The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Endpoint Security - Market Quadrant 2023 *

An Analysis of the Market for Endpoint Security Revealing Top Players, Trail Blazers, Specialists and Mature Players.

March 2023

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.

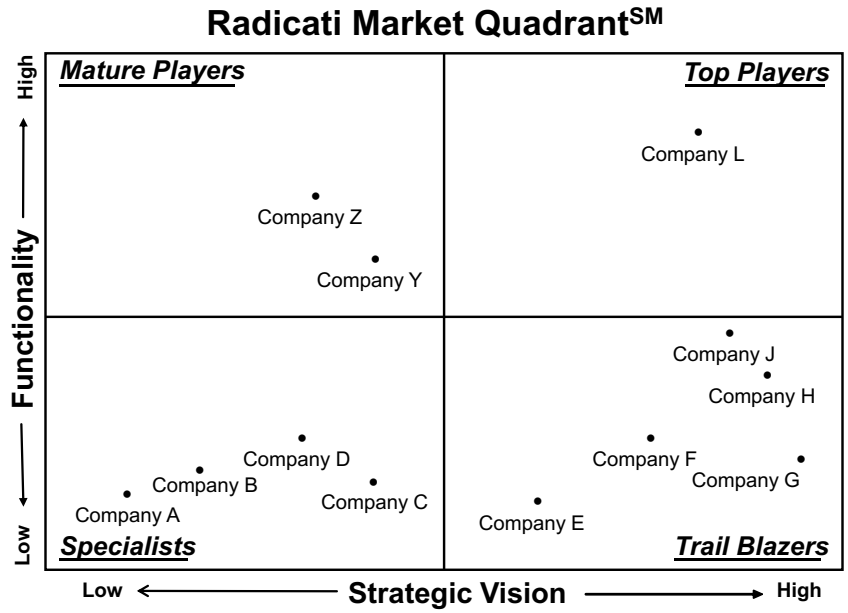

Figure 1: Sample Radicati Market Quadrant

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 – ENDPOINT SECURITY

This edition of Radicati Market Quadrants[SM] covers the "**Endpoint Security**" segment of the Security Market, which is defined as follows:

- **Endpoint Security** – are appliances, software, cloud services, and hybrid solutions that help to secure and manage endpoints for business organizations of all sizes. Endpoint security solutions must be able to prevent, detect, block and remediate all threats to the endpoint. Often these solutions also combine deep forensic capabilities, and managed services for threat hunting and neutralization. Leading vendors in this market, include: *Bitdefender, Cisco, CrowdStrike, Cybereason, ESET, Microsoft, OpenText, SentinelOne, Sophos, Symantec, Trellix, Trend Micro, VMware Carbon Black, WatchGuard,* and *WithSecure*.

- Vendors in this market often target both consumer and business customers. However, this report deals only with solutions aimed at businesses, ranging from SMBs to very large organizations. Government organizations are considered "business/corporate organizations" for the purposes of this report.

- The line between traditional and next generation endpoint solutions no longer exists as nearly all vendors offer behavior-oriented solutions which include endpoint detection and response (EDR) or extended detection and response (XDR), sandboxing, advanced persistent threat (APT) protection, managed detection and response (MDR), and more.

- Organizations no longer view endpoint security as an isolated discipline affecting only the endpoint but as an integral part of an organization-wide defense posture, where endpoint security shares threat intelligence feeds and policy controls with all other major security components, including firewalls, secure web gateways, secure email gateways, data loss prevention (DLP), and more.

- The endpoint security market is seeing strong growth as organizations of all sizes deploy sophisticated and feature-rich solutions to help protect against all threats and malicious attacks. The Endpoint Security market is expected to reach $13.4 billion in 2023, and grow to over $29.7 billion by 2027. Figure 1, shows the projected revenue growth from 2023 to 2027.

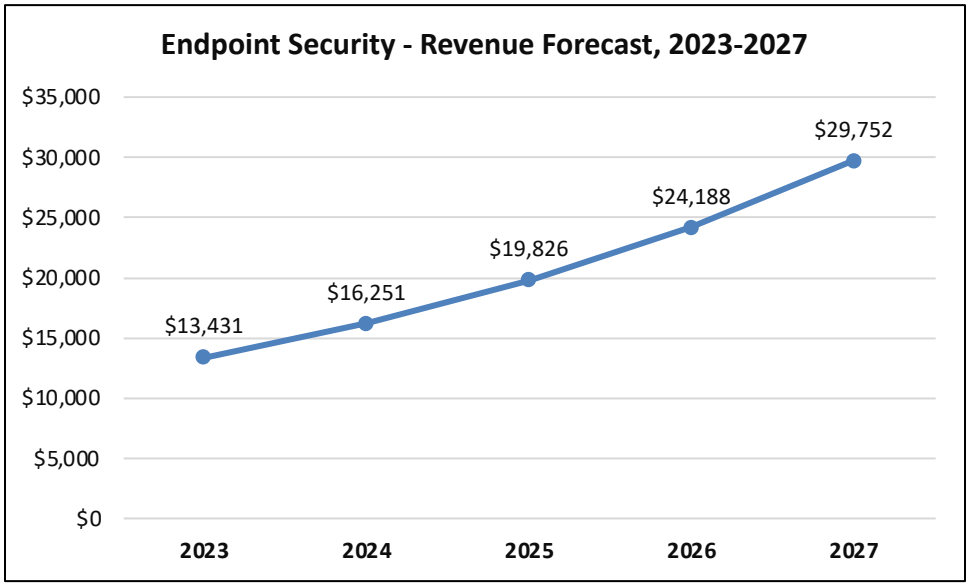

Figure 2: Endpoint Security Market Revenue Forecast, 2023-2027

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 *Endpoint Security* 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, appliance and/or virtual appliance, cloud-based services, or hybrid.

- ***Platform Support*** – the range of computing platforms supported, e.g., Windows, macOS, Linux, iOS, Android, and others.

- ***Malware detection*** – is usually based on signature files, reputation filtering (proactive blocking of malware based on its behavior, and a subsequent assigned reputation score), and proprietary heuristics. The typical set up usually includes multiple filters, one or more best-of-breed signature-based engines as well as the vendor's own proprietary technology. Malware engines are typically updated multiple times a day. Malware can include spyware, viruses, worms, rootkits, and much more.

- ***Antivirus Removal Tools*** – serve to uninstall previously used security software on a user's machine. Running multiple security solutions on one device can cause conflicts on the endpoints, which can result in downtime.

- ***Directory integration*** – can be obtained via Active Directory or a variety of other protocols, such as LDAP. By integrating with a corporate directory, organizations can more easily manage and enforce user policies.

- ***Firewall*** – functionality typically comes with most endpoint security solutions, and offers a more granular approach to network protection, such as blocking a unique IP address. Intrusion prevention systems are also commonly included as a feature in firewalls. Intrusion detection and prevention systems protect against incoming attacks on a network.

- ***URL Filtering*** – enables organizations to manage and control the websites their employees are allowed to visit. Solutions can block particular websites, or define categories of websites (e.g. gambling) to block, as well as integrate with sandboxing and or threat intelligence feeds to detect and stop malicious URLs.

- ***Third Party Patch Assessment*** – is a common feature included in many endpoint security solutions. It serves to inventory software on protected endpoints to determine if any of the software on the endpoint is out-of-date. It is meant to alert administrators about important software updates that have not yet been deployed.

- ***Third Party Patch remediation*** – lets administrators deploy a missing software update discovered during the patch assessment phase. It should be possible for administrators to deploy software updates directly from the management console.

- ***Reporting*** – lets administrators view activity that happens on the network. Endpoint Security solutions should offer real-time interactive reports on user activity. Summary views to give an overall view of the state of the network should also be available. Most solutions allow organizations to run reports for events that occurred over the past 12 months, as well as to archive event logs for longer-term access.

- ***Web and Email Security*** – features enable organizations to block malware that originates from web browsing or emails with malicious intent. These features are compatible with applications for web and email, such as browsers, email clients, and others. These features also help block blended attacks that often arrive via email or web browsing.

- ***Device control*** – allows control on the use of devices on endpoints, such as USB drives, CD/DVDS, and more. Some solutions provide only basic binary control policies (i.e.

allow/disallow), while others allow more granular controls, e.g. blocking a device by user, or group of users, and more.

- ***Encryption*** – support for full-disk encryption (FDE) to lock an entire drive, or file-based encryption to lock specific files.

- ***Network access control (NAC)*** – lets administrators block network access to certain endpoints for various reasons. It is commonly used to bar new endpoints from joining the network that have yet to deploy the organization's security policies.

- ***Mobile device protection*** – many endpoint security vendors integrate some form of mobile protection into their endpoint solutions. Some endpoint security vendors offer mobile protection through separate add-ons for Mobile Device Management (MDM) or Enterprise Mobility Management (EMM).

- ***Data Loss Prevention (DLP)*** – allows organizations to define policies to prevent loss of sensitive electronic information. There is a range of DLP capabilities that vendors offer in their solutions, ranging from simple keyword-based detection to more sophisticated Content-Aware DLP functionality.

- ***Administration*** – should provide easy, single pane-of-glass management across all users and resources. Many vendors still offer separate management interfaces for their on-premises and cloud deployments. As more organizations choose a hybrid deployment model, an integrated management experience that functions across on-premises and cloud is required.

- ***Sandboxing*** – does the solution include sandboxing capabilities or integrate with a third-party sandboxing solution for pre- or post-execution malware detection.

- ***Advanced Persistent Threat (APT)*** – endpoint protection solutions should integrate with APT solutions for real-time threat correlation across the entire customer environment.

- ***EDR/XDR*** – endpoint protection solutions should include Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solutions or integrate with third party EDR/XDR solutions.

- ***Managed Detection and Response (MDR)*** – managed services which allow organizations to outsource their security services for 24/7 threat detection, response and remediation.

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 – ENDPOINT SECURITY

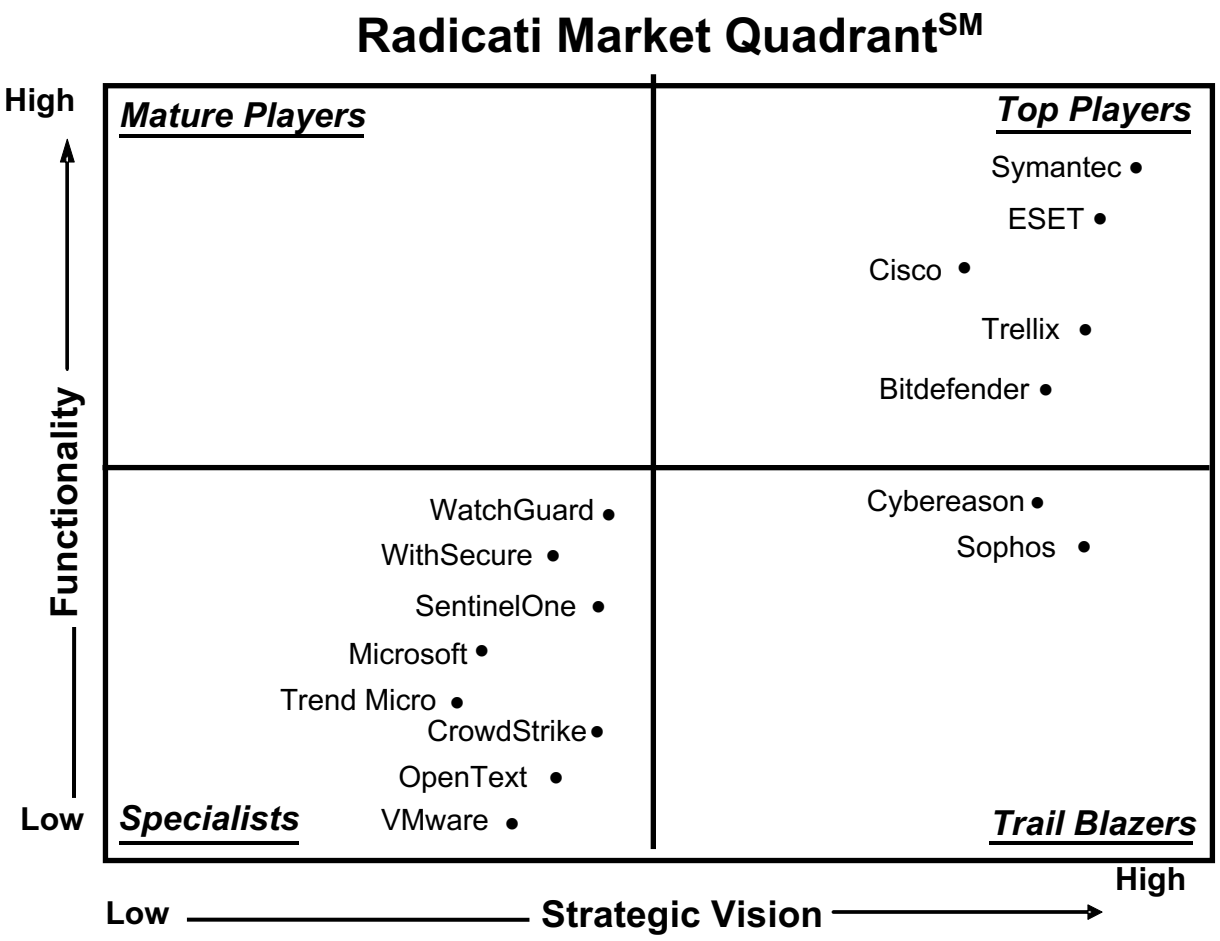

Figure 3: Endpoint Security Market Quadrant, 2023*

* Radicati Market Quadrant℠ is copyrighted March 2023 by The Radicati Group, Inc. This report has been licensed for distribution. Only licensee may post/distribute. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT TRENDS

- The **Top Players** in the Endpoint Security market are *Symantec, ESET, Cisco, Trellix* and *Bitdefender.*

- The **Trail Blazers** quadrant includes *Cybereason,* and *Sophos.*

- The **Specialists** in this market are *WatchGuard, WithSecure, SentinelOne, Microsoft, TrendMicro, CrowdStrike, OpenText* and *VMware Carbon Black.*

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

ENDPOINT SECURITY - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

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

Symantec (a division of Broadcom Software) 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. Broadcom is publicly traded.

SOLUTIONS

Symantec Endpoint Security solutions are powered by the Symantec Global Intelligence Network that offers real-time updates to prevent attacks, stop breaches, and mitigate risk. Symantec offers the following endpoint protection solutions:

- **Symantec Endpoint Security (SES) Complete –** supports on-premises, cloud, and hybrid options for deployment and management. It delivers artificial intelligence-guided security

management by combining multiple technologies to address threats across the entire attack chain. Protections begin with Symantec Endpoint Protection which delivers: malware protection, advanced machine learning, behavioral analysis, reputation filtering, exploit and intrusion prevention, deception, mail security, web security, firewall, device control, antivirus removal tools, recovery tools, reporting, REST APIs, and integration with Symantec intelligent threat cloud capabilities. The solution also includes Mobile Threat Defense, Endpoint Detection and Response (EDR), Threat Hunter, protections against Active Directory exploits, attack surface reduction capabilities, such as Adaptive Protection, application control, and extended operating system protections. It protects all endpoints including workstations, laptops, mobile phones, tablets, and servers and is compatible with Windows, macOS, Linux, Android, iOS, VMware ESX, Citrix XenServer, and other virtual machines. The solution is managed from a centralized console, which supports the definition of granular management policies. Key capabilities include:

- *Adaptive Protection* – blocks behaviors of trusted applications utilized in Living-off-the-land enabled threats with no operational impact.

- *Application Control* – assesses the risk level of applications and their vulnerabilities, and allows only "known good" applications to run.

- *Active Directory Security* – automatically learns an organization's entire Active Directory structure and uses obfuscation to prevent attackers from stealing credentials and moving laterally within the organization.

- *Endpoint Detection and Response (EDR)* – detects advanced attacks, provides real-time analytics, and enables SOC teams to actively hunt threats and pursue forensic investigations and remediation.

- *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 Symantec's Adaptive Technology in SES Complete using AI and contextual analysis to automatically separate normal from suspicious behavior.

- *Threat Intelligence API* – provides access to Symantec's Global Intelligence Network (GIN). Through API integration into partners with SIEM/SOAR/TIP, SOC teams can easily identify the scope of an attack and streamline their threat investigations.

- *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.

- *Advanced mobile threat defense* – uses predictive technology in a layered approach that leverages crowd-sourced threat intelligence, in addition to device and server-based analysis, to proactively protect mobile devices from malware, network threats, and application or OS vulnerability exploits.

Symantec **Endpoint Security Enterprise** is another option in the Symantec endpoint portfolio, which offers a subset of the Symantec Endpoint Security Complete capabilities including Symantec Endpoint Protection, mobile threat defense and flexible deployment options across cloud, on-premises, and hybrid.

STRENGTHS

- Symantec offers a single management console to protect Windows, macOS, Linux, iOS, Android, Embedded and Virtual machines, as well as a single integrated agent on the endpoint for seamless management and performance. Hybrid management options, combining on-premises and cloud also are available.

- Symantec Endpoint Security offers multi-layered protection powered by artificial intelligence and advanced machine learning to provide prevention, detection and response, as well as deception, Active Directory security, Adaptive Protection, application control, XDR and Adaptive Incidents.

- Symantec Endpoint Security has built-in EDR capabilities, including Threat Hunter which combines advanced machine learning with Symantec's SOC analyst expertise.

- The level of granularity and flexibility in the management console is higher than that of many competing solutions in the market.

- The firewall functionality included can block unique IP addresses and leverages reputation analysis from Symantec's Global Intelligence Network. It can also do behavioral analysis and apply application controls.

- Symantec solutions are well aimed at the complex needs of large multinational enterprise customers.

WEAKNESSES

- Endpoint management (ITMS) is available primarily as an on-premises managed solution.

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

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

- Symantec sold its Managed Services business, including its MDR services, to Accenture. It now offers MDR services in partnership with Accenture.

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 Endpoint protection solutions include the following components:

- **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 many more. The ESET PROTECT platform provides over 170 built-in reports and allows organizations to create custom reports from over 1000 data points.

- **ESET Endpoint Security for Windows –** is ESET's flagship endpoint security product for Windows. It offers a low footprint, support for virtual environments, and combines reputation-based malware protection with advanced detection techniques enhanced by ESET's machine learning engine, Augur.

- **ESET Endpoint Security for macOS** – is ESET's security product for macOS platforms. Similarly, to its Windows counterpart, it offers a low footprint, support for virtual environments, cross-platform protection, and combines reputation-based malware protection with advanced detection techniques enhanced by ESET's machine learning engine Augur.

- **ESET Endpoint Security for Android –** offers reputation-based malware protection, anti-phishing, app control, web control, anti-theft, SMS/call filtering and device security. It integrates with ESET PROTECT, allowing for security policies to be deployed across both PCs and mobile devices.

- **ESET Server Security for Microsoft Windows Server –** is a lightweight server security product, which integrates with the ESET LiveGrid reputation technology for advanced detection techniques. It features support for virtualization (e.g., optional snapshot independence, process exclusions, clustering support), Hyper-V and Network Attached Storage scanning, and a Windows Management Instrumentation (WMI) connector. It is also available as a VM Extension in Microsoft Azure.

- **ESET Security for Microsoft SharePoint Server –** provides advanced protection for SharePoint servers to protect against malicious uploads and unwanted files.

- **ESET Mail Security for Microsoft Exchange and IBM Servers** – combines server malware protection, spam filtering, web-based quarantine, email scanning and optional Cloud Sandbox analysis. It includes the malware protection technology included in ESET Endpoint solutions (i.e., ESET LiveGrid reputation technology, ESET machine learning engine Augur, Anti-Phishing, Exploit Blocker, and Advanced Memory Scanner), proprietary antispam engine, and selective database on-demand scanning.

- **ESET Full-Disk Encryption** – is an add-on to ESET Endpoint solutions enabling full disk encryption across the entire network from a cloud based ESET PROTECT console with a single click. It can encrypt system disks, partitions, and entire drives.

- **ESET Endpoint Encryption** – is a standalone solution which provides data encryption, including full-disk encryption (FDE), as well as files, folders, removable media, and email encryption.

In addition, ESET provides the following services and solutions:

- **ESET Inspect** – is ESET's XDR-enabling component of the ESET PROTECT platform, delivering breach prevention, enhanced visibility, and remediation. Provides risk managers and incident responders with threat and system visibility, allowing them to perform in-depth root cause analysis and immediately respond to incidents.

- **ESET LiveGuard Advanced** – is ESET's cloud-based advanced threat defense that uses advanced scanning, machine learning, cloud sandboxing and in-depth behavioral analysis to prevent targeted attacks as well as new or unknown threats, especially ransomware.

- **ESET's Threat Intelligence Reports & Feeds** – is ESET's threat intelligence service for detection of Advanced Persistent Threats (APTs), blocking of suspicious domains and IOCs (Indicators of Compromise), prevention of botnet or phishing attacks.

- **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.

- **ESET NetProtect** – is ESET's DNS security solution for CSPs (Content Service Providers). It provides protection on the network / internet provider level against malicious domains and inappropriate content while browsing the internet.

- **ESET Premium Support** – is ESET's cybersecurity service which offers 365/24/7 tailored support through access to a team of ESET experts.

- **Security Services for Endpoints** – works together with ESET endpoint security products to deliver a complete security solution that works to prevent and react proactively. It reinforces IT security teams with on-call support from ESET experts.

- **ESET Secure Authentication** – is a mobile-based multi-factor authentication (MFA) solution that protects organizations from weak passwords and unauthorized access.

- **ESET Cloud Office Security** – provides advanced preventive protection for users of Microsoft 365 applications.

STRENGTHS

- ESET solutions offer a low footprint with low system resource usage.

- ESET's management console, ESET PROTECT, provides real-time visibility for on premise and off premise endpoints, as well as full reporting for ESET enterprise-grade solutions from a single pane of glass securely deployed on premise or in the cloud. It covers desktops, servers, agentless virtual machines, and managed mobile devices.

- ESET has a global network of installed business solutions that feed information back into the ESET LiveGrid, its cloud-based reputation system.

- ESET Endpoint Security is well suited to offer protection for companies with heterogeneous environments (e.g., Windows, macOS, and Linux).

- 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 is widely recognized in Europe but currently lacks market visibility in North America. The vendor is working 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 Secure Endpoint is a cloud-based endpoint security solution designed to detect, prevent, and remediate advanced threats. It provides a holistic view of servers and endpoints running Windows, Mac, Android, Apple iOS, Linux, as well as virtual systems. It is available through a public or on-premises private cloud deployment model.

Secure Endpoint integrates with **Cisco SecureX**, a human-driven platform which brings XDR, incident management and automated playbooks to the entire security portfolio; **Cisco Umbrella**, a cloud-driven secure internet gateway which extends protection to devices, remote users and distributed locations; **Cisco Duo**, a multi-factor authentication solution that verifies user identity before allowing access to corporate resources.

Secure Endpoint comes with the following key capabilities:

- *Threat Prevention* – is provided through layered security capabilities which include file reputation, traditional anti-virus, cloud-based sandboxing, file-less in-memory exploit prevention, system process protection, ransomware protection and dynamic behavior-based protection. Cisco Secure Endpoint can automatically detect and block known and emerging threats through real time technologies that include: behavior analysis, big data analytics, machine-learning, signatures and fuzzy fingerprinting. File analysis reports provide detailed behavioral indicators of compromise with mappings applicable to the MITRE ATT&CK framework. Cisco Talos further augments threat intelligence dynamically through the cloud or content updates to the various engines.

- *Threat Detection* – Secure Endpoint provides continuous monitoring and detection of files already on endpoints to help identify malicious behavior and decrease time to detection. Additionally, SecureX, built-in to Secure Endpoint helps accelerate incident investigations through automatic context enrichment and allows customers to leverage Cisco incident management playbooks, as well as create their own automated playbooks.

- *Threat Response* – Secure Endpoint provides a suite of response capabilities to contain and eliminate threats across all endpoints. Native integration between Cisco Secure Endpoint and Duo allows customers to automatically prevent compromised endpoints from being used as trusted devices for multi-factor authentication. In addition, SecureX provides threat context enrichment and extends response capabilities by allowing customers to configure or use Cisco curated workflows to automate response actions across the entire security infrastructure.

- *Email and Web security* – all file disposition and dynamic analysis information is shared across the Cisco Secure Ecosystem via collective intelligence. If a file is determined to be malicious via Cisco Secure Email or Web Appliance, that information is shared across all Cisco Secure platforms. SecureX orchestration enables to streamline Cisco curated or customer configured workflows between Secure Email and Secure Endpoint for automated cross layer investigation and response actions.

- *Firewall* – Secure Endpoint integrates with Cisco Secure Firewall. All detection information is sent to the Cisco Secure Firewall management platform and can be used to correlate against other network threat activity. Cisco Firewall and Cisco Identity Services Engine

(ISE) can be tightly integrated, which allows Secure Endpoint events to trigger policy responses and enforcement in ISE.

- *Patch Assessment* – Secure Endpoint uses a feature called Vulnerable Software that identifies if the installed software is up to date according to the vendor, or if the installed version has an exploitable vulnerability. Additionally, the advanced live search in Secure Endpoint built on top of osquery provides cataloged queries to identify Windows hotfixes and/or patch levels of the endpoint, providing scannerless patch assessment directly on the endpoint. SecureX orchestration further provides a repository of (extensible) sample automations that customers leverage to hunt for and confirm critical vulnerabilities.

- *Reporting* – Secure Endpoint offers static, dynamic, and historical reports. These include reporting on high-risk computers, overall security health, including vulnerable software and virus definition update status, threat root cause activity tracking, identification of various APTs, Advanced Malware assessments, and mobile-specific root cause analysis.

- *Management* – Secure Endpoint comes with its own management console and can also integrate with the Cisco Secure Firewall console (for Cisco NGIPS or Cisco Secure Firewall deployments) to deliver tighter management across all deployed Cisco security solutions.

- *Integrations* – Secure Endpoint has an API that allows customers to sync Secure Endpoint with other security tools or SIEMs. These integrations have grown from SIEM/SOAR/MDM integrations to include SOC and managed threat detection and response platforms.

Cisco AnyConnect Secure Mobility Client offers VPN access through Secure Sockets Layer (SSL), endpoint posture enforcement and integration with Cisco Secure Web Appliance. It assists with the deployment of Secure Endpoint, and expands endpoint threat protection to VPN-enabled endpoints, as well as other Cisco AnyConnect services.

STRENGTHS

- Cisco offers a broad security portfolio, which encompasses threat intelligence, heuristics, behavioral analysis and sandboxing. Cisco has also integrated unified access security and multi-factor authentication capabilities from its Duo Security acquisition.

- Built-in to Cisco Secure Endpoint, the Cisco SecureX platform delivers threat response with

automatic threat context enrichment and unified threat response capabilities across the Cisco Secure Ecosystem, including Endpoints, Network, Email, DNS, and more.

- Cisco Secure Endpoint offers rich native integrations to Cisco Firewall, Secure Email, Umbrella DNS Security and other Cisco security solutions to provide network edge to endpoint visibility.

- Cisco offers APIs for their endpoint solutions (as well as Secure Malware Analytics and Cisco Umbrella solutions) to integrate with a customer's existing security architecture, as well as other security tools or SIEMs.

- Customers report that Secure Endpoint is easy to use, and highly efficient in dealing with prevention and remediation.

WEAKNESSES

- While Cisco Secure Endpoint can automatically disable Microsoft Defender, it does not provide features to help uninstall other previously installed third party security software.

- While Cisco Secure Endpoint offers third party software patch assessment, it does not offer third party patch software remediation. However, it does integrate with third party ticketing systems to automatically raise tickets for patch remediation.

- Cisco Secure Endpoint does not provide its own content aware DLP functionality, however it integrates with Digital Guardian through Secure Malware Defense.

- Secure Endpoint does not offer native full-disk encryption (FDE), however SecureX device insights however provide customers with visibility into the status of the endpoint's underlying operating system encryption capabilities.

- While Cisco Secure Endpoint can be deployed independently of other Cisco security solutions, it's full strength and rich functionality is best leveraged when deployed in conjunction with other Cisco security solutions.

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 Endpoint Security offers a full range of security and data protection capabilities which can be deployed in a variety of modes, including cloud, on-premises or hybrid. It comprises the following capabilities:

Trellix Endpoint Security (ENS) – is an endpoint protection platform (EPP), which uses machine learning analysis, analytics for file-less attacks, dynamic application containment, and works with local and global threat intelligence to provide comprehensive insights across all threat vectors: file, web, message, and network. Trellix endpoint security solutions are compatible with Windows workstations and servers, macOS, Linux and virtual platforms. In-depth defenses collaborate to inform, analyze and automate responses.

Trellix Endpoint Detection and Response (EDR) – is a cloud-native management console which offers cloud-based EDR to provide automated, AI-guided investigations for security practitioners of any experience level. It works with Trellix Endpoint Security, as well as with third-party endpoint security solutions.

Trellix Endpoint Forensics – performs fast, targeted investigations across thousands of endpoints by sweeping thousands of endpoints for evidence of compromise, including malware and irregular activities. It enables remote investigation securely over any network, without requiring access authorization, and collects targeted forensic data with intelligent filtering to return only needed data.

Threat Insights – leverages threat intelligence to simplify detection and response to improve threat assessment and response efficiencies. It offers real-time intelligence gathered from Trellix

Advanced Research Center to proactively identify potential threats, help organizations prioritize their security posture, as well as provides actionable recommendations for changes to an organization's security posture.

Trellix Device Control – offers comprehensive device management that helps control and block confidential data copied to removable storage devices. Parameters, such as product ID, vendor ID, serial number, device class, and device name, can be specified and categorized. Different policies such as, block or encrypt, can be enforced based on the content loaded onto devices.

Trellix Application Control – prevents zero-day attacks by blocking execution of unauthorized applications leveraging threat intelligence and custom rules. It uses inventory search and pre-defined reports to quickly find and fix vulnerabilities, compliance, and security issues in the customer environment. Trellix Application Control lets administrators combine rules based on file name, process name, parent process name, command line parameters, and username for enhanced protection.

Trellix Threat Intelligence Exchange – secures systems in real time by operationalizing threat intelligence data and delivering protection to all points in the enterprise as new threats emerge. It leverages Data Exchange Layer (DXL) to instantly share threat data to all connected security systems, including third-party solutions.

Trellix Protection for Native Security – extends the base security built into Windows 10 with enhanced detection for fileless and zero-day threats. It utilizes a lightweight agent and combined policy management, to deliver advanced behavioral analytics for collective defense through a single console.

Trellix ePolicy Orchestrator (ePO) – supports the management of Trellix Endpoint Solutions. It is available with a choice of on-premises, virtual, or SaaS-based delivery and provides a single management system with centralized visibility across multiple security products and the entire threat defense lifecycle. Insight into security events allows administrators to understand and target updates, changes, and installations to systems.

Additional capabilities in the Trellix Portfolio to protect endpoints include:

- **Trellix Mobile Security** – offers on-device threat detection and protection for iOS and Android mobile devices. It protects against application and network threats, using machine learning algorithms to help identify malicious behavior.

- **Data Loss Protection DLP Endpoint** – safeguards sensitive data and helps comply regulatory compliance with automated reporting. It empowers users to manually classify documents, increase employee data protection awareness, and reduce administrative burden. It integrates with Threat Intelligence Exchange and Data Exchange Layer (DXL) to help block sensitive data in applications identified as malicious.

- **Trellix XDR** – the Trellix Endpoint Security platform is natively integrated into Trellix XDR to provide optimized SOC efficiencies. It instantly analyzes data from across the customer environment to predict and prevent emerging threats, identify root causes, and respond in real time. It also helps enhance existing security solutions by seamlessly integrating third-party tools with Trellix's full portfolio of infrastructure, SecOps, and data protection tools.

STRENGTHS

- Trellix offers on-premises, cloud and SaaS management options while retaining a centralized management experience.

- Trellix ePolicy Orchestrator is a powerful, single management console that allows administrators to create and manage policies across most Trellix security solutions.

- Trellix's endpoint security portfolio delivers a broad range of defenses, including advanced defense capabilities needed for zero-day threats, while also integrating and working with third party solutions and native OS security controls.

- Trellix provides advanced threat defenses, like pre-execution and post-execution machine learning analysis and advanced analytics for file-less based attacks.

- Trellix's Endpoint Security provides a framework which enables IT to easily view, respond to, and manage the threat defense lifecycle.

WEAKNESSES

- While Trellix offers strong content aware DLP capabilities, these are available as a separately priced add-on or can be purchased through the more expensive Trellix Complete solution bundle.

- Trellix solutions do not provide native third-party software patch assessment and remediation, however Trellix can provide this in partnership with Tenable.

- Trellix does not provide Network Access Controls (NAC), which serves to bar or quarantine new endpoints from joining the network that have yet to deploy the organization's security policies.

- Trellix ENS provides web browsing controls through labeling of suspicious websites. It does not, however, support blocking of suspicious URLs or website browser isolation.

- While highly capable, Trellix endpoint solutions are a best fit for medium to large customers with adequate budgets.

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 extends 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.

TRAIL BLAZERS

CYBEREASON INC

200 Clarendon Street
Boston, MA 021161
www.cybereason.com

Cybereason, founded in 2012, offers solutions that protect organizations from cyberattacks through prevention, detection, threat hunting and response. Cybereason is a privately held international company headquartered in Boston with customers in over 40 countries.

SOLUTIONS

The **Cybereason Defense Platform** combines AI-powered detection and response (EDR and XDR), intelligence-based behavioral next-generation antivirus (NGAV) prevention, anti-ransomware prevention and proactive threat hunting to deliver context-rich analysis of every element of a malicious operation (i.e. MalOp). The MalOp interface replaces single threaded alerts with comprehensive correlations and root cause analysis across the network and all impacted devices, instantly delivering the insights required to end attacks. The Cybereason Defense Platform supports multiple deployment options, including cloud, on premises, hybrid, and air-gapped. The platform comprises the following capabilities:

- **Cybereason XDR** – offers vendor agnostic, unified detection and response capabilities that find and end MalOps (malicious operations) across the entire IT stack including endpoint, application suites, user personas, on-premise network and cloud deployments. Cybereason XDR helps consolidate tooling and centralize all detection and response efforts across the enterprise, and also unifies device and identity context in a correlated, visual investigation experience.

- **Cybereason Prevention** – leverages multiple layers of prevention including signature-based technologies, behavioral, and machine-learning approaches to stop threats from both known and unknown attacks; this includes ransomware, fileless and .Net attacks, as well as zero day malware. Cybereason also provides Endpoint Controls which allows organizations to manage specific controls tied to different types of devices, implement personal firewall policies, and enforce disk encryption. Cybereason Prevention is deployed quickly within a single, lightweight agent for all operating systems and endpoint types. Once installed, security analysts can leverage a single console to easily investigate through a full context, single visual timeline, which helps quickly identify and remediate threats.

- **Cybereason EDR** – correlates an entire attack across all endpoints in a customer's environment to give security teams a single view of an attack story in real time, which allows them to quickly examine and respond to attacks at scale. Teams can understand the scope of an attack in seconds, and can stop threats and remediate issues across all affected machines with a single click. Security analysts can quickly identify any malicious activity in their environment and easily hunt for attacker activity with syntax-free and visual based searches. Cybereason EDR can identify threats quickly using behavioral analysis that leverages cross-machine correlations and enriched data from across all endpoints in real-time, and helps significantly reduce the workload for security teams.

- **Cybereason Digital Forensics and Incident Response (DFIR)** – allows analysts to easily investigate and uncover malicious files across operating systems (e.g. Windows, macOS, and Linux), with built in interactive File Search and native Yara rule support. Security analysts are also able to investigate through access to auto-generated end-to-end root cause analysis, real-time telemetry data, and forensics artifacts.

Cybereason also offers a suite of services to augment customers' security teams, which include:

- *Cybereason MDR* – offers 24/7 monitoring, incident triage, recommendations, ongoing, proactive hunting to identify malicious activity.

- *Incident Response* – involves immediate and on demand incident response, including scoping, investigation, consultation, and containment of incidents.

- *Assessment Services* – offers customized review of customer environments to help identify and address misconfigurations, identify needed critical patches, and assist with security policy enforcement.

STRENGTHS

- Cybereason supports deployments to cloud, hybrid, and on-premises environments. It offers an on-premises offering, known as Private Infrastructure Protection (PIP), which has a dedicated support team and full feature parity with its SaaS deployment.

- The Cybereason platform collects endpoint telemetry and correlates both known malware and behavioral detections of unknown malware across multiple devices to show the full attack timeline, via a single screen and workflow.

- Cybereason provides multi-layered prevention capabilities that include signatureless or file-less prevention, signature based anti-malware, exploit protection, behavioral document protection, anti-ransomware, as well as endpoint controls such as personal firewall, disk encryption, and USB blocking.

- Cybereason's interactive investigation console can be easily leveraged by analysts of all skill levels to investigate every detail on an endpoint including behaviors, processes, and observed activity across all devices in the enterprise.

- The Cybereason Defense Platform is attractively priced, while delivering a highly advanced, comprehensive set of features and functionality.

WEAKNESSES

- Cybereason does not offer Antivirus removal tools, however its deployment services team does provide complimentary and customized services to assist with implementation.

- While the Cybereason Defense Platform performs URL filtering through customizable reputation lists and correlation with threat intelligence, it does not block access.

- Cybereason does not provide native DLP functionality, however, it can refer customers to partner solutions.

- Cybereason does not offer its own Sandboxing technology, however, it integrates with the VMRay solution.

- Cybereason Defense Platform offers protection for devices on multiple OS (e.g. Windows, Mac, Linux, IOS, and Android). Additional capabilities, however, are needed to better protect cloud-based applications via containers. The vendor has this on its roadmap.

- Cybereason is currently best known in Europe and Asia/Pacific. The vendor is working to raise awareness of its solutions in North America.

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

- **Sophos Intercept X Advanced with XDR** – also includes integrated endpoint detection and response capabilities using the same agent. XDR functionality is available for Windows, macOS and Linux devices. **Intercept X 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 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).

Intercept X includes the following key capabilities:

  - *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.

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

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

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

- *XDR* – synchronizes native endpoint, server, firewall, email, cloud and Microsoft 365 security offering a holistic view of an organization's environment to support threat detection, and investigation and response actions.

- *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.

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

- *Device control* – can be used to block the use of storage devices, optical drives, wireless devices (e.g., Bluetooth), and mobile devices. Granular use policies can be created for different groups or individuals.

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

- *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.

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

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 Intercept X Advanced employs a single endpoint agent for combined traditional and next-generation protection, which delivers AV, deep learning, anti-exploit, anti-ransomware, EDR, HIPS, Application Control, DLP, Device control, firewall, web protection and web filtering.

- Sophos offers strong XDR capabilities, in an easy to consume format that is easily accessible for security teams across a wide expertise range.

- Sophos' CryptoGuard technology supports file roll-back capabilities in the event of a ransomware incident.

- Sophos synchronized security integrates Endpoint and Network security for full perimeter threat visibility through automation of threat discovery, investigation, and response.

- Sophos solutions are easy to deploy and manage, and don't require extensive training to take advantage of all features and functionality.

- Sophos offers simple per-user license pricing, which covers all devices a user may wish to protect.

WEAKNESSES

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

- Sophos Intercept X endpoint solutions do not have direct access to Sophos' 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).
- Customers we spoke with as part of this research, indicated that reporting features, while adequate, could be improved to offer greater customization.

- Sophos endpoint solutions are aimed at small to mid-size organizations which don't require a great deal of customization or integration with existing infrastructure.

SPECIALISTS

WATCHGUARD TECHNOLOGIES

505 Fifth Avenue South, Suite 500
Seattle, WA 98104,
www.watchguard.com

WatchGuard Technologies, offers network security and intelligence, secure Wi-Fi, multi-factor authentication and advanced endpoint protection. In 2020 it acquired Panda Security, a provider of advanced endpoint security solutions. WatchGuard is privately owned.

SOLUTIONS

WatchGuard offers the cloud-native **Unified Security Platform (USP)**, a scalable platform for security delivery. Within the USP, **WatchGuard Cloud** is the centralized management interface, and the authority for security policy management, dissemination, and enforcement for security

solutions for network, Wi-Fi, MFA and the WatchGuard endpoint security products. WatchGuard Endpoint Security includes:

- **WatchGuard EPP** – offers all the capabilities of Endpoint Protection, plus it adds web access control (URL filtering by category) and antispam and anti-malware protection for Microsoft Exchange. It is available for Windows, macOS, Linux, and Android, however, web access control functionality is available for Windows only.

- **WatchGuard EDR** – is the endpoint detection and response (EDR) solution, complemented by WatchGuard's managed service offering. It provides protection against unknown malware and targeted attacks through visibility at the endpoint of users, files, processes, registry, memory and network behavior. This visibility serves to block attacks using behavioral analysis and containment strategies, as well as to carry out detailed forensic analysis to determine the root cause of breaches, as well as implement mechanisms to avoid future incidents.

- **WatchGuard EPDR** – combines EPP capabilities with EDR capabilities, and managed services. It offers protection for desktops, laptops, and servers, delivered from the cloud. It automates the prevention, detection, containment and response against advanced attacks, zero-day malware, ransomware, phishing, memory exploits, and malwareless attacks, inside and outside the corporate network. It includes the *Zero-Trust Application Service* and the *Threat Hunting and Investigation Service (THIS)* at no extra charge.

- **WatchGuard DNSWatchGo** – offers DNS-level protection for computers on an off the network (no VPN required), providing an additional layer of security to block connections from phishing attacks and C2 connections, and content filtering that limits access to risky areas of the web with 130 pre-defined blocking categories.

- **WatchGuard Advanced EDR and Advanced EPDR** – provide all the feature provided in WatchGuard EDR and EPDR, with additional capabilities to proactively search for compromised endpoints with Indicators of Compromise (IoCs), including YARA rules and supervise, or harden endpoints from the execution of scripts and common attack techniques utilized by sophisticated threats.

- **WatchGuard ThreatSync** – is a cloud service that provides XDR technology for WatchGuard Network and Endpoint Security products. It provides extended detection

capabilities by correlating data from different WatchGuard security products that indicate the presence of threat actors in the organization. By using cross-domain and correlating activities monitored across different security products, ThreatSync scores and detects malicious scenarios that could be indicators of compromise (IoCs), enabling swift containment.

WatchGuard EDR, WatchGuard EPDR, WatchGuard Advanced EDR and WatchGuard Advanced EPDR leverage the following services:

- *Zero-Trust Application Service* – is WatchGuard's Security's executable classification service, which monitors and prevents the execution of malicious applications and processes on endpoints.

- *Threat Hunting and Investigation Service (THIS)* – is a managed service which provides real-time and retrospective intelligence on all the events taking place on an organization's systems to discover unknown threats by investigating anomalous users, machines and application behavior. The data helps investigators conduct forensic analysis that make remediation processes more efficient and help reduce the attack surface. In addition, any new indicators of compromise feed the solution's technologies and automate detection in the early attack phases without human intervention.

The services leverage EDR capabilities and Endpoint telemetry that is collected and turned into actionable insights, in real time through applications specifically designed for internal SOCs, MSSPs and MDR (Managed Detection and Response) service providers.

WatchGuard also offers the following complementary add-ons:

- **Advanced Reporting Tool (ART)** – is an optional module that can be used to augment Adaptive Defense and Adaptive Defense 360, to provide detailed information on applications and vulnerabilities.

- **WatchGuard Patch Management** – is an add-on which manages vulnerabilities in operating systems and third-party applications on Windows endpoints and servers.

- **WatchGuard Data Control** – is an add-on to WatchGuard (formerly Panda) Adaptive Defense and WatchGuard (formerly Adaptive Defense 360), which discovers, audits and monitors unstructured sensitive or personal data on endpoints.

- **WatchGuard Full Encryption** – is an add-on to WatchGuard Endpoint Protection, WatchGuard Endpoint Protection Plus, WatchGuard (formerly Panda) Adaptive Defense and WatchGuard (formerly Panda) Adaptive Defense 360, which centrally controls and manages full disk encryption and key recovery, leveraging BitLocker in Windows systems.

- **SIEMFeeder** – is a module that sends in real time, events collected on endpoints and enriched with security intelligence, to integrate into SIEM solutions.

- **Aether** – is WatchGuard's cloud-based administration console. It provides a wide range of APIs and tools to help integrate into organizations' existing applications and processes.

In addition, WatchGuard's Orion platform (formerly Cytomic), focuses on the needs of organizations with mature security operations centers, and on MSSPs expanding into Managed Detection and Response services. **Orion** is a cloud-based threat hunting platform that queries and analyzes real-time events and 12 months of enriched events for hunting, conducts IOC searches, launches OSQuery queries, initiates remediation actions directly on the endpoints, and conducts automated template-based investigations through the integration of the Jupyter Notebooks platform.

STRENGTHS

- WatchGuard EPDR and Orion combine in a single solution the capabilities of endpoint protection, Endpoint Detection & Response (EDR) and managed services. The solution is delivered in a light agent connected through cloud-based technologies to offer prevention, detection and response capabilities.

- WatchGuard delivers an easy to use, intuitive administration console with rich, actionable reporting.

- WatchGuard offers a Data Control module, which provides an unattended solution to control, monitor and search sensitive data and Personal Information at the endpoints. It doesn't require any additional agent, and its capabilities are integrated into the WatchGuard EPDR agent.

- WatchGuard solutions are attractively priced.

- WatchGuard is delivering on the integration of user, endpoint and network security into a single platform, expanding the company's endpoint footprint in North America.

WEAKNESSES

- WatchGuard currently only supports centralized management of full volume encryption for BitLocker for Windows devices.

- WatchGuard currently only provides basic MDM capabilities. Customers should check carefully on available features and functionality.

- WatchGuard currently provides only basic DLP capabilities, through its Data Control module. The vendor is working to enhance this with future releases.

- While WatchGuard's Endpoint EPP is available for Windows, macOS, Linux, and Android, the web access control functionality is only available for Windows and Mac.

WITHSECURE

Tammasaarenkatu 7
P.O. Box 24
00181 Helsinki
Finland
www.withsecure.com

WithSecure, formerly F-Secure Business, founded in 1988, offers cyber security products and services for enterprise customers. The company offers cloud-based solutions for endpoint protection, detection and response, Microsoft 365 and Salesforce protection, advanced threat protection and vulnerability management, as well as managed detection and response and security consulting services. WithSecure has a global presence, with headquarters in Finland, and is publicly traded.

SOLUTIONS

WithSecure's cloud-native endpoint protection is available with EDR and vulnerability management with a single agent and cloud-based management, or as a managed service:

- **WithSecure Elements Endpoint Protection** (cloud service) **–** includes the following key endpoint protection features:

  - *Workstation* **–** security for Windows and macOS workstations, including advanced behavior and heuristic analysis, ransomware protection, as well as application control, device control and fully integrated patch management.

  - *Server* **–** server security for Windows, Linux and Citrix. Additional Teams, OneDrive, SharePoint and Exchange components, with application control, device control and fully integrated patch management.

  - *Mobile* **–** mobile security for iOS and Android devices. Personal VPN (Wi-Fi Security), proactive App and Web protection and support for third party Mobile Device Management (MDM).

- **WithSecure Elements Endpoint Detection and Response** (cloud service) **–** includes the following key EDR features:

  - *Advanced threat protection* **–** with real-time behavioral, reputation, similarity and big data analysis with machine learning that identifies threats and alerts with a broad context.

  - *Endpoint agents* **–** allow the execution of a variety of remote response actions, like host isolation, on Windows and macOS. Multiple EDR response actions for one or more hosts (e.g., process kill and delete file) can be chained.

  - *Automated response* **–** actions are available to contain attacks whenever high-risk level detections are identified. In addition, a comprehensive list of response actions can be triggered for more detailed investigation and counter measures.

  - *On-demand access* **–** is available to WithSecure's managed detection and response team for incident analysis and investigations, with a 2-hour response time.

WithSecure Business Suite is an on-premises alternative for endpoint protection. **WithSecure Countercept** is WithSecure's GDPR compliant MDR, managed advanced threat hunting and response service, which offers 24/7 protection against skilled cyber adversaries. A Europe only Countercept variant, where all aspects of the service are delivered from within Europe, is also available.

WithSecure Elements Endpoint Detection and Response is an XDR solution when it is combined with **WithSecure Elements Collaboration Protection, Microsoft 365 Edition**, a solution to protect cloud-based Office 365 email and collaboration (SharePoint, OneDrive, Teams) from advanced threats like phishing, as well as detecting compromised Azure AD accounts. WithSecure Elements Security Center is a cloud native management platform, which also manages **WithSecure Elements Vulnerability Management**, a solution which delivers extensive network- and host-based vulnerability scanning, prioritization and management.

STRENGTHS

- WithSecure Elements is a cloud-native XDR platform with fully integrated patch and vulnerability management, using a single endpoint agent for all its functionality.

- WithSecure offers strong EDR detection coverage and on-demand expert services for incident analysis and investigations delivered by WithSecure's MDR team.

- WithSecure uses a multi-layered architecture for malware detection and endpoint protection. Including DeepGuard, its advanced behavioral analytics engine.

- Real-time threat intelligence from WithSecure Security Cloud ensures up-to-date protection. Updates are transparent and delivered constantly, without disrupting employee productivity.

- The footprint of WithSecure with regards to CPU and RAM usage is much smaller than that of other vendors in the space.

- Setting administrative policies is an easy, simple process. MSPs can leverage multi-company management to standardize policies across all customers they manage.

- WithSecure Elements Endpoint Protection for Servers brings advanced user-session monitoring for file shares, including restoration of files when malware is detected coming from a remote unprotected client.

WEAKNESSES

- WithSecure does not offer DLP capabilities.

- WithSecure's Business Suite on-premises offering is not as extensive as its cloud-based offering since EDR and iOS/Android protection are not offered on-premises.

- WithSecure does not yet offer protection for cloud workloads, e.g., for containers.

- WithSecure only supports native Windows and macOS full disk encryption.

- WithSecure XDR capabilities are currently focused on integrating with Microsoft 365 (i.e., Mail, SharePoint, OneDrive, Teams), rather than all/any other web, email, and network assets. The vendor is working to address this as part of its roadmap.

- WithSecure has improved its market visibility, especially with its consulting and managed services, but still needs to make progress in this area in North America.

SENTINELONE

605 Fairchild Dr.
Mountain View, CA 94043
www.sentinelone.com

SentinelOne, founded in 2013, delivers artificial intelligence powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single platform. In 2022, SentinelOne acquired Attivo Networks, a developer of identity detection and response technology. SentinelOne is publicly traded.

SOLUTIONS

SentinelOne **Singularity XDR** provides a unified platform for extended threat detection, investigation, response, and hunting across endpoints, cloud workloads, IoT security, and IT operations capabilities. It offers autonomous 'Sentinel' agents for Windows, Mac, Linux, and Kubernetes and supports a variety of form factors including physical, virtual, VDI, customer data centers, hybrid data centers, and cloud service providers. Sentinels are managed via a globally available multi-tenant SaaS designed for ease-of-use and flexible management. SentinelOne is available in the following tiered product offerings:

- **Singularity Core** – is an entry level endpoint security product, which offers basic XDR functions coupled with traditional endpoint protection capabilities. Key capabilities include: a visual representation of attack behavior, static artificial intelligence and file-based attack prevention, threat intelligence, behavioral artificial intelligence file-less attack detection, autonomous threat response, autonomous remediation response, autonomous rollback response, the ability to quarantine devices from the network, incident analysis, agent anti-tamper protection, and application inventory.

- **Singularity Control** – adds to the capabilities of Core a "security suite" of features for endpoint management which include OS Firewall control with location awareness, USB device control, Bluetooth controls, rogue visibility to uncover devices on the network that need Sentinel agent protection, and secure remote shell capabilities.

- **Singularity Complete** – is intended for enterprises that need modern endpoint protection and control plus advanced XDR features. It also offers patented technology that automatically contextualizes all OS process relationships, even across reboots, and stores them for future investigations. It is designed to lighten the load on security administrators, SOC analysts, threat hunters, and incident responders by automatically correlating telemetry and mapping it into the MITRE ATT&CK® framework.

In addition, SentinelOne also offers the following functionality:

- **Singularity Cloud** – offers workload security and visibility to assets running in public clouds, private clouds, and on-premises data centers, so that security teams can manage both Linux and Windows servers, and Docker or Kubernetes containers from one platform.

- **Singularity Identity** – defends Active Directory, Azure AD Domain Controllers, and Domain-joined assets from attack.

- **Singularity Ranger AD** – delivers actionable insights to reduce the on-premises and cloud-based Active Directory attack surface.

- **Singularity Ranger** – delivers enterprise level network visibility and controls. It provides instant asset inventory and information about rogue devices to help investigate how managed and unmanaged devices interact with critical assets.

- **Singularity Mobile** – offers AI-powered protection for mobile devices to protect against zero-day mobile malware and phishing attacks.

- **Singularity RemoteOps** – empowers SOC analysts to remotely investigate threats across multiple endpoints and remotely manage their entire fleet. It allows incident responders to run scripts to easily collect forensic artifacts, modify incident response tools, in order to improve investigation and response workflows.

- **Singularity Cloud Funnel** – enables security teams to stream XDR data to Amazon S3 for data storage, integration with SIEM/SOAR tools, correlation with outside data sources, and other security workflows.

- **Singularity BinaryVault** – automates malicious and benign file upload, forensic analysis, ad security tool integration.

- **VIGILANCE Respond/Respond PRO** – are subscription services designed to supplement its endpoint security SaaS offerings. It offers 24x7 managed detection and response through the expertise of an in-house, Team of cybersecurity experts monitoring millions of endpoints.

- **Singularity Marketplace** – offers integration with a number of leading partner solutions, including Splunk, ServiceNow, AWS, Zscaler, Netskope, Okta, and many others.

STRENGTHS

- Unlike many other next-generation endpoint protection platforms, SentinelOne can be deployed both in the cloud and on-premises.

- SentinelOne offers a fully converged Endpoint Protection Platform (EPP) and Extended Detection & Response (XDR) platform in a single lightweight agent. It can run on its own or complement existing AV solutions from other vendors.

- SentinelOne's autonomous endpoint agent provides prevention, detection, and response without any reliance on cloud systems or look up. This allows for faster detection and response to advanced attacks at machine speed.

- SentinelOne's autonomous agent includes remediation technology. This allows the agent to automatically return a system to its pre-threat state without any end user impact or system downtime.

- SentinelOne provides advanced threat hunting, where the indexing of the data done by the autonomous agent allows security analysts to receive full context of any behavior, or indicators of compromise (IOC) off a single pivot. This includes encrypted TLS sessions.

WEAKNESSES

- While SentinelOne has solid integrations and performance, it needs to work to improve in-product workflows, as well as the quality of integration with partner technology solutions.

- While SentinelOne provides patch assessment, it does not currently provide patch remediation (i.e., deployment of missing of missing updates discovered during the patch assessment phase).

- SentinelOne does not offer application whitelisting.

- SentinelOne does not currently offer full-disk encryption (FDE) functionality.

- SentinelOne does not offer URL filtering or browser isolation.

- SentinelOne does not currently offer content aware DLP capabilities, or CASB functionality. However, through Singularity Marketplace, SentinelOne integrates with a number of partners that offer these capabilities.

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's endpoint security solutions are branded under the **Microsoft 365 Defender** umbrella name, as follows:

- **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 also offers **Microsoft Defender for Business** which offers endpoint protection aimed at small businesses with up to 300 employees.

Microsoft Defender for Endpoint can be managed from the **Microsoft 365 Defender Portal**, which provides a unified control point across the entire enterprise environment encompassing Microsoft Defender for Office 365, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Defender for Cloud Apps. **Microsoft Sentinel** brings together integrated SIEM visibility across the entire Microsoft 365 Defender suite of solutions, and Microsoft Defender Cloud Apps.

Microsoft has also folded numerous endpoint protection features directly into the operating system, starting with Windows 10, Windows Server 2016, and the more recent Windows 11. Key features comprise:

- **Windows Defender Antivirus (WDA)** – is loaded into the system directly at configuration time, to provide basic endpoint anti-malware protection.

- **Microsoft Defender Security Center** – is a local security dashboard.

- **Microsoft Defender SmartScreen** – provides phishing and malware filtering for Microsoft Edge browsers and Internet Explorer.

- **Microsoft Defender Application Guard** – helps isolate and sandbox Internet Explorer and Edge browsers.

- **Microsoft Defender Application Control** – is an application whitelisting solution that can also limit the capabilities of unsigned scripts, as well as enforce established use policies. It overlaps somewhat in functionality with Microsoft App Locker, another application whitelisting technology, which was originally available with Windows 7 but has also been upgraded for use in Windows 10.

- **Secure Boot** – helps ensure that devices boot using only trusted software.

- **Windows Defender Device Guard** – allows Windows desktops to be locked down to run only trusted apps (similarly to mobile phones).

- **Windows Defender Exploit Guard** – provides exploit mitigation, blocks risky activity, can be used to restrict HTTP and HTTPS connections to malicious hosts, and can be used to restrict access to designated folders.

- **Windows Defender Credential Guard** – prevents unauthorized access to OS credential information.

- **Windows Defender System Guard** – protects key OS components starting at boot-time.

On earlier Windows 8 and 9 platforms, protection consists of **Microsoft System Center Endpoint Protection (SCEP)**, and **Microsoft Intune**. Microsoft has also extended Windows Defender ATP to support older Windows 7 and Windows 8.1 platforms.

- **Microsoft System Center Endpoint Protection (SCEP)** – is Microsoft's solution for anti-malware and endpoint protection for traditional endpoint devices (laptops, desktops and servers). It provides real-time, policy-based protection from malware, spyware and other threats. It also provides file cleaning, where infected files are replaced with clean versions downloaded from a Microsoft cloud location, as well as the ability to configure Windows Firewall settings. SCEP is designed for Windows client workstations and servers and is included at no additional cost as part of the Microsoft Enterprise Client Access License and Core CAL programs. Separate security applications, however, are required for Mac and Linux platforms.

- **Microsoft Intune –** is Microsoft's cloud-based Unified Endpoint Management (UEM) solution for mobile device management of Windows, macOS, iOS, and Android.

SCEP and Intune can both be managed through **Microsoft Endpoint Configuration Manager (MECM),** formerly Microsoft System Center Configuration Manager (SCCM), which unifies policy management and device management.

STRENGTHS

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

- Microsoft offers customers a complete vision which goes well beyond simply endpoint malware protection to encompass Advanced Threat Protection (ATP), as well as information security, data loss prevention and identity management.

- Microsoft offers a strong set of security features for Windows 10 and 11 platforms, making it easier for users and administrators to adopt a strong security posture.

- Microsoft Defender for Endpoint (MDE) is a good first step for organizations looking for an entry-level XDR solution.

- SCEP and Intune are some of the least expensive endpoint security solutions on the market, as many customers can get these solutions at no additional cost with their existing licensing agreements.

WEAKNESSES

- Despite Microsoft's strong investments in security, customers still cite Microsoft's malware detection capabilities as being less accurate than competing security solutions. Most customers deploy Microsoft technologies as a baseline, while also deploying additional security solutions from other vendors for more advanced protection.

- 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.

- While Microsoft's P1 MDE plan is aimed at Microsoft 365 E3 customers, to benefit from the full power of Microsoft's security solutions, customers must upgrade to the higher-end Microsoft 365 E5 enterprise plans.

- Microsoft offers a highly complex ecosystem of security solutions involving the operating system and many additional components. However, integrating all components correctly and maintaining them fully integrated throughout Microsoft's continuous upgrade cycle can be daunting for many organizations.

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

- Encryption capabilities are only offered via the Microsoft Desktop Optimization Pack.

- Microsoft Endpoint Configuration Manager does not offer granular device control for removable media, CD/DVDs, and other common devices.

- While Microsoft offers endpoint protection for non-Windows platforms (including macOS, iOS, Linux and Android platforms), feature parity is not available across all platforms and customers should check carefully on the features and capabilities they require.

TREND MICRO

Shinjuku MAYNDS Tower, 1-1,
Yoyogi 2-Chome, Shibuya-ku
Tokyo, 151-0053, Japan
www.trendmicro.com

Founded in 1988, Trend Micro provides security solutions for organizations, service providers, and consumers. Trend Micro's cloud-based Smart Protection Network brings together threat reporting and analysis based on a worldwide threat assessment infrastructure. Trend Micro is publicly traded.

SOLUTIONS

As part of the **Trend Micro One** unified cybersecurity platform, **Trend Micro Workforce One** brings together endpoint, email, mobile and web security.

Apex One is the endpoint component of Workforce One which combines machine learning and other techniques, to protect against ransomware and advanced attacks. It combines traditional endpoint protection with endpoint detection and response (EDR) and managed detection and response (MDR) capabilities. Apex One supports a broad range of threat detection techniques including machine learning (both pre-execution and runtime), and IOA behavioral analysis. It also provides virtual patching powered by early threat intelligence from Trend Micro's Zero Day Initiative. It delivers actionable insight through a single console which includes an EDR investigative toolset option which enables threat hunting, patient zero identification, and root cause analysis. The EDR investigative capabilities are available for PC and Mac platforms. Apex One is delivered as single agent and is available in a SaaS or on-premises deployment model.

Apex One can integrate with additional components which include:

Vulnerability Protection – delivers virtual patching to prevent zero-day threats.

Application Control – prevents unknown applications from executing on endpoints. It combines policies, whitelisting and blacklisting capabilities, as well as an extensive application catalog.

Data Loss Prevention (DLP) – prevents data loss via USB, email, software as a service application, web, mobile devices, and cloud storage.

Endpoint Sensor/XDR Endpoint Sensor – provides context-aware investigation and response (EDR/XDR), recording and reporting to allow threat analysts to assess the nature of an attack across email, endpoints and servers.

Endpoint Encryption – encrypts data stored on endpoints including PCs, Macs, DVDs, and USB drives. It is available as a separate agent which provides full-disk encryption, folder and file encryption as well as removable media encryption. Endpoint encryption is only available as an on-premises component and as a separate agent from Apex One single agent.

Trend Micro Apex Central – is a centralized security management console which provides visibility and reporting across multiple components. It extends visibility across on-premises, cloud and hybrid deployment models. It also provides access to actionable threat intelligence from the Trend Micro Smart Protection Network which relies on global threat intelligence to deliver real time security.

Security for Mac – provides a layer of protection specific to Mac clients and adheres to a Mac OS look and feel.

Apex One integrates into **Trend Micro Vision One** for XDR (Extended detection and response) managed services which offer correlated detection and response across email, endpoints, servers, cloud workloads, and networks. Apex One customers have access to XDR free of charge for up to 10% of their users, which is intended as a steppingstone into Trend Micro's Managed XDR offering.

STRENGTHS

- Trend Micro's Smart Protection Suites offer a broad portfolio of solutions that bring together endpoint, server, web, email protection and more, into a cohesive security management framework to meet diverse customer needs.

- Apex One delivers the benefits of traditional endpoint protection, as well as EDR/XDR in a single a single client available for both on-premises and SaaS deployment.

- Trend Micro prices per user, which is a cost advantage as users typically have multiple devices.

WEAKNESSES

- Trend Micro has been slow to innovate its portfolio, particularly as it pertains to the addition of advanced threat detection technologies, such as XDR.

- Customers report that Trend Micro's XDR capabilities are still not as advanced as those of competing solutions.

- The Apex Central management console and Vision One XDR platform have different UIs and workflows, which makes it cumbersome for administrators to switch between the two.

- Trend Micro Endpoint Encryption is available on-premises only and as a separate agent from the Apex One single agent.

- DLP is only available as a separate add-on.

- Mobile Security is a separate add-on.

CROWDSTRIKE

150 Mathilda Place
Sunnyvale, CA 94068
www.crowdstrike.com

CrowdStrike, Inc., a wholly owned subsidiary of CrowdSrike Holdings, Inc., delivers cloud-based workload security, endpoint security, threat intelligence, incident response, and cyberattack response services. CrowdStrike is publicly traded.

SOLUTIONS

CrowdStrike **Falcon Endpoint Protection** is a cloud-based endpoint protection solution which combines next-generation antivirus, endpoint detection and response (XDR/EDR), managed threat hunting, IT hygiene, and threat intelligence through a single agent. It combines artificial intelligence and machine learning techniques to protect against known and unknown threats.

Falcon comprises the following components:

- *Falcon Prevent* – is CrowdStrike's next-generation antivirus (NGAV) solution which delivers protection based on machine learning and artificial intelligence, as well as behavior-based indicators of attack (IOA), exploit blocking, threat intelligence, automated IOA remediation, and more.

- *Falcon Insight XDR* – is CrowdStrike's endpoint detection and response (XDR/EDR) solution. It relies on the CrowdStrike Threat Graph, an advanced graph data model, which collects and inspects event information in real time. It provides an integrated, central repository for cross-domain telemetry. It brings data together across EDR, identity, cloud workload, mobile, vulnerability management, threat intelligence, and cloud security posture management (CSPM). Through the CrowdXDR Alliance for it also integrates with third-party partner solutions for email security, web security, CASB, network detection and response (NDR), firewall, and identity and access management (IAM).

- *Falcon Device Control* – provides visibility and control over USB device usage.

- *Falcon X* – is CrowdStrike's global threat feed providing customized reports and analysis to help predict and prevent zero-day attacks.

- *Falcon Firewall Management* – offers centralized firewall management, making it easier to manage and enforce host firewall policies.

- *Falcon OverWatch* – is CrowdStrike's 24/7 Managed Detection and Response (MDR) service which brings together threat hunting, alert prioritization, and incident response.

- *Falcon Discover* – offers IT hygiene and asset inventory, to help identify unauthorized systems and applications in real-time, as well as remediate issues to improve security posture.

- *Falcon for Mobile* – extends proactive threat identification and response, and incident investigation to Android and iOS mobile devices.

- *CrowdStrike Services* – offers pre and post incident response services through CrowdStrike's own team of experts.

Falcon Endpoint Protection is available in four bundles:

- **Falcon Go** – includes Falcon Prevent, Falcon Device Control and CrowdStrike Services.

- **Falcon Pro** – adds threat intelligence, and Falcon Firewall Management.

- **Falcon Elite** – adds Insight XDR, Falcon Discover, and Falcon Identity Protection. Falcon threat intelligence, device control, firewall management, Falcon OverWatch are optional add-ons.

- **Falcon Complete** – offers fully managed detection and response (MDR) as a service, powered by CrowdStrike expertise and backed by a breach warranty guarantee of up to $1 million.

The **CrowsStrike Store** provides access to a broad range of partner solutions, such as User Entity Behavior Analytics (UEBA), and more.

STRENGTHS

- CrowdStrike solutions are based on a lightweight agent and managed services cloud architecture, which delivers protection features across Windows, macOS, and Linux platforms.

- CrowdStrike offers an integrated set of advanced endpoint protection capabilities which combine next-generation AV, EDR/XDR, advanced threat protection (ATP), with Managed Detection and Response (MDR), making this functionality accessible to organizations which may not have the IT resources to run this type of capabilities on their own.

- CrowdStrike solutions are managed through a unified management console which provides sophisticated workflows for detection and response.

WEAKNESSES

- Customers we spoke with as part of this research, indicated a high rate of false positives. CrowdStrike does not participate in extensive third-party malware testing, making it difficult to assess its efficacy.

- CrowdStrike's business focuses mainly on OverWatch, its Managed Detection and Response (MDR) solution, as opposed to its product-based solutions.

- CrowdStrike does not offer content aware DLP functionality, or support ICAP for integration with third party DLP vendors.

- CrowdStrike has lost some mindshare, as almost all competing endpoint protection vendors now offer EDR/XDR, ATP and MDR capabilities.

- A full CrowdStrike deployment including all options, tends to be more expensive than many competing next generation endpoint solutions.

OPENTEXT

275 Frank Tompa Drive
Waterloo, ON
N2L 0A1
Canada
www.opentext.com

OpenText, founded in 1991, information management solutions, powered by OpenText Cloud Editions, a cloud-native containerized architecture. OpenText is well known for its content services and analytics products as well as eDiscovery and archiving solutions. OpenText is a publicly traded company. In January 2023, OpenText closed the acquisition of Micro Focus International plc ("Micro Focus"), a provider of software technology and services.

SOLUTIONS

OpenText Security solutions include **OpenText EnCase Endpoint Security**, **OpenText EnCase Endpoint Investigator,** and **OpenText MDR.** OpenText Security solutions address enterprise risk, information security and digital investigation needs and are backed by forensic-grade technology.

Webroot offers an integrated platform of three internet security solutions developed for Managed Service Providers (MSPs) and SMBs, these include: **Webroot Business Endpoint Protection**, **Webroot DNS Protection,** and **Webroot Security Awareness Training**. The solutions are powered by the **Webroot Threat Intelligence Platform**, a security threat intelligence platform that is continuously collecting, analyzing and correlating security data such as file behaviors and reputations, URL and IP reputation, phishing websites in real-time, mobile application reputations and more.

- **OpenText EnCase Endpoint Security** – is an EDR solution which provides security teams with a comprehensive view to validate, analyze, and respond to incidents quickly. It enables a deep level of endpoint visibility to detect anomalous user and system activity, threat intelligence and forensic-grade incident response. EnCase Endpoint Security offers automation and operational efficiencies to help incident responders find and triage security incidents faster and reduce the risk of loss or damage.

- **OpenText EnCase Endpoint Investigator** – provides Digital Forensic Incident Responders (DFIR) and forensic investigators seamless, remote access to laptops, desktops and servers. It offers evidence processing, integrated workflows and flexible reporting.

- **OpenText Managed Detection and Response (MDR)** – is a remote, cloud-based virtual Security Operations Center (V-SOC). It relies on artificial intelligence, custom TTPs, and advanced workflows to develop correlations between computer, network and device logs leading to actionable, high-fidelity alerts. BrightCloud Threat Intelligence Services is integrated directly providing context to help understand the nature, scope and impact of any security event.

- **Webroot Business Endpoint Protection** – is a real-time, cloud-based approach to preventing system compromises through advanced machine learning and threat intelligence. It is compatible with Microsoft Windows PCs and Servers, as well as Apple Mac devices; Terminal Servers and Citrix; VMware; Virtual Desktops and Servers, and Windows embedded Point of Sale (POS) systems. It offers the following capabilities:

    - *Real-Time Anti-Virus/Anti-Malware* – the Webroot client agent continuously monitors and shares encrypted meta-data with the Webroot Threat Intelligence Platform to predict, detect, prevent, contain and protect against malicious system compromises. Webroot uses a lightweight endpoint client agent that moves data intensive malware discovery processing to the cloud.

    - *Zero Definition Updates* – Webroot requires no system signatures or definition updates as the collective file and process security intelligence is held within the Webroot platform and instantly available to all protected customers' systems.

    - *Webroot Evasion Shield* – is a propriety, patented anti-malware technology that delivers new script and code detection capabilities, to stop APT and script-based attacks.

- *Web Reputation Protection & Filtering* – is provided through several different shield components within the Webroot endpoint security solution. The endpoint Web Threat Shield uses Webroot's BrightCloud Threat Intelligence Services (part of the Webroot Threat Intelligence Platform) to score and block sites with poor reputations and known infected (or malicious) domains.

- *Identity & Privacy Shield* – secures and isolates the browser (and any other application needed) from the rest of the endpoint.

- *Real-time anti-phishing protection* – uses machine learning in real-time when a user clicks on a link with a poor reputation score to determine if it is a phishing site, and blocks the connection request as needed.

- *Outbound Firewall* – checks all outbound TCP/UDP requests and destinations against the Webroot Threat Intelligence Platform.

- *Last 'known good' Auto-restore and Remediation* – through monitoring and journaling all unknown files and processes, any changes made to the endpoint can be reversed and restored to a last 'known good' state.

- *Offline Protection* – the endpoint agent enacts a separate policy to stop attacks when it is not connected or available to the Webroot Threat Intelligence Platform. Upon reconnecting to the Webroot Threat Intelligence Platform, if any new data is analyzed and found to be malicious, the endpoint system is auto remediated to its last 'known good' state.

- *Global Management Console* – An MSP-focused management console designed to meet the needs of multi-location and multi-site management. It integrates with the Webroot Unity API that allows MSPs to access on-demand real-time threat and other endpoint telemetry data for use within their own management, reporting, billing, and workflow applications.

- *Unity API* – supports integration into other IT management platforms, including Remote Monitoring and Management (RMM), Professional Services Automation (PSA), customized billing platforms, and internal IS systems. It also can be deployed by MSPs for custom automation of processes, reports and other services.

STRENGTHS

- OpenText EnCase Endpoint Security and OpenText EnCase Investigator have small footprints and run on a single EnCase agent.

- Webroot Business Endpoint Protection has a small installation footprint and system performance requirements are light, allowing the standard agent to be used in both older machines (where less processing power is available), as well as virtual environments, where system resources are also defined.

- Webroot can coexist in an environment with other endpoint security platforms, whereas most other solutions have difficulty operating on a machine with other security software.

- Webroot Business Endpoint Protection is easy to manage and offers built-in automatic rollback and auto-remediation of infected endpoints. Management is fully cloud-based and can work with any browser.

- Webroot offers Dwell Time reporting, which alerts and informs administrators of the precise time an endpoint was infected and how long it has taken for Webroot to fully remediate the infection. This can be coupled with forensics and data auditing.

WEAKNESSES

- OpenText EnSuite lacks full analytic capabilities, such as visualization, NoSQL-based correlation, business intelligence (BI), and others.

- Webroot Business Endpoint Protection and OpenText EnSuite do not include encryption or DLP capabilities.

- Webroot does not offer URL classification filtering as part of its endpoint platform.

- Webroot Business Endpoint Protection and OpenText EnSuite, do not extend protection to mobile devices, leaving this to best-of-breed MDM vendors.

- Webroot does not provide third party software patch assessment and management.

- Webroot does not offer EDR or XDR functionality at this time.

- Webroot does not provide sandboxing technology on the endpoint. EnCase Endpoint Security supports sandboxing through integration into third-party solutions.

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 consolidates multiple endpoint security capabilities into one agent and management console, making it easy to prevent, investigate, remediate, and hunt for threats. It offers the following modules which can be managed through the same user interface, with a single login:

- **Endpoint standard** – delivers next-generation antivirus and endpoint detection and response (EDR) functionality. It analyzes attacker behavior patterns to detect malware, fileless, or living-off-the-land zero-day attacks.

- **Managed detection** – is a real-time managed alert monitoring and triage solution. It relies on the CB Predictive Security Cloud to captures and store all OS events across every individual endpoint. It delivers visibility for security operations center (SOC) and incident response (IR) teams. Leveraging this data, allows teams to proactively hunt for threats, as well as uncover suspicious and stealthy behavior, disrupt active attacks, and address potential defense gaps. It enables organizations to respond and remediate in real-time, stopping active attacks and quickly repairing damage.

- **Audit and remediation** – delivers real-time device assessment and remediation. It serves to audit the current system state and track and harden the security posture across protected devices.

- **Enterprise EDR** – offers threat hunting and containment. It serves to proactively hunt for abnormal activity using threat intelligence and customizable detections.

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

STRENGTHS

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

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

- VMware Carbon Black 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 Cloud 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

