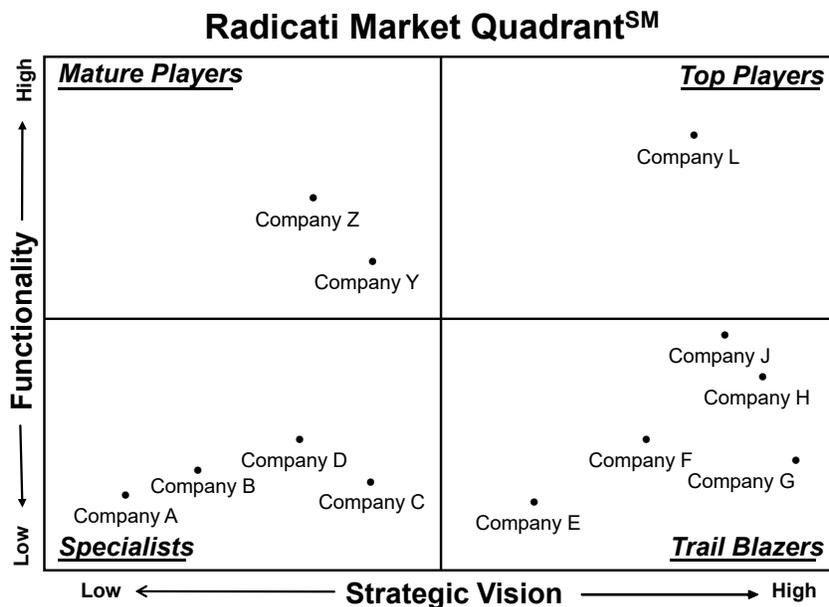


Figure 1: Sample Radicati Market Quadrant

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 QuadrantsSM 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, Cisco, ESET, Microsoft, Palo Alto Networks, Sophos, Symantec, 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 \$8.2 billion in 2023, to over \$18.6 billion by 2027.

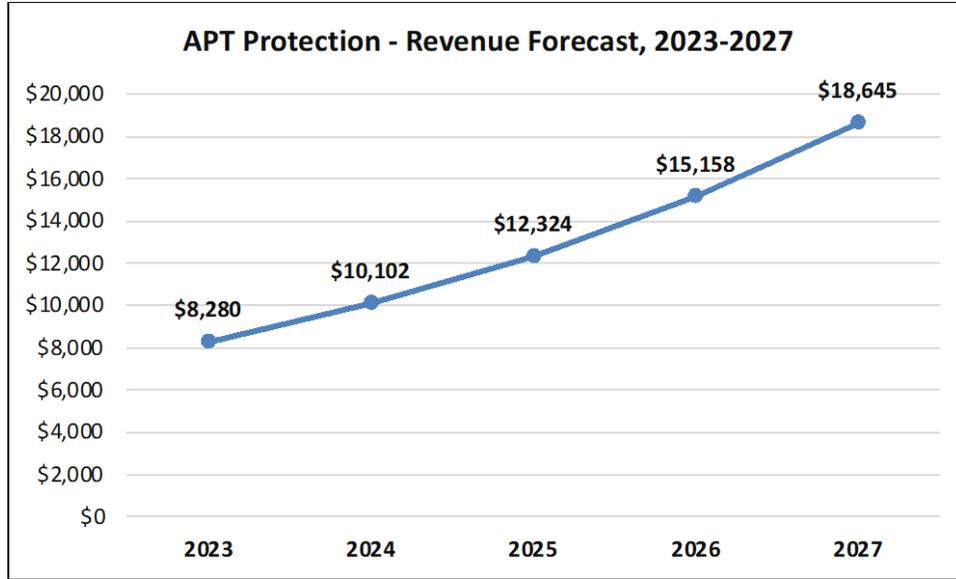


Figure 2: APT Protection Market Revenue Forecast, 2023 – 2027

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

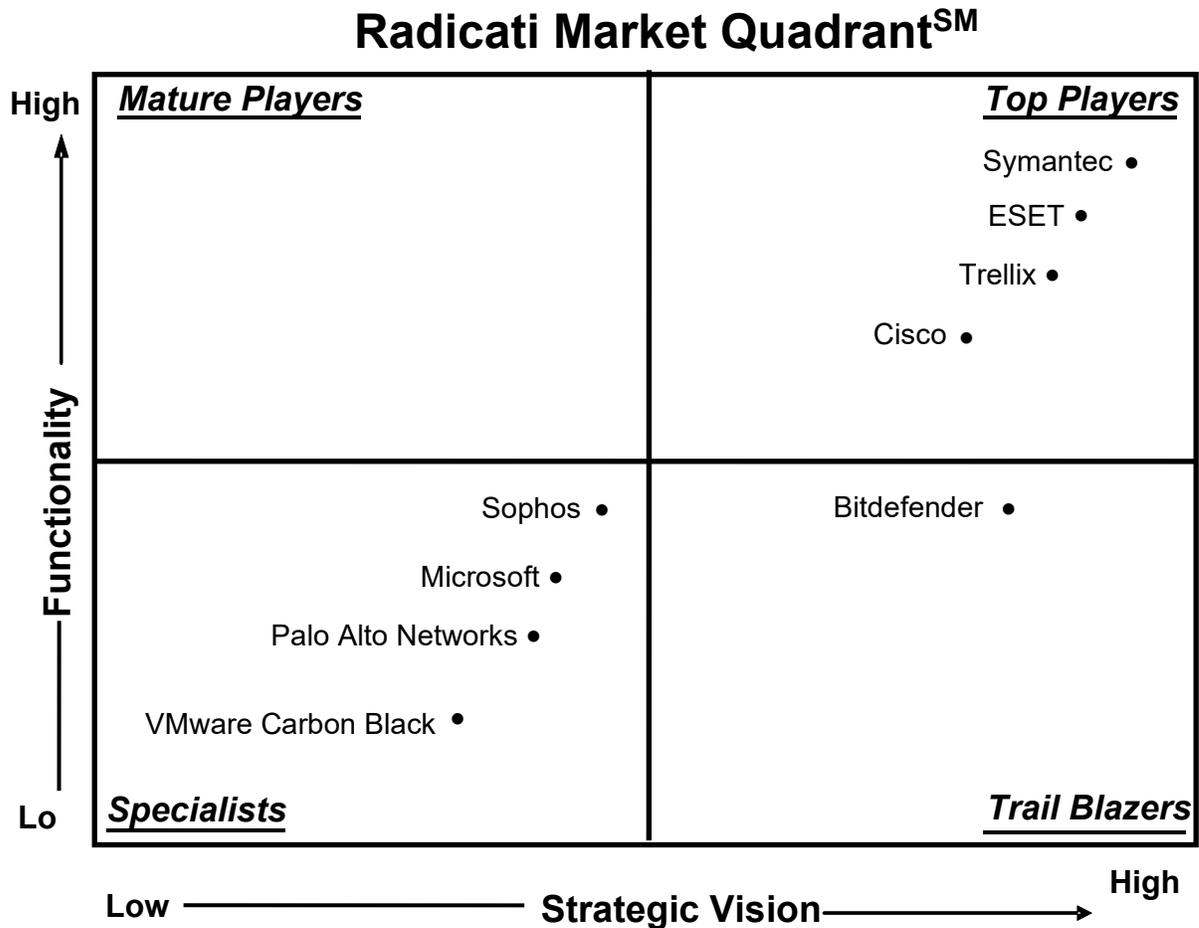


Figure 3: APT Protection Market Quadrant, 2023*

* Radicati Market QuadrantSM is copyrighted March 2023 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market QuadrantsSM 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 QuadrantsSM 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, ESET, Trellix, and Cisco*.
- The **Trail Blazers** quadrant includes *Bitdefender*.
- The **Specialists** quadrant includes *Sophos, Microsoft, Palo Alto Networks, and VMware Carbon Black*.
- There are no **Mature Players** in this market at this time.

APT PROTECTION - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

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

Symantec offers a wide range of security solutions (network, endpoint, information and identity) for the enterprise market. Symantec operates one of the largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. Symantec is an operating division of Broadcom, a publicly traded company.

SOLUTIONS

Symantec provides network, endpoint, information 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 as on-premises, cloud or hybrid deployments. 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 Network Protection*** – is an enterprise-grade, cloud-delivered SaaS solution, with the Symantec Secure Web Gateway at its core to block known threats, malicious sources, risky sites, unknown content categories, and malware delivery networks at the gateway in real-time. Network Protection provides these capabilities through an integrated collection of threat protection technologies with a user-based license that allows deployment in the cloud, on-premises, or hybrid deployments. Key capabilities include:
 - *Symantec proxy-based SWG* – can be deployed either through cloud-hosted SWG, on-premises as an appliance, or a virtual machine and is powered by Symantec Intelligence Services. It categorizes, 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 the cloud or on-premises SWG 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.

 - *Symantec Zero Trust Network Access (ZTNA)* – enables security and IT teams to create a Zero Trust application access architecture and cloak all unauthorized network resources, without the need for traditional VPN appliances.

 - *Management Center and Reporting* – offers centralized management and reporting capabilities for Network Protection and enables consistently applied security policies.

- ***Symantec Security Analytics*** – utilizes high-speed network traffic analysis and full-packet capture, indexing, and deep packet inspection (DPI) to enable incident response and eradicate threats that may have penetrated the network. It can be deployed as an appliance, virtual appliance or in the cloud, providing full visibility and forensics. 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 (SES) Complete*** – 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, Adaptive Incidents, Threat Intelligence Integration and Threat Hunter to provide 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.

 - *XDR* – correlates events and incidents from CloudSOC with those observed in SES Complete. Through visibility provided by CloudSOC into additional control points, such as Secure Web Gateway (Symantec Web Protection), and DLP (included in DLP Cloud), XDR allows analysts to quickly investigate IOCs and understand related response actions.

 - *Adaptive Incidents* – leverages Adaptive Technology in SES Complete using AI and contextual analysis to automatically separate normal from suspicious behavior.

 - *Threat Hunter* – assists SOCs by combining Symantec’s expert analyst research with advanced machine learning and global threat intelligence to provide alerts, insights and guidance related to unfolding attacks.

- *Upgrading from SEP to SES Complete* – does not require the installation of a new agent, as both use the same agent. SESC can be deployed as cloud-managed, on-premises, or a hybrid modality. SES Complete 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 affected endpoints while investigating threats using a choice of on-premises and cloud-based sandboxing.
- ***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, machine learning, artificial intelligence, web isolation, ZTNA, CASB, and more. 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.
- Symantec Security Analytics, coupled with Symantec SSL 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 experienced security teams. However, some of Symantec's cloud solutions, with simplified licensing, offer streamlined protection for smaller customers.
- While customers can use SES Complete and Symantec ITMS (Altiris) products together to support workflows for patch management and remediation, these 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** – 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, ESET Mail Security, ESET LiveGuard Advanced products, ESET Inspect is a cloud-delivered, multitenant, 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**) – 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 service** – provides global knowledge, gathered by ESET experts, on targeted attacks, advanced persistent threats (APTs), zero-days and botnet activities. Informed by ESET Intelligence Feeds, it helps organizations improve their proactive security posture and enhance their threat hunting and remediation capabilities. ESET's Premium APT Reports package includes in-depth technical reports describing recent campaigns, toolsets, and tactics, providing in-depth contextual detail on adversaries' actions aimed at the needs of C-level personnel, specialized SOC staff or national CERTs.

STRENGTHS

- ESET PROTECT is a unified single-click security management platform which includes ESET Inspect to deliver extended detection and response (XDR) with granular visibility, risk assessment, incident response, investigation, and remediation. It supports all major operating systems (i.e., Windows, macOS, and Linux).
- ESET solutions offer multi-language support and a large set of localized versions.
- ESET Endpoint security solutions use Intel® TDT as an additional source of threat telemetry to assist in the detection of threats which use advanced evasion techniques, such as zero-day variants, binary obfuscation, cloaking in a virtual machine, and fileless attacks.
- Customers appreciate ESET solutions for their ease of deployment and ease of use.

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. However, the vendor is working on delivering a Connect Cloud Gateway solution that will serve as a central hub for integration with third party solutions, including CASB solutions.

- ESET currently lacks visibility in North America. The vendor is working on to address this.

TRELLIX

6220 America Center Dr.

San Jose, CA 95002

www.trellix.com

Trellix is a cybersecurity company founded in 2022 when a consortium led by Symphony Technology Group (STG) acquired and merged McAfee Enterprise and FireEye. Trellix offers security solutions, threat intelligence and services that protect business endpoints, networks, servers, the Cloud and more. Trellix is privately held.

SOLUTIONS

Trellix Intelligent Virtual Execution (IVX) 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, Intelligent Virtual Execution 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.

IVX 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, IVX integrates with other solutions to make immediate decisions about next steps.

ATD plugs in and integrates out-of-the-box with other Trellix solutions, including:

- Trellix EDR
- Trellix ePolicy Orchestrator (ePO)
- Trellix Intrusion Prevention System (IPS)
- Trellix Threat Intelligence Exchange: including Application Control, Endpoint protection, Security for Email Servers, and Server Security.

These integrations operate directly or over the Data Exchange Layer (DXL), which serves as the information broker and middleware messaging layer for Trellix security products. Trellix 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. IVX also supports third party email gateways, and integration with BRO-IDS, an open source network security monitor.

STRENGTHS

- IVX is available through flexible deployment options, which include appliance, virtual appliance and cloud form factors with CapEx and OpEx purchase options. IVX is also available through the AWS Marketplace.

- Combination of in-depth static code, machine learning and dynamic analysis through sandboxing, provide strong analysis and detection capabilities.
- Tight integration between IVX and security solutions directly, through APIs, open standards or the Trellix Data Exchange Layer (DXL), allows instant information sharing and action across the network when malicious files are detected. Trellix Security Innovation Alliance partners can also integrate to publish and subscribe to DXL threat intelligence.
- IVX 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

- IVX does not support Apple macOS, or Linux platforms.
- Cloud deployment is not currently available on Azure.
- IVX mobile malware inspection is only available for Android (.apk) applications. However, management and protection for iOS and Android devices is provided through Trellix Mobile Security.
- For remediation, Trellix 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 Trellix Endpoint Security (ENS).
- While highly capable, Trellix solutions are a best fit for medium to large customers with adequate budgets.

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 – 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 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 third-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 crypto mining, 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 – 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. Through 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 all Cisco security 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.
- 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.

TRAIL BLAZERS

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, protection, detection, and response solutions worldwide. The company has customers in 170 countries and offices around the world. The company is privately held.

SOLUTIONS

Bitdefender GravityZone is a hosted enterprise security platform that provides security controls and security posture management across endpoints, cloud workloads, networks and users. Organizations which favor on-premises deployments can leverage the flexibility of GravityZone to deploy it as a virtual-appliance-based on-premises private cloud. Bitdefender security tools support an exceptional variety of contemporary platforms including Windows, Linux, Mac, Android, iOS and Microsoft Exchange.

Bitdefender also delivers Extended Detection and Response (XDR), Managed Detection and Response (MDR), as well as a comprehensive set of security packages and optional add-on products and services.

GravityZone XDR delivers threat protection, detection, and response with out-of-the-box analytics, allowing correlation of disparate alerts and enabling security teams to rapidly triage and respond to incidents across identity, network, email, cloud, and endpoints.

Bitdefender Managed Detection and Response (MDR) gives companies 24x7 access to a team of cybersecurity experts. It combines endpoint, network, cloud, identity, and productivity application telemetry into actionable security analytics, augmented by the threat-hunting

expertise of a fully staffed security operations center (SOC) with security analysts from global intelligence agencies.

Bitdefender security packages include:

- **GravityZone Business Security Enterprise** (formerly known as GravityZone Ultra) – combines endpoint protection with endpoint detection and response (EDR) capabilities to defend the endpoint infrastructure (workstations, servers, and containers) throughout the threat lifecycle. Cross-endpoint event correlation combines EDR with the infrastructure-wide analytics of XDR (eXtended Detection and Response).
- **GravityZone Business Security Premium** (formerly known as GravityZone Elite) – is an integrated endpoint protection, risk management, and attack forensics platform which includes all the APT protection capabilities of GravityZone Business Security Enterprise, 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** – is an 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 managed from the same GravityZone platform:

GravityZone Security for Email – provides comprehensive email security and protection from known and emerging threats, including impersonation attacks, Business Email Compromise (BEC), CEO fraud, phishing, ransomware and more.

GravityZone Patch Management – empowers organizations to keep their operating systems and software applications up to date and gain a comprehensive view of the patch status across their entire Windows install base. It delivers updates for an organization’s entire fleet of workstations, physical servers, or virtual servers.

GravityZone Full Disk Encryption – encrypts boot and non-boot volumes on fixed disks, desktops and laptops and gives you simple remote management of the encryption keys. It provides centralized handling of the native device encryption mechanisms provided by Windows (BitLocker) and Mac (FileVault and the diskutil command-line utility) to ensure optimal compatibility and performance.

GravityZone Security for Mobile Devices – helps organizations maintain compliance and enforce bring-your-own-device (BYOD) policies for mobile devices.

GravityZone Security for Servers – includes dedicated server protection and detection technologies, designed for the hybrid and multi-cloud environments.

GravityZone Security for Containers – protects container workloads against Linux and container attacks using AI threat prevention, Linux-specific anti-exploit technologies, and context-aware endpoint detection and response (EDR).

GravityZone Integrity Monitoring – helps organizations meet compliance and regulatory security standards by monitoring the integrity of entities such as files, registries, directories, installed applications, and users for escalation of privilege throughout the organization.

GravityZone Security for Storage delivers proven protection for ICAP-compatible file-sharing and network storage systems that is easy to manage.

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.

- GravityZone offers integration of endpoint-to-endpoint correlation with cloud, identity, productivity apps, and network sensors to extend the detection capabilities and help reduce attack dwell time. It also delivers complex EDR/XDR results in a human-readable format with guided actions to help reduce complexity for IT teams.

WEAKNESSES

- Bitdefender 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 and mid-market products and lacks greater visibility in the enterprise market. The vendor is working to address this.

SPECIALISTS

SOPHOS

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

Sophos offers IT security solutions for businesses, which include endpoint, encryption, email, next-generation firewall (NGFW), mobile security and unified threat management. All solutions are managed through Sophos Central, a cloud-based management platform, backed by

SophosLabs, its global network of threat intelligence centers. Sophos is owned by private equity firm Thoma Bravo and headquartered in Oxford, U.K.

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 MDR**, and **Intercept X Advanced with MDR Complete**, 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. Intercept X Advanced with MDR includes Sophos **Managed Detection and Response (MDR)**, a 24/7 managed detection and response service. Intercept X Advanced with MDR Complete offers increased MDR support through full-scale incident response, root cause analysis, and dedicated incident response lead. All four plans can optionally add **Sophos Zero Trust Network Access (ZTNA)** gateways or cloud-delivered Sophos ZTNAaaS, which delivers secure remote access to applications, data and services based on clearly defined access control policies.

- **Sophos Firewall** – is Sophos’ flagship next-generation firewall which provides comprehensive Web Gateway and SD-WAN 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, allowlisting, 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 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 MDR*, and *Intercept X Advanced for Server with MDR Complete*) 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.
- *Live Discover* – 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.
- *Live Response* – 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 MDR 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.
- Sophos solutions are aimed at small to mid-size organizations which don't require a great deal of customization or integration with existing infrastructure.

MICROSOFT

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

Microsoft offers 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, XDR, automatic investigation and remediation, managed hunting, and unified security management. It is available in two plans: P1 included with Microsoft 365 E3 licenses, or P2 included with Microsoft 365 E5 licenses. A Microsoft Defender Vulnerability Management add-on which provides discovery, assessment, prioritization and remediation of endpoint vulnerabilities or misconfigurations is also

available for P2 customers. MDE 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, however, feature parity is not always 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 training, and cross-domain XDR capabilities.

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.

- **Microsoft 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** – 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 is investing heavily in its security solutions portfolio, to deliver an impressive ecosystem of solutions that encompass the OS, applications, and services. In particular, Microsoft continues to work diligently to address on-going customer concerns over spam, spoofing, phishing attacks, as well as blended attacks which may occur through attachments and harmful URLs.
- 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 Defender for Endpoint is a good first step for organizations looking for an entry-level EDR solution.
- Microsoft ATP cloud-based solutions are easy to deploy and manage for customers of all sizes.

WEAKNESSES

- Microsoft offers many different plans at different price points, but it is often 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 will typically need to upgrade to the high-end Microsoft 365 E5 enterprise license.

- While Microsoft has been investing heavily in its anti-malware, anti-spam, 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-premises 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.

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.

Palo Alto Networks also offers the **WildFire WF-500-B** appliance, which 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 strong expertise in threat detection through its Unit 42 threat research team.
- 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-premises solution is not available in a virtual form factor.
- Palo Alto Networks' WildFire, has lost some mindshare as many competing vendors are now offering similar functionality.
- Customers report that they would like to be able to customize the WildFire solution more closely, through the manual submission of malicious files and urls, as well as the ability to define rule-based analysis.

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. In May 2022, Broadcom announced its intent to acquire VMware and re-brand itself as VMware.

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 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.
- **VMware Carbon Black Container** – offers continuous visibility, security and compliance for containers and Kubernetes applications from development to production. It supports the creation of customizable policies to ensure secure configuration and compliance with organizational requirements and industry standards (e.g., CIS benchmarking). It helps enforce policies from build to deployment to detect vulnerabilities and misconfigurations to

prevent them from being deployed to production.

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 it 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 supports mobile security functionality only through integration with VMware Workspace ONE Mobile Threat Defense.
- VMware Carbon Black Cloud does not offer its own DLP, however, integrations with third party DLP solutions are possible through the platform's open APIs.
- VMware Carbon Black Cloud does not provide device control.
- VMware Carbon Black Cloud currently only offers application control capabilities through an on-premises application control product. The vendor views this as a benefit for high security, disconnected uses such as banking, finance and government applications.
- At the time of this writing, it is too early to know how the Broadcom acquisition of VMware will affect the Carbon Black brand, as Broadcom already has a sizeable portfolio of security solutions from previous acquisitions.

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**
- **Social Media**
- **Instant Messaging**
- **Archiving & Compliance**
- **Wireless & Mobile**

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:

- Strategic Business Planning
- Management Advice
- Product Advice
- TCO/ROI Analysis
- Investment Advice
- Due Diligence

MARKET RESEARCH PUBLICATIONS

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

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