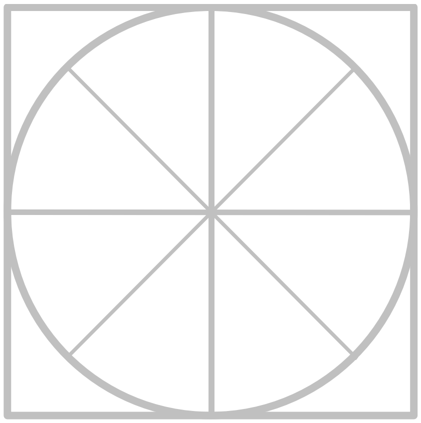
The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Endpoint Security - Market Quadrant 2024 *



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

March 2024

* Radicati Market Quadrant^{SM} is copyrighted March 2024 by The Radicati Group, Inc. This report has been licensed for distribution. Only licensee may post/distribute. Vendors and products depicted in Radicati Market Quadrants^{SM} should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants^{SM} are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED

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

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

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

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

    a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.
    b. Established vendors that offer very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.

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

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

b. In other cases, a vendor may simply have become complacent and be outdeveloped 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.

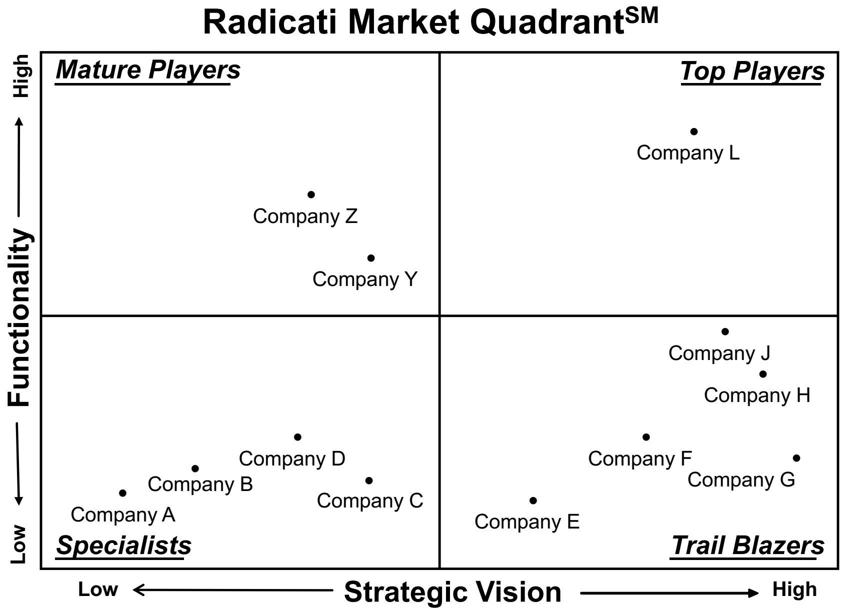


Figure 1: Sample Radicati Market Quadrant

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, SentinelOne, Sophos, Symantec, Trellix, Trend Micro, VMware Carbon Black* 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.

- 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.

- Nearly all vendors in this space 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.

- The endpoint security market is seeing strong growth as organizations of all sizes need to protect against all forms of threats and malicious attacks. The Endpoint Security market is expected to reach nearly $16.3 billion in 2024, and grow to over $36.5 billion by 2028. Figure 1, shows the projected revenue growth from 2024 to 2028.

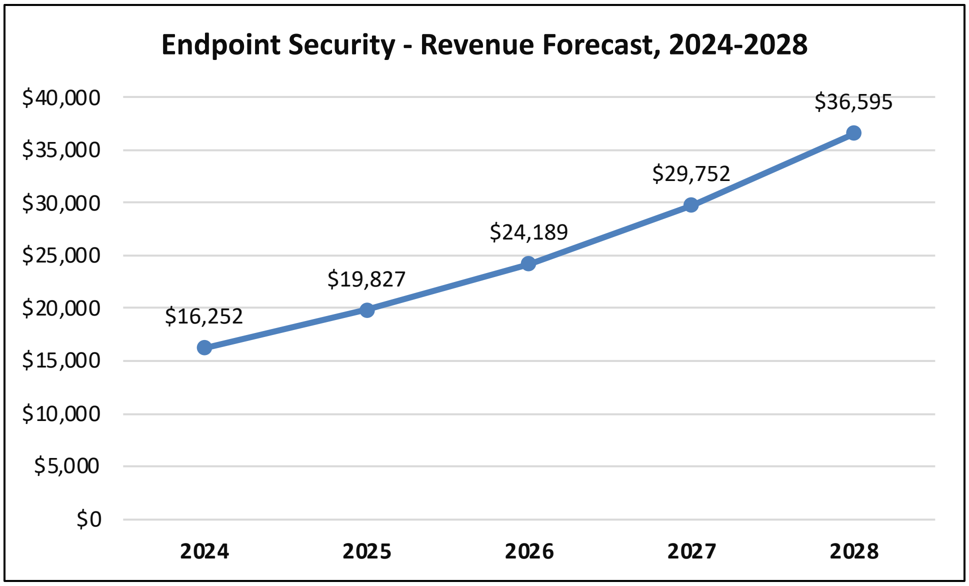


Figure 2: Endpoint Security Market Revenue Forecast, 2024-2028

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

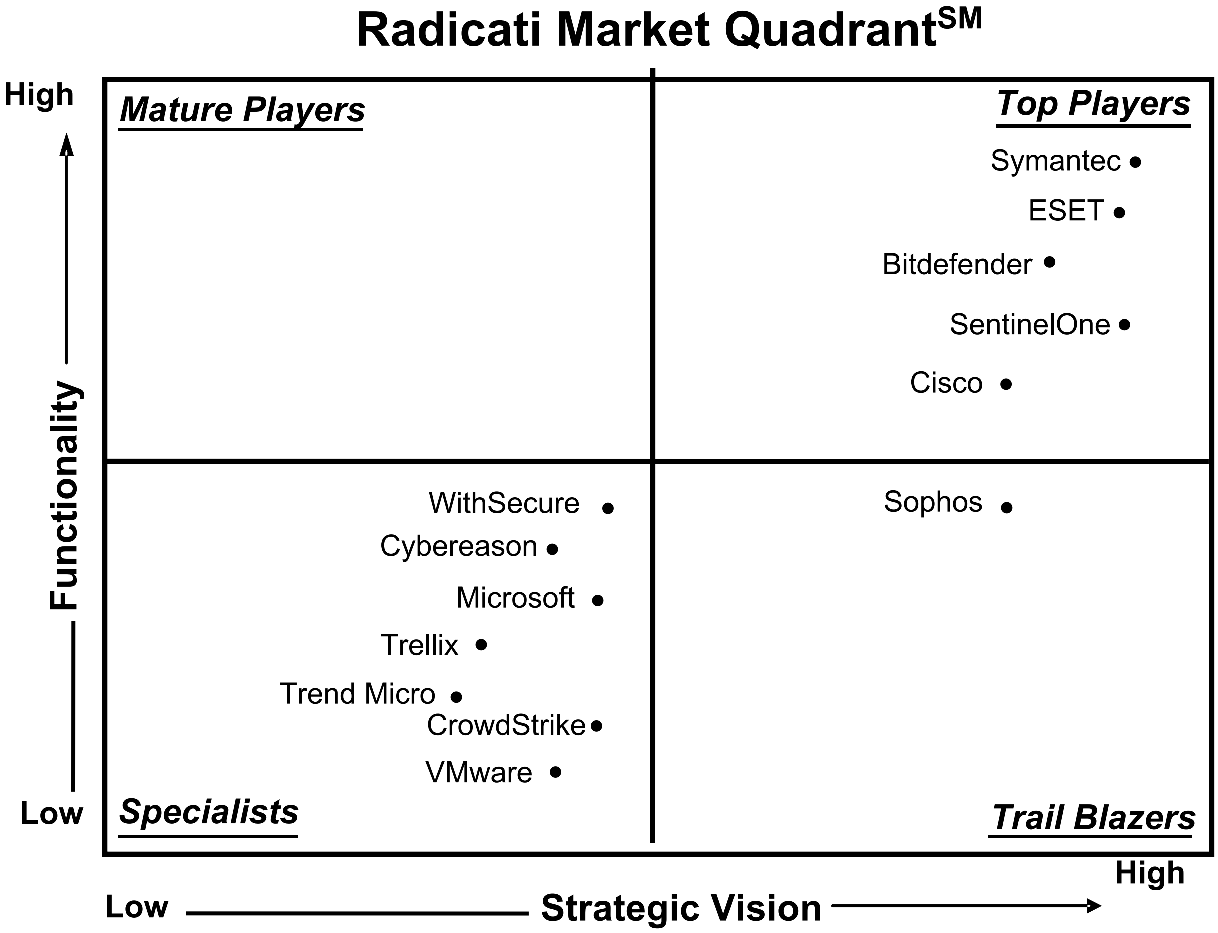


Figure 3: Endpoint Security Market Quadrant, 2024[*]

[*] Radicati Market Quadrant^{SM} is copyrighted March 2024 by The Radicati Group, Inc. This report has been licensed for distribution. Only licensee may post/distribute. Vendors and products depicted in Radicati Market Quadrants^{SM} should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants^{SM} are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT TRENDS

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

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

- The **Specialists** in this market are *WithSecure, Cybereason, Microsoft, Trellix, Trend Micro, CrowdStrike* and *VMware Carbon Black.*

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

ENDPOINT SECURITY - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC BY BROADCOM

3421 Hillview Ave
Palo Alto, California, 94304
www.broadcom.com

Symantec offers security solutions (network, endpoint, information, email and identity) for the enterprise market. Symantec operates one of the largest civilian cyber intelligence networks, providing visibility and protection 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 enabling real-time updates to prevent attacks, stop breaches, and mitigate risk. Symantec's endpoint protection solutions include:

- **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:

- *Hybrid Infrastructure* – supports deployments on premises, in the cloud and hybrid, enabling organizations to choose the security infrastructure that best meets their needs.

- *Adaptive Protection* – blocks, with no impact on business operations, the behaviors of trusted applications utilized in Living-off-the-land and other sophisticated threats.

- *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. SES Complete also provides enhanced event streaming via Kafka and the Open

Cybersecurity Framework (OCSF) to allow event transfer into SOC tools.

- *Adaptive Incidents* – combines Symantec's Adaptive Technology in SES Complete with 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. Additional granularity for threat intel is also provided by dedicated API's. Support for TAXII Service integration is also available to consume information associated with STIX and TAXII.

- *Threat Hunter* – assists SOCs by combining Symantec's expert analysts with advanced machine learning and global threat intelligence to provide alerts, insights and in-console and live 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.

- Symantec Endpoint Security supports on-premises, cloud and hybrid deployments, allowing organizations the flexibility to align their security approach to their IT infrastructure strategy.

- Symantec Endpoint Security uses a single agent, which redirects endpoint traffic to other Symantec controls (e.g. Cloud SWG, ZTNA, CASB, web isolation, and more) and replaces the need for a VPN. It also provides tight integration with other products in Symantec's security suite and enables ease of deployment and management for Endpoint, Cloud Secure Web Gateway and DLP.

- Symantec Endpoint Security consists of 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.

- The firewall functionality included can block unique IP addresses and employs reputation analysis from Symantec's Global Intelligence Network. It also can 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 an option, that is available for separate purchase.

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

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 built-in reports and allows organizations to create custom reports.

- **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, Microsoft Intune, or VMware Workspace ONE, 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 ESET's fully native encryption solution that can be activated with a single click across the entire network from the ESET PROTECT console. 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. Through the use of AI-powered modules, it can automatically correlate various metadata from sensors or auto-remediate known detections.

- **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 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. The service comes in two versions: ESET MDR, a lightweight cloud version suitable for SMBs; and ESET Detection Response Ultimate, which offers an Enterprise level SOC experience.

- **ESET NetProtect** – is ESET's DNS security solution for CSPs (Communication 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 and Google Workspace 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 supports third party vendor integrations, including CASB, through its newly released ESET Connect API Gateway platform.

- ESET currently holds a smaller market share in North America compared to other global regions where it operates. The company is working to address this through increased sales and marketing focus on this region.

BITDEFENDER

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

Bitdefender, founded in 2001, is a global cybersecurity company delivering threat prevention, protection, detection, and response solutions and services to business and government organizations. The company has customers in 170 countries and offices around the world. The company is privately held.

SOLUTIONS

Bitdefender GravityZone is an enterprise security platform that provides risk analytics, prevention, protection and extended detection and response. It is a unified platform that secures endpoints, mobile devices, cloud workloads, networks, productivity apps, users, and identities. Organizations which favor on-premises deployments can leverage the flexibility of GravityZone to deploy it as a virtual-appliance-based on-premises or in the cloud. Bitdefender security tools support an exceptional variety of platforms including Windows, Linux, macOS, 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) provides 24x7 protection and 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 three fully staffed security operations centers (SOCs).

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, Risk Assessment, Ransomware Mitigation, and Network Attack Defense are part of the core technology stack.

- **Bitdefender CSPM+** – combines Cloud Security Posture Management (CSPM) with Cloud Infrastructure Entitlement Management (CIEM) to provide comprehensive visibility of cloud inventories and configurations, identities and privileges, helping organizations identify configurations which are outside of a rich set of compliance regimes and meet internal standards. [launch scheduled for March 2024]

- **Bitdefender Offensive Services** – provides organizations with Penetration (Pen) Testing and Red Teaming services to ensure key security weaknesses and vulnerabilities are identified to improve the security of IT environments.

Bitdefender offers the following add-ons managed from the same GravityZone platform:

Gravityzone Security for Email – provides 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 macOS (FileVault and the diskutil command-line utility) to ensure optimal compatibility and performance.

GravityZone Security for Mobile – protects Android and iOS devices with anti-malware technologies, driven by real-time threat intelligence and machine learning technologies.

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

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

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

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

STRENGTHS

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

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

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

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

- Through the acquisition of Horangi, Bitdefender has added Cloud Security Infrastructure Management and Cloud Infrastructure Entitlement Management capabilities.

- Bitdefender consistently achieves strong scores in independent AV tests.

WEAKNESSES

- 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.

SENTINELONE

444 Castro St. Fl 4
Mountain View, CA 94041-2017
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. SentinelOne is publicly traded.

SOLUTIONS

SentinelOne Singularity Enterprise leverages AI to provide unified, protection for identities, endpoints, and the cloud. Coupled with deployment services and threat intelligence, Singularity Enterprise safeguards businesses, reduces risk, and maximizes the value of organization's security investments.

The following products and services are offered as part of Singularity Enterprise:

- **Singularity Platform** – is a Centralized XDR platform that augments and extends protection, detection, response, and remediation through integrations across attack surfaces.

- **Singularity Complete** – offers prevention, detection, response, and remediation capabilities.

- **30-Day Data Retention** – enhances incident response, threat hunting, and forensics analysis; ensures compliance, tackles evolving threats, reduces false positives, and aids in swift post-breach recovery.

- **Identity Threat Protection** – identity threat detection and response (ITDR) capabilities to prevent advanced identity-born attacks and protect high-value enterprise assets.

- **WatchTower** – threat-hunting service targets active global APT campaigns, novel attacker techniques, and emerging trends in cybercrime.

- **Singularity Ranger Insights** – network discovery and vulnerability management solution that identifies, prioritizes, and provides real-time insights into enterprise risks, facilitating maximum risk reduction.

- **Singularity RemoteOps Forensics** – integrated digital forensics and incident response (DFIR) solution that automates evidence collection, accelerates investigations, simplifies workloads, and reduces response times.

- **SentinelOneGo** – guided onboarding, deployment, and training advisory service with a structured methodology to ensure quick setup of the Singularity Enterprise solution.

In addition, SentinelOne also offers the following modular products and services:

- **Singularity Cloud Workload Security** – real-time cloud workload protection (CWPP) for cloud VMs, containers, and Kubernetes clusters across AWS, Azure, Google Cloud, and private cloud. AI-powered agent detects and stops runtime threats.

- **Singularity Cloud Data Security –** Threat detection for Amazon S3 and NetApp including malware scanning of new and historical files/objects; enablement of compliance against security rules to scan any foreign file before it enters the network; use of signature-based reputation and ML-powered Static AI engines to detect malware in the future; and automatic quarantine of malicious files.

- **Singularity Cloud Network Security –** (available May 2024) offers agentless cloud native application protection platform (CNAPP) with a unique Offensive Engine.

- **Singularity Hologram** – deception technology that uses decoy assets to trap in-network attackers. It provides onboarding of a deception grid from a centralized console and collects valuable forensic telemetry to provide insight into attacker methods. Singularity Hologram supports any operating system and can be deployed within an organization's network or projected into multi-cloud CSP environments.

- **Singularity Ranger AD** – provides continuous Active Directory risk assessments to reduce the identity attack surface .

- **Singularity Ranger** – Real-time network attack surface control solution that finds and fingerprints all IP-enabled devices on the network.

- **Singularity Threat Intelligence** – powered by threat intelligence from Mandiant, it provides a deeper understanding of organizations' threat landscape, monitoring emerging threats to proactively reduce risk and identify adversaries in their environment.

- **Singularity Mobile** – is an AI-powered MTD solution provides autonomous threat protection, detection, and response for iOS, Android, and ChromeOS devices.

- **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 and Google Cloud Storage buckets for data storage, integration with SIEM/SOAR tools, correlation with outside data sources, and other security workflows.

- **VIGILANCE Respond** – 24x7 Managed Detection and Response (MDR) services designed to supplement Singularity Enterprise. It enables security teams to offload threat investigation and response to a global team of SentinelOne cybersecurity experts.

- **Vigilance Respond Pro** – Includes all features of Vigilance Respond, plus digital forensics and incident response (DFIR) with access to experts for incident management, containment and consultation.

- **Singularity Marketplace** – an ecosystem of leading partner solutions, including Splunk, ServiceNow, AWS, Zscaler, Netskope, Okta, Mimecast, Mandiant, Proofpoint, Recorded Future, Snyk, Armis, IBM Security, and others. One-click applications help enterprises unify prevention, detection, and response across attack surfaces and implement XDR.

STRENGTHS

- Unlike many other next-generation endpoint protection platforms, SentinelOne offers on-premises/hybrid, cloud, and air-gapped network deployment.

- 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 provide patch remediation (i.e., deployment 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.

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 experienced 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-premise private cloud deployment model.

Secure Endpoint brings together EDR, XDR, USB device control, and Talos Threat Hunting. It is available in three plans: *Essentials, Advantage,* and *Premier*. It is also included as part of Cisco's *User Protection Suite* (which brings together *Secure Access, Duo, Email Threat Defense* and *Secure Endpoint*) and Cisco Breach Protection Suite (which brings together *XDR, Email Threat Defense* and *Secure Endpoint Advantage*).

Secure Endpoint delivers 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. 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.

- *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, Cisco XDR can provide threat context enrichment and helps 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.

- *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.

- *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.

Secure Endpoint integrates with **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.

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 XDR delivers unified threat response 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. It can, however, 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).

- Cisco's XDR functionality is still relatively new to market and may not yet be fully fine-tuned.

- Cisco XDR must be licensed separately and is only available in higher price plans.

- 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.

- Cisco's multiple security solutions tend to overlap in functionality and can be complex and confusing for customers to deploy correctly.

TRAIL BLAZERS

SOPHOS

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

Sophos offers IT security solutions for businesses, which include 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**, **MDR,** and **MDR Advanced**. 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. MDR includes Sophos **Managed Detection and Response (MDR)**, a 24/7 managed detection and response service. MDR Advanced 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, allow listing, 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 Essentials,* 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).

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 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

WITHSECURE

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

WithSecure, founded in 1988 and formerly known as F-Secure Business, offers cloud-based solutions for endpoint protection, detection and response, Microsoft 365 and Salesforce protection, advanced threat protection, cloud security posture management 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 through a single agent and cloud-based management, or as a managed service. It is available as follows:

- **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. Local 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 'Elevate to WithSecure' expert services*– is available to WithSecure's managed detection and response team for incident analysis and investigations.

WithSecure Countercept is WithSecure's GDPR compliant managed advanced threat hunting and response service (MDR), which offers 24/7 protection. A Europe only Countercept variant, where all aspects of the service are delivered from within Europe, is also available. WithSecure also offers a co-monitoring service, which is a lower cost alternative for 24/7 monitoring.

WithSecure Elements Endpoint Detection and Response can be combined with **WithSecure Elements Collaboration Protection, Microsoft 365 Edition**, to offer an XDR solution that can protect cloud-based Microsoft 365 email and collaboration (SharePoint, OneDrive, Teams) services from advanced threats, as well as detect compromised Entra ID accounts.

WithSecure Elements Security Center is a cloud native management platform. It also manages **WithSecure Elements Vulnerability Management**, a solution which delivers extensive network- and host-based vulnerability scanning, prioritization, and management. In addition, **WithSecure Elements Cloud Security Posture Management** supports remediation of misconfigurations on Amazon Web Services and Microsoft Azure platforms.

STRENGTHS

- WithSecure Elements is a cloud-native solution 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 ransomware and other malware detection and endpoint protection. Including DeepGuard, its advanced behavioral analytics engine.

- 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 ransomware or other malware is detected coming from a remote unprotected client.

WEAKNESSES

- WithSecure does not offer DLP capabilities.

- WithSecure does not offer forensic or intrusion detection capabilities for zero-day protection, which are common with competing solutions.

- 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 is best known in Europe and has a global presence, however it lacks visibility in North America.

CYBEREASON

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, MA.

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 correlations and root cause analysis across the network and all impacted devices, 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-premises network and cloud deployments. Cybereason XDR helps consolidate tooling and centralize all detection and response efforts across the enterprise, and 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 crossmachine 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. It is available in two plans: Essentials plus Extended Response (XR), and Complete.

- **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.

The Cybereason Defense Platform is available in three plans as follows:

o *Enterprise* – brings together Threat Intelligence, NGAV & AV, anti-ransomware protection, endpoint controls and EDR.

o *Enterprise Advanced* – adds MDR Essentials plus Extended Response (XR).

o *Enterprise Complete* – adds MDR Complete.

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

- Cybereason has undergone significant management changes in the past year, while also attracting major new investment capital. At the time of this writing, it is too early to assess how beneficial these changes will be to the company's long-term direction.

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 include:

- **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.

  - o *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.

  - o *Managed Detection and Response* – Microsoft Defender for Endpoint includes **Microsoft Threat Experts**, a managed detection and response (MDR) service which combines targeted attack notification with on-demand SOC expert services. It is available as part of the Microsoft 365 E5 subscription plan.
    Microsoft Defender for Endpoint is also available for macOS, Linux, Android and iOS platforms, however, feature parity is not always available across all platforms.

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

Microsoft Defender for Endpoint integrates with **Microsoft Defender XDR**, a unified pre- and post-breach defense suite that natively coordinates detection, prevention, investigation, and response across a wide range of services. It takes automatic action to prevent or stop attacks and self-heal affected mailboxes, endpoints, and user identities. Defender XDR incidents can be streamed to **Microsoft Sentinel (SIEM**). Microsoft also plans to embed **Microsoft Security Copilot**, a platform that brings together AI and human expertise, into Microsoft Defender XDR.

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), Microsoft Defender Security Center, Microsoft Defender SmartScreen, Microsoft Defender Application Guard, Microsoft Defender Application Control, Secure Boot, Windows Defender Device Guard, Windows Defender Exploit Guard, Windows Defender Credential Guard, Windows Defender System Guard.*

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). 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),** 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.

- In order 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.

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, and more. Trellix is privately held.

SOLUTIONS

Trellix Endpoint Security Suite offers a unified solution to protect endpoints and devices at the network edge. It can be deployed in a variety of modes, including cloud, on-premises or hybrid, and 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 feeds from local and global threat intelligence to provide 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.

- **Trellix Endpoint Security (HX)** – 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.

- **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 Application and Change 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 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.

- **Trellix MOVE AntiVirus** – offers security for virtualized environments (desktop and servers) across all major hypervisors and Windows VMs with agentless support for VMware, Windows, and Linux VMs.

Additional key capabilities in the Trellix Portfolio to protect endpoints include:
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 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 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.

Trellix ePolicy Orchestrator (ePO) – supports the management of Trellix Endpoint Solutions. It is available with a choice of on-premise, 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.

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.

STRENGTHS

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

- 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.

- While Trellix ENS provides web browsing controls through labeling of suspicious websites, it does not 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 security teams and budgets.

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

Trend Micro offers endpoint security through its **Trend Vision One** cyber security platform which delivers XDR across endpoint, email, cloud, network and OT security.

Vison One – Endpoint Security is Trend Micro's cloud solution aimed at endpoints, servers and cloud workloads, which integrates advanced threat protection, EDR/XDR, and threat intelligence. It comes in three packages:

- *Core* – which protects Windows, Linux and macOS endpoints and servers. It offers anti-malware, behavioral analysis, machine learning, web reputation, device control, DLP, firewall, app control, intrusion prevention IPS (OS), and virtualization protection.

- *Essentials* – adds EDR/XDR.

- *Pro* – adds intrusion prevention IPS (server application), and integrity monitoring and log inspection.

All packages can be augmented with email security, mobile security, network security, cloud security and Trend Micro's Zero Trust Secure Access. Essentials and Pro can be further augmented with Trend Micro's MDR **Trend One Service,** and **Trend Vision One – Attack Risk Management (ASRM).**

STRENGTHS

- Trend Micro’s Trend Vision One platform offers 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.

- Vison One – Endpoint Security delivers the benefits of traditional endpoint protection, as well as EDR/XDR in an easy to deploy cloud solution.

- 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 EDR/XDR.

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

- Customers report that access to the higher plans that include the XDR solution, is costly compared to competing solutions.

- Customers report that the management interface could be improved to provide clearer alerts and streamline scripting of workflows.

- Trend Micro lacks visibility in North America.

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 & XDR** 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 Device Control* – provides visibility and control over USB device usage.

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

- *Falcon Intelligence* – automatically investigates incidents and accelerates alert triage and response.

- *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 OverWatch* – is CrowdStrike's 24/7 Managed Detection and Response (MDR) service powered by CrowdStrike expertise and backed by a breach warranty guarantee of up to $1 million. It 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 Identity Protection* – offers threat detection and real-time prevention of identity-based attacks combining AI, behavioral analytics and a policy engine to enforce risk-based conditional access.

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

CrowdStrike also offers:

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

- *Falcon Insight for IOT* – extends EDR/XDR to Extended Internet of Things (XIoT) devices.

- *CrowdStrike Falcon Forensics* – streamlines collection of point-in-time and historic forensic data for post-breach analysis of cybersecurity incidents and compromise assessments.

Falcon Endpoint & XDR is available in the following bundles:

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

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

- **Falcon Enterprise** – adds Falcon Insight XDR, and Falcon OverWatch. Falcon Insight XDR Connector packs, which extend XDR to third party products, are available as add-ons.

- **Falcon Elite** – adds Falcon Discover, and Falcon Identity Protection. Falcon Insight XDR Connector packs are available as add-ons. CrowdStrike Services are also an add-on.

- **Falcon Complete MDR** – offers Falcon Prevent, Falcon Insight XDR, Falcon OverWatch, and Falcon Discover. Falcon Identity Protection is available as an add-on. Falcon Insight

XDR Connector packs are available as add-ons, and CrowdStrike Services are also add-ons.

The **CrowdStrike Marketplace** 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 report 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 focus seems to be mainly on OverWatch, its Managed Detection and Response (MDR) solution, as opposed to product-based solutions.

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

- CrowdStrike once a leader in XDR, appears to have lost some mindshare, as almost all competing vendors now offer XDR, ATP and MDR capabilities.

- A full CrowdStrike deployment including all options, tends to be more expensive than most competing 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. VMware was acquired by Broadcom in November 2023, and currently operates as an autonomous business unit within Broadcom.

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 XDR** – powered by the *VMware Contexta* threat intelligence cloud, extends detection, visualization, and analysis of endpoint, network, workload, and user data in context to enable more effective threat hunting and faster response.

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 assess how beneficial the Broadcom acquisition will be to 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