The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Endpoint Security - Market Quadrant 2021 *

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

November 2021

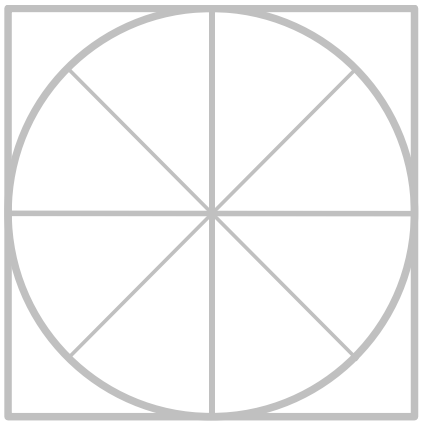

TABLE OF CONTENTS

==========

==========

RADICATI MARKET QUADRANTS EXPLAINED

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

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

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

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

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

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

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

b. In other cases, a vendor may simply have become complacent and be out-developed by hungrier, more innovative Trail Blazers or Top Players.
c. Companies in this stage will either find new life, reviving their R&D efforts and move back into the Top Players segment, or else they slowly fade away as legacy technology.

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

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

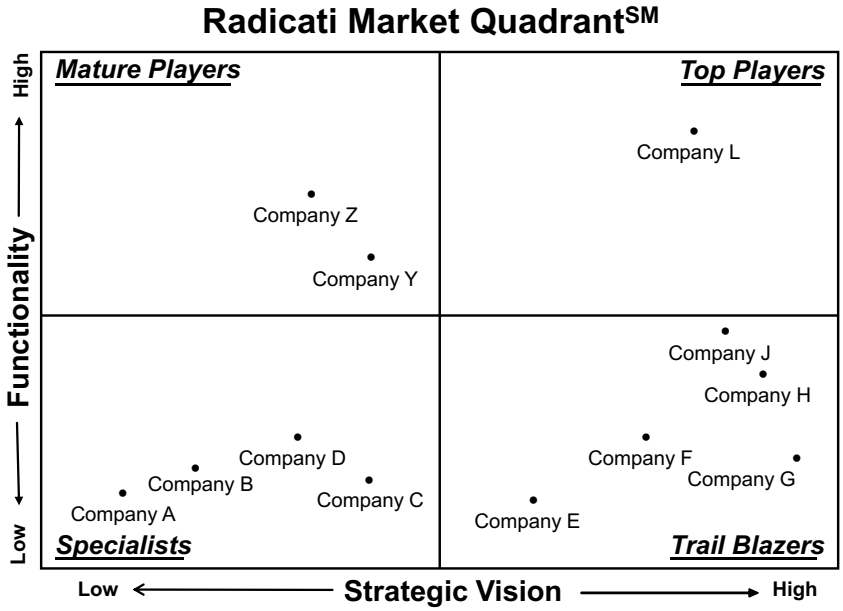

Figure 1: Sample Radicati Market Quadrant

INCLUSION CRITERIA

We include vendors based on the number of customer inquiries we receive throughout the year. We normally try to cap the number of vendors we include to about 10-12 vendors. Sometimes, however, in highly crowded markets we need to include a larger number of vendors.

MARKET SEGMENTATION – ENDPOINT SECURITY

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

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

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

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

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

- The endpoint security market continues to experience very strong growth as organizations of all sizes deploy increasingly sophisticated and feature-rich solutions to help protect against all threats and malicious attacks. The Endpoint Security market is expected to surpass $9.4 billion in 2021, and grow to over $19.8 billion by 2025. Figure 1, shows the projected revenue growth from 2021 to 2025.

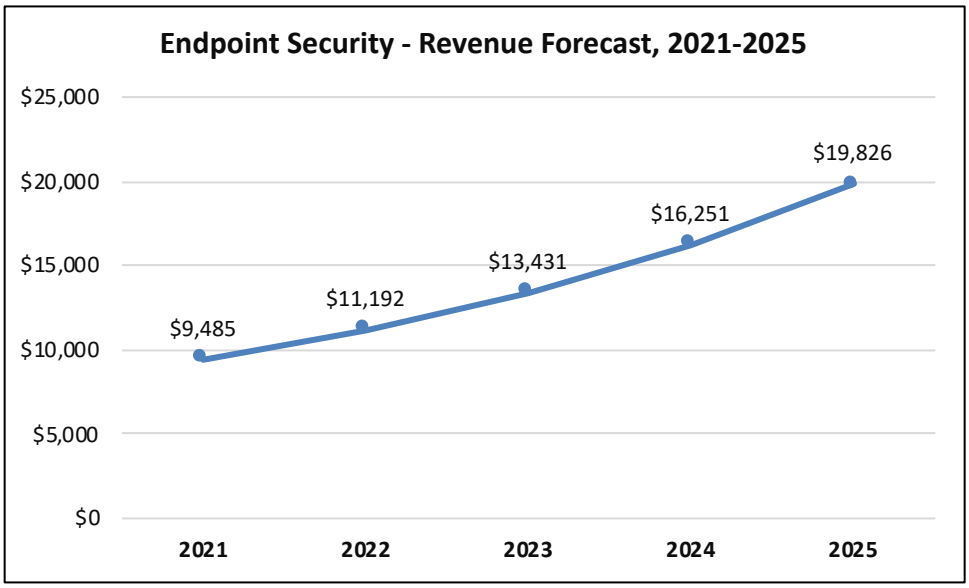

Figure 2: Endpoint Security Market Revenue Forecast, 2021-2025

EVALUATION CRITERIA

Vendors are positioned in the quadrant according to two criteria: *Functionality* and *Strategic Vision*.

Functionality is assessed based on the breadth and depth of features of each vendor's solution. All features and functionality do not necessarily have to be the vendor's own original technology, but they should be integrated and available for deployment when the solution is purchased.

Strategic Vision refers to the vendor's strategic direction, which comprises: a thorough understanding of customer needs, ability to deliver through attractive pricing and channel models, solid customer support, and strong on-going innovation.

Vendors in the *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

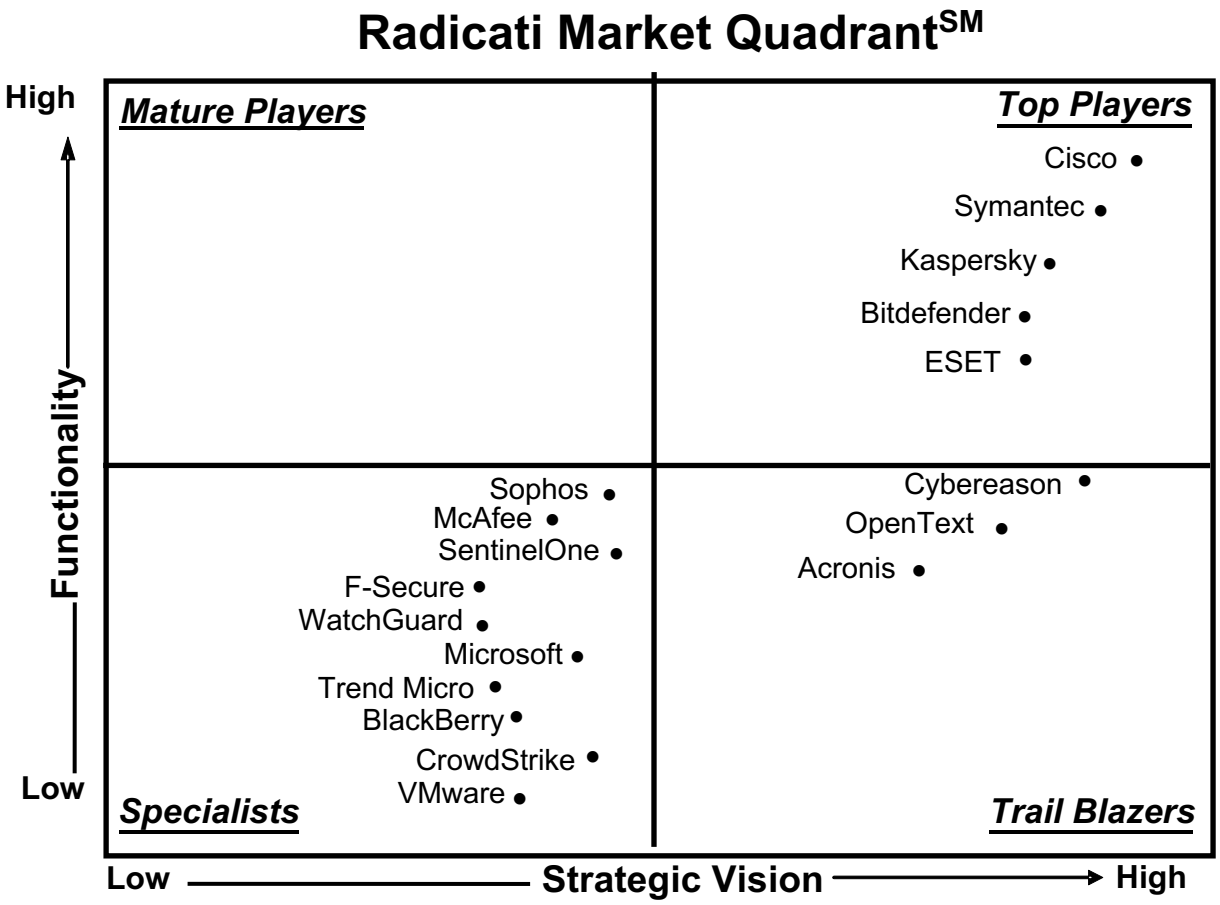

Figure 3: Endpoint Security Market Quadrant, 2021*

* Radicati Market Quadrant℠ is copyrighted November 2021 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT TRENDS

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

- The **Trail Blazers** quadrant includes *Cybereason, OpenText,* and *Acronis.*

- The **Specialists** in this market are *Sophos, McAfee, SentinelOne, F-Secure, WatchGuard, Microsoft, TrendMicro, BlackBerry, CrowdStrike, and VMware Carbon Black.*

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

ENDPOINT SECURITY - VENDOR ANALYSIS

TOP PLAYERS

CISCO

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

Cisco is a leading vendor of Internet communication and security technology. Cisco's security solutions are powered by the Cisco Talos Intelligence Group (Talos), made up of leading threat researchers. Cisco is publicly traded.

SOLUTIONS

Cisco Secure Endpoint (formerly *Advanced Malware Protection for Endpoints*) is a cloud-based endpoint security solution designed to detect, prevent, and remediate advanced threats in a single agent. 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 comprises the following key capabilities:

- *Threat Prevention* – is provided through layered security capabilities which include file reputation, traditional anti-virus, cloud-based sandboxing, file-less in-memory exploit prevention, system process protection, ransomware protection and dynamic behavior-based protection. Cisco Secure Endpoint can automatically detect and block known and emerging threats through real time technologies that include: behavior analysis, big data analytics, machine-learning, signatures and fuzzy fingerprinting. An agent-based capability for offline and realtime behavior analysis protects against malicious use of dual use tools like powershell for launching living-of-the-land attacks. Malicious verdicts from the detonation of unknown files in the sandbox are automatically added to the file reputation in the Cisco's collective threat intelligence cloud. 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. Cloud based machine learning and cross layer static analysis are also used to scale malware detection. For instance, if malicious file behavior is detected, the file is automatically blocked across all endpoints and the Cisco Secure Ecosystem of security control points, and security teams are provided with a recorded history of the malware's behavior and trajectory. Additionally, SecureX, built-in to Secure Endpoint across all offer tiers, helps accelerate incident investigations through automatic context enrichment and allows customers to leverage Cisco incident management playbooks, as well as create their own automated playbooks.

- *Threat Response* – Secure Endpoint provides a suite of response capabilities to contain and eliminate threats across all endpoints. Automated Actions allow administrators to configure event triggered automated responses such as capturing forensic snapshots, endpoint isolation and other incident triage actions. Administrators can search across endpoints using a web-browser based management console using OpenIOC queries for known indicators of compromise and/or more advanced live searches of endpoint telemetry built on top of osquery. Native integration between Cisco Secure Endpoint and Duo also allow customers to automatically prevent compromised endpoints from being used as trusted devices for multi-factor authentication. In addition, SecureX provides threat context enrichment and extends response capabilities by allowing customers to configure or use Cisco curated workflows to automate response actions across the entire security infrastructure.

- *Email and Web security* – all file disposition and dynamic analysis information is shared across the Cisco Secure Ecosystem via collective intelligence. If a file is determined to be malicious via Cisco Secure Email or Web Appliance, that information is shared across all Cisco Secure platforms. Native integration between Secure Endpoint and the Cisco Secure Ecosystem provides global outbreak control, threat context enrichment and global trajectory view of malware ingress across key attack vectors. SecureX orchestration enables to streamline Cisco curated or customer configured workflows between Secure Email and Secure Endpoint for automated cross layer investigation and response actions.

- *Firewall* – Secure Endpoint integrates with Cisco Secure Firewall. All detection information is sent to the Cisco Secure Firewall management platform and can be used to correlate against other network threat activity. Cisco Firewall and Cisco Identity Services Engine (ISE) can be tightly integrated, which allows Secure Endpoint events to trigger policy responses and enforcement in ISE. Secure Endpoint's built-in SecureX incident manager and orchestration provide programable automation workflows that allow orchestration for extended detection and response.

- *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. SecureX orchestration further provides a repository of (extensible) sample automations that customers leverage to hunt for and confirm critical vulnerabilities in the environment and automatically generate tickets on third party ticketing solutions via API to streamline remediation and/or isolate the host.

- *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 with the SecureX platform built-in to deliver XDR outcomes with packaged integrations across multiple third party solutions and the Cisco Secure portfolio, including the Cisco Secure Firewall.

- *Integrations* – Secure Endpoint has an API and built-in XDR platform for custom integrations, and packaged integrations with SIEM/SOAR/MDM tools as well as third party Intelligence sources, operational tools and visibility and protection solutions for enhanced

threat context enrichment and streamlined ITOps and SecOps use cases for endpoint security and extended detection and response across Cisco and third party solutions.

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

STRENGTHS

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

- Cisco Secure Endpoint delivers Endpoint Protection and Endpoint Detection and Response capabilities in a single agent.

- Built-in to Cisco Secure Endpoint, the Cisco SecureX platform delivers threat response with automatic threat context enrichment and unified threat response capabilities across the Cisco Secure Ecosystem, including Endpoints, Network, Email, DNS, and more.

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

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

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

WEAKNESSES

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

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

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

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

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

SYMANTEC

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

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

SOLUTIONS

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

- **Symantec Endpoint Security 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, 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:

- *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.

- *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.

- *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.

- *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.

- *Adaptive Protection* – provides attack surface reduction that evolves with the threat landscape to address each organization's unique environment. It relies on Advanced Machine Learning to automate granular behavioral rules resulting in no operational impact.

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

STRENGTHS

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

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

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

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

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

- Symantec's Integrated Cyber Defense (ICD) platform offers a unified cloud management console across a broad portfolio of security solutions (e.g. endpoint security, network security, information security, and more). It delivers data, analytics, and insights across multiple control points for improved visibility and implementation of extended detection and response (XDR).

WEAKNESSES

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

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

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

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

- Symantec lost some mindshare following the Broadcom acquisition. The vendor is working to address this.

KASPERSKY

39A Leningradsky Highway
Moscow 125212
Russia
www.kaspersky.com

Kaspersky, founded in 1997, provides a wide range of security products and solutions for enterprise business customers and consumers worldwide. The company's business solutions are aimed at a broad range of customers including large enterprises, small and medium-sized businesses. Kaspersky is privately owned.

SOLUTIONS

Kaspersky Optimum Security is a cloud native solution with an on-premise option that brings together endpoint protection, Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR) into a single multi-layered security approach. It comprises the following main components:

- **Kaspersky Endpoint Security for Business** – is a multi-layered endpoint protection platform, which provides security, visibility and manageability of all endpoint devices, including physical and virtual machines, mobile devices, and servers. Kaspersky supports a broad array of platforms, including Windows, Linux, macOS, Android, and iOS. It integrates with Remote Monitoring and Management (RMM) and Professional Services Automation

(PSA) systems from ConnectWise, Autotask, Tigerpaw and SolarWinds. Kaspersky Endpoint Security for Business is available in three different tiers, as follows:

- *Select* – provides trusted Threat Prevention (for Windows, macOS and Linux) with Behavior Detection, Exploit Prevention, Host Intrusion Prevention, Remediation Engine, Web, Device and BadUSB controls, Mobile Threat Defense, Mobile Device Management (MDM), and Security Management.

- *Advanced* – in addition to Select capabilities, adds Application Control for servers, Adaptive Anomaly Control to capture deviations from user's behavior baseline and stop execution, Data Protection (i.e. OS encryption management, full disk and file-level encryption), Firewall and OS firewall management, Patch Management, Protection for terminal servers, OS and third party application deployment.

- *Total* – in addition to all Select and Advanced capabilities, protects the enterprise perimeter by preventing the effects of web-based attacks before they reach the endpoint level, by blocking malware, online phishing, reducing access to unsolicited resources and preventing illegitimate data transfers at the gateway level.

- **Kaspersky Endpoint Detection and Response Optimum** – is an EDR tool which works together with endpoint protection and provides endpoint visibility, root cause analysis and automated response options as well as Indicator of Compromise (IoC) scanning. It adds an automated layer of defense, providing attack spread path visualization, and delivers detailed information on the alert, the host, suspicious objects, and more.

- **Kaspersky Managed Detection and Response Optimum –** is an MDR service which delivers continuous 24/7 managed protection, enabling organizations with a lack of resources and expertise to automatically hunt down evasive threats, including those that circumvent existing detection and prevention systems, while freeing up mature IT security teams to focus on critical.

Kaspersky Optimum Security exists within Kaspersky security ecosystem and is complemented by:

- **Kaspersky Sandbox (KSB)** – complements endpoint protection with functionality that can easily detect new, unknown and evasive threats. It creates a virtualized environment, where

suspicious objects are sent, analyzed with a variety of methods (e.g. simulating user activity, behavior analysis, monitoring outgoing connections, and more), and their reputation recorded. If objects are identified as malicious, the whole infrastructure can be scanned and malicious activity prevented, ensuring an automated response across all endpoints.

- **Kaspersky Hybrid Cloud Security** – protects public datacenters (i.e. Microsoft Azure and Amazon AWS), physical servers, desktops and private data centers based on native API integrations with VMware, Citrix, Microsoft Hyper-V, KVM and Docker virtual environments. Kaspersky Hybrid Cloud Security is optimized for integration with public and private discovery and deployment tools, and relies on virtualization to optimize resource use and reduce infrastructure costs.

All endpoint security products are managed by the **Kaspersky Security Center** console, which delivers security management and control through a single administrative tool. The management console allows organizations to identify all endpoint assets (physical, virtual, mobile), conduct fast vulnerability assessments, achieve a real-time hardware and software inventory, and offer actionable reporting. The console can be used as a SaaS offering, or be deployed on public cloud or on-premises environments and accessed through a web-interface.

For SMB customers, Kaspersky offers **Kaspersky Endpoint Security Cloud**, which is an endpoint protection product that provides a cloud-based management solution for securing Windows and macOS endpoints, file servers, iOS and Android devices.

In addition, **Kaspersky EDR** provides IT security/SOC enterprise teams with a tool for in-depth incident investigation and centralized response. It offers advanced threat discovery, deep investigation and threat hunting, as well as incident response.

Kaspersky offers a full-scale Enterprise Security solution comprising the following products and services: Endpoint Security, Endpoint Detection and Response, Hybrid Cloud Security, Managed Detection and Response, Embedded Systems Security for ATM and PoS protection, Private Security Network, Security Awareness training, Premium Support and Professional Services.

STRENGTHS

- Kaspersky Endpoint Security for Business supports a broad range of operating systems, including Windows, Linux, macOS, Android and iOS; as well as virtualized environments including VMware, Citrix, KVM, MS Hyper-V and Docker.

- Kaspersky EDR Optimum provides alert context and quick automated response options to analyze and remediate evasive threats, as well as search the infrastructure for current threats with Indicator of Compromise (IoC) scanning and automatic response to discovered threats.

- Kaspersky MDR Optimum supports multiple operating systems, including Windows, Linux and macOS as well as virtualized environments, making it easier for organizations with heterogenous infrastructures to protect their assets in a managed way.

- Kaspersky solutions rely on its own low footprint, high-performance security technologies. Machine learning based Behavior Detection technology implements a Memory Protection mechanism, which guards system-critical processes and prevents leaking user and administrator credentials.

- The cloud-based or on premises Kaspersky Security Center management consoles provides a comprehensive management tool that allows organizations to identify all endpoint assets (e.g. physical, virtual, and mobile), as well as conduct fast vulnerability assessments. It can also automatically perform patch remediation and offer actionable administrator reporting.

- Kaspersky offers strong support for virtual environments. Kaspersky Hybrid Cloud Security offloads resource intensive anti-malware scans onto a specialized virtual appliance, an approach which places less load on computing resources and helps businesses maintain high virtualization densities and performance.

- Kaspersky Endpoint Security for Business includes MDM, mobile security and mobile application management capabilities, all of which can be managed through a single console.

WEAKNESSES

- Kaspersky Endpoint Security for Business does not currently provide content-aware DLP, or support ICAP for integration with third-party DLP solutions. This functionality, however, is

available for Microsoft Office 365 and Microsoft Exchange.

- Kaspersky Endpoint Security for Business does not support 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).

- Kaspersky EDR Optimum does not currently provide support for Linux and MacOS endpoints. The vendor has this on its future roadmap.

- Kaspersky EDR Optimum is not yet available for mobile devices. The vendor has this on its future roadmap.

- While the Kaspersky Security Center console currently allows monitoring of Kaspersky's Secure Email Gateway (thus helping integrate visibility across endpoints and email security), management of email security currently requires a separate console. Integration of email security management capabilities is on the roadmap for future releases.

BITDEFENDER

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

Bitdefender, founded in 2001, delivers next-generation anti-virus software, internet security software, endpoint security, and other security solutions through a network of value-added alliances, distributors and reseller partners. The company delivers solutions for businesses and consumers across more than 150 countries. The company is privately held.

SOLUTIONS

Bitdefender's **GravityZone**, is a hosted enterprise security platform that provides security controls and security posture management across endpoints, cloud workloads, network and users. For customers with restricted cloud usage, GravityZone can also be deployed on-premises.

Bitdefender security agents can be installed on all leading platforms including Windows, Linux, Mac, Android, iOS and Microsoft Exchange.

The Bitdefender Business Portfolio includes a number of GravityZone security packages and a-la-carte offerings, as follows:

GravityZone Business Security package – is aimed at small businesses. It provides protection for physical and virtual desktops and servers, combining security with centralized management. It is available on-premises, or as a cloud service.

GravityZone Advanced Business Security package – is aimed at the needs of medium sized businesses. It offers the same services as Business Security but adds security services for protecting Microsoft Exchange servers and mobile devices. It includes a feature called Smart Central Scan, which allows Security administrators to offload anti-malware processes to a centralized scanning server, thus lowering the resource consumption on protected systems. The solution is available on-premises or as a cloud service, and can protect desktops, servers and Microsoft Exchange mailboxes. The mobile security (MDM) component, however, is only available for on-premises deployment.

GravityZone Elite package – offers the same services as Advanced Business Security but adds two pre-execution detection layers; HyperDetect, and Sandbox Analyzer. Hyperdetect uses specialized local machine learning models and behavior analysis techniques to detect hacking tools, exploits and malware obfuscation techniques. Sandbox analyzer detonates payloads in a contained virtual environment, analyzes their behavior, reports malicious intent and provides actionable insight. The solution is available on-premises or as a cloud service, and can protect desktops, servers and Microsoft Exchange mailboxes. The mobile security (MDM) component, however, is only available for on-premises deployment.

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

Bitdefender eXtended Endpoint Detection and Response (XEDR) – is natively integrated into GravityZone and extends EDR analytics and event correlation capabilities beyond the boundaries of a single endpoint, to enable organizations to deal more effectively with complex cyber-attacks involving multiple endpoints. It brings together device intelligence across the enterprise network, to help incident response teams effectively investigate and respond to advanced threats.

GravityZone Enterprise Security – is aimed at the needs of large enterprises and hybrid infrastructures. It is available only as an on-premises solution and provides security services for protecting physical and virtual desktops and servers, Microsoft Exchange servers and mobile devices.

GravityZone Security for Virtualized Environments (SVE) – is a security module delivered within GravityZone Enterprise Security. It uses a vendor-agnostic architecture to support any hypervisor, whether natively integrated or standalone. SVE leverages multiple techniques to achieve deduplication and provide high operational value. This offloading is also present in the AWS module, and can also be used in physical environments (e.g. laptops or desktops) since the enforcement point, Bitdefender Enterprise Security Tools (BEST) is common to SVE and Endpoint Security; BEST can operate in full offload, partial offload or traditional local scanning.

GravityZone Security for Containers – protects containers and cloud workloads against modern Linux and container attacks by using AI threat prevention, Linux-specific anti-exploit technologies and context-aware endpoint detection and response (EDR). The Bitdefender endpoint agent for Linux does not require Linux-kernel components, enabling rapid deployment of new distributions.

GravityZone Security for MSPs – is a solution portfolio tailored to meet the needs of Managed Security Service Providers. It offers a multi-tenant management console and simple monthly licensing. It is available in different packages which include endpoint protection, patch management, Advanced Threat Security (with HyperDetect and Sandbox Analyzer), and Endpoint Detection and Response.

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

Bitdefender also offers **Email Security, Security for Storage, Patch Management and Full Disk Encryption add-ons**, all of which can be managed via the GravityZone console.

GravityZone Hypervisor Introspection (HVI) – is aimed at protecting virtual workloads, enabling data centers and organizations to increase their security posture across their entire infrastructure. HVI is an opensource project,

STRENGTHS

- Bitdefender relies on various non signature based techniques including heuristics, machine learning models, anti-exploit, cloud-based sandbox analyzer and process inspector to keep up with the latest threats.

- Bitdefender's GravityZone Ultra Suite is an integrated platform, easily deployed by organizations of all sizes, to covers risk analytics, hardening, prevention, and XDR for endpoints, cloud resources, and network connected devices.

- Bitdefender tends to receive very high scores in third-party AV testing.

- All Bitdefender anti-malware technologies are developed in-house. Bitdefender licenses its technology to a number of OEM partners.

- Bitdefender GravityZone integrates with Microsoft Active Directory, as well as VMware vCenter and Citrix XenServer to facilitate syncing of inventories and policy enforcement and management. In addition, Bitdefender can automatically detect other computers within the network using Windows Network Discovery, and protection can be deployed remotely to all unprotected systems.

- The new Linux and Container security stack does not require Linux-kernel components, facilitating deployment of new distributions by organizations.

WEAKNESSES

- Bitdefender offers a Mobile Security (MDM) solution for Android and iOS platforms. However, it is currently available only for its GravityZone on-premises solutions.

- While offering highly accurate malware and threat detection solutions, Bitdefender currently lacks integration with SOAR tools. The vendor has this on its roadmap.

- While Bitdefender offers DLP fully integrated into GravityZone at no extra charge, this is still fairly basic functionality.

- Bitdefender currently supports only full volume encryption. The vendor is working to add greater granularity in future releases.

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

ESET

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 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, anti-theft, SMS/call filtering and device security. It integrates with ESET PROTECT, allowing for security polices to be deployed across both PCs and mobile devices.

- **ESET Mobile Device Management for iOS** – is an integration of the Apple iOS MDM framework with ESET PROTECT which supports the configuration of security settings for iOS devices. Administrators can enroll iPhones and iPads, as well as setup security profiles and adjust device settings, such as: anti-theft, settings for Microsoft Exchange, WiFi, VPN accounts, Passcode, iCloud and more.

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

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

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

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

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

- **ESET PROTECT** – is a cloud based management console with the possibility of an on premises deployment. Provides real-time visibility of all endpoints: desktops, servers, virtual machines, as well as managed mobile devices. A single pane of glass enables full reporting for ESET Security solutions. It serves to control endpoint prevention, detection & response layers across all platforms.

In addition, ESET provides the following services and solutions:

- **ESET Enterprise Inspector** – is ESET's EDR solution for identification of anomalous behavior and breaches, risk assessment, incident response, investigations and remediation. It references its detections to the MITRE ATT&CK framework.

- **ESET Dynamic Threat Defense (EDTD)** – is ESET's managed cloud sandbox analysis solution. It is managed by ESET PROTECT and provides an additional layer of security for ESET products like Mail Security and Endpoint products by utilizing cloud-based sandboxing technology to detect new, never-seen-before threats.

- **ESET's Threat Intelligence service** – provides global knowledge gathered by ESET threat intelligence experts on targeted attacks, IOCs (IP, URL, file hash) advanced persistent threats (APTs), zero-days and botnet activities. It can integrate with existing SIEM tools and features YARA rules to allow organizations to set up custom rules.

- **ESET Managed Detection and Response Service** – is ESET's cybersecurity service for the investigation of incidents, analysis of potentially harmful files and fast response and remediation of incidents.

- **ESET Premium Support** – is ESET's cybersecurity service for responsive, tailored support to reduce the risk of any interruption in operational continuity. It offers 365/24/7 access to a team of ESET experts.

- **Security Services for Endpoints** – ESET's 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. It supports mobile applications, push notifications, hardware tokens, and FIDO security keys. It also integrates with ADFS 3.0, or the SAML protocol.

- **ESET Cloud Office Security** – provides advanced preventive protection for users of Microsoft 365 applications. It combines spam filtering, anti-malware scanning and anti-phishing to help prevent incoming external email from being used as a channel for targeted attacks. Anti-malware protection also protects OneDrive, Teams and SharePoint Online and helps mitigate the risk of malware spreading to other devices.

STRENGTHS

- ESET Endpoint Security solutions are well-known to offer high performance and high detection rates.

- ESET solutions offer a low footprint with low system resource usage. The solutions are designed for ease of deployment and use.

- 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, Linux, and more.

WEAKNESSES

- ESET does not currently offer extended detection and response (XDR). The vendor has this on its roadmap.

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

- ESET is widely recognized in Europe but currently lacks market visibility in North America. The vendor is working to address this.

TRAIL BLAZERS

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 privately held.

SOLUTIONS

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

- **Cybereason XDR** – offers unified detection and response capabilities that find and end MalOps (malicious operations) across the entire IT stack including endpoint, application

suites, user personas, on-premise network and cloud deployments. Cybereason XDR simplifies log management and data collection tasks, agent deployment and maintenance cycles, and unifies device and identity context in a single, visual investigation experience.

- **Cybereason Prevention** – leverages signature based, behavioral, and machine-learning approaches to stop threats from both known and unknown attacks; this includes 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 time-line, 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 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. Cybereason EDR can identify threats quickly using behavioral analysis that leverages cross-machine correlations and enriched data from across all endpoints in real-time, and helps significantly reduce the workload for security teams.

- **Cybereason Investigation & Hunting** – 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 can quickly identify any malicious activity in their environment and easily hunt for TTPs with syntax-free and visual based searches. 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, through any combination of detection, investigation, breach containment, and response needs. It also offers a $1M breach protection warranty with select product and service packages. Services offered include:

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

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

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

STRENGTHS

- The Cybereason Defense Platform, composed of EPP and EDR and XDR functionalities, is available via multiple deployment options, or as a managed service via a single agent deployment.

- The 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 joined a strategic partnership with Google Cloud to deliver a unified XDR solution, Cybereason XDR powered by Chronicle, which allows customers to understand the full scope of attacks fast within a single view, easily hunt for threats, and efficiently remediate attacks.

- 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 an advanced, comprehensive set of features and functionality.

WEAKNESSES

- The Cybereason Defense Platform currently does not have native vulnerability assessment capabilities. The vendor is working to address this through technology partners.

- The Cybereason Defense Platform does not currently support URL filtering, a capability which is common with many competing solutions.

- Cybereason does not currently offer its own Sandboxing technology. However, the vendor integrates with the VMRay solution.

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

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

- Cybereason is currently best known in Europe and Asia/Pacific, however, the vendor is in investing to increase its presence in North America.

OPENTEXT

385 Interlocken Crescent, Suite 800
Broomfield, CO 80021
www.webroot.com

OpenText offers information management solutions, powered by OpenText Cloud Editions, a cloud-native containerized architecture. Webroot, an OpenText company acquired in 2019, delivers threat intelligence and protection for endpoints and networks to business and consumer users worldwide. EnCase, originally developed by Guidance Software and acquired by OpenText in 2017, is a suite of products designed for forensic, cybersecurity, security analytics and e-discovery. OpenText is publicly traded.

SOLUTIONS

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

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

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

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

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

- **Webroot Business Endpoint Protection** – is a real-time, cloud-based approach to preventing system compromises through advanced machine learning and threat intelligence. It is compatible with Microsoft Windows PCs and Servers, as well as Apple Mac devices;

Terminal Servers and Citrix; VMware; Virtual Desktops and Servers, and Windows embedded Point of Sale (POS) systems. It offers the following capabilities:

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

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

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

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

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

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

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

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

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

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

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

STRENGTHS

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

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

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

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

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

WEAKNESSES

- OpenText EnSuite solutions are not available as a SaaS software offering.

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

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

- Granularity on the firewall is somewhat limited when compared to other vendors.

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

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

ACRONIS INTERNATIONAL GMBH

Rheinweg 9,
8200 Schaffhausen
Switzerland
www.acronis.com

Acronis is a cyber protection company which develops on-premises and cloud software for endpoint protection, backup, disaster recovery, and secure file sync and share. The company has corporate headquarters in Schaffhausen, Switzerland, with global headquarters in Singapore, and 18 offices worldwide. Acronis is privately held.

SOLUTIONS

Acronis offers several solutions in the endpoint security space, which include: **Acronis Cyber Protect**, **Acronis Detection and Response**, and **Acronis DeviceLock DLP**. Acronis solutions can be deployed on-premises, or in private or public clouds. The solutions are aimed at SMEs and MSPs on a worldwide basis. Platforms supported include Windows 7+, Windows Server 2008 R2+, macOS, and Linux. Android and iOS support is only provided for Data Protection.

- **Acronis Cyber Protect** – is an endpoint protection solution that integrates data protection with cybersecurity, bringing together cybersecurity and endpoint protection management, antimalware, and backup and recovery into a single pane of glass. Acronis Cyber Protect is delivered as one agent, one management interface and one license to offer ease of use and deployment through an integrated solution. It offers the following key features and functionality:

    - *Vulnerability assessments* – patch management, removal of malware from backups, and drive health.

    - *Continuous data protection* – real-time malware defenses, self-defense capabilities.

    - *Integrated disaster recovery* – forensic backups, and the ability to co-exist with other security solutions.
    - *Auto-discovery* – of new devices, vulnerability assessments, and data protection map.

    - *Remote agent installation* – backup and disaster recovery, unified protection policies management, data loss prevention (DLP) with device control.

    - *Defenses against malware and exploits* – with behavior-based heuristics, hard drive health control, dashboards and reports.

    - *Patch management* – integrated with backup, malware quarantine, rescue with bootable media, and remote device wipe.

    - *Continuous Data Protection* – helps avoid any data loss in key applications.

- *Fail-safe Patching* – automatically backs up endpoints before installing any patches enabling immediate roll-back.

- *Anti-malware scans of data in the Acronis Cloud* – serve to offload and enable more aggressive scans and vulnerability assessments in central storage.

- *Forensic Backup* – helps include valuable digital evidence in backups to simplify and speed up investigations.

- *Data Protection Map* – serves to monitor the protection status of files with classification, reporting, and unstructured data analytics.

- *Safe Endpoint Recovery* – scans for malware and updates AV definitions during recovery to prevent threats from reoccurring.

- *Smart Protection Plan* – provides auto-adjust patching, scanning, and backup to current Acronis Cyber Protection Operations Centers alarms.

- *Global and Local Allowlists* – support more aggressive heuristics by preventing false detections with automatic allowlisting.

- **Acronis Detection and Response** – based on Acronis' acquisition of Nyotron, is a last line of defense that protects organizations against threats that may evade typical anti-malware defenses. It is designed around a zero trust approach, it detects and prevents any deviations from legitimate OS behavior and provides real-time visibility, as well as automatic and manual remediation capabilities. Acronis Detection and Response adds post-breach threat detection and response capabilities to the security stack. It offers the following key capabilities:

  - *Automatic, real-time protection* – automatically stops threats once detected, unlike solutions that require manual or semimanual threat hunting and remediation.

  - *Threat-agnostic protection* – helps detect and prevent advanced attacks that evade next-generation antiviruses (NGAVs), such as new or unknown malware and ransomware, fileless attacks, zero-day attacks, and advanced persistent threats (APTs).

- *Zero trust approach* – increases threat detection accuracy with a zero trust approach, recognizing any deviations from legitimate OS behavior instead of having to identify constantly evolving attack techniques.

- *No data deluge* – empowers security teams with detailed, focused visibility into threats and incidents without the need for manual threat hunting and analysis of overwhelming amounts of data.

- **Acronis DeviceLockDLP** – is an endpoint data loss prevention solution that reduces the risk of insider-related data leaks. It enforces fine-grained contextual controls (based on user authentication, security group memberships, data types, device types or network protocol, data flow direction, state of media or SSL encryption, date and time, and other factors) in combination with content analysis and filtering to block or allow data access and transfer operations. Acronis DeviceLock DLP is comprised of multiple complementary, function-specific components allowing customers to choose the best configuration for their security requirements and budget.

STRENGTHS

- Acronis's solution tightly integrates backup, disaster recover (DR), anti-malware, anti-ransomware, detection and response, patch management, vulnerability assessments, URL filtering, email protection, and DLP into a single product.

- Acronis offers as a single agent, with a single UI, policy, and management portal for all its solutions.

- Acronis scores highly in independent third party AV tests.

- Acronis deep integration offers continuous data protection, fail safe patching, safe endpoint recovery (integrates anti-malware and patching into recovery), and forensic backup (image-based backups that capture additional data for forensic investigations).

WEAKNESSES

- Acronis' solution does not yet offer integration with directory services. The vendor has this on its roadmap.

- Acronis does not currently offer EDR capabilities, however this is on the vendor's near term roadmap.

- The Acronis solution does not offer integrated firewall functionality. However, an open REST-API is available for integration.

- The Acronis solution does not offer full disk encryption or network access control (NAC).

- Mobile device protection capabilities are only minimal, at this time.

- Acronis does not yet offer MDR services, however this is on the vendor's roadmap.

- While offering some unique capabilities and a strong cybersecurity feature set, Acronis is still not well known in the endpoint protection space. The vendor is working to address this.

SPECIALISTS

SOPHOS

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

Sophos offers IT security solutions for businesses, which include encryption, endpoint, email, Web, next-generation firewall (NGFW), and more. All solutions are connected with Sophos Central, Sophos's integrated cloud-based management console, and backed by SophosLabs, its

global network of threat intelligence centers. The company is headquartered in Oxford, U.K. In 2020, Sophos was acquired by private equity firm Thoma Bravo.

SOLUTIONS

Sophos offers the following endpoint security solutions: **Intercept X Advanced**, **Intercept X Advanced with XDR**, **Intercept X with MTR Standard,** and **Intercept X with MTR 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. The Sophos **Managed Threat Response (MTR)** Service adds a 24/7 managed detection and response service in addition to the features in Intercept X Advanced with XDR.

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

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

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

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

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

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

Opera.

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

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

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

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

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

Sophos Intercept X Advanced for Server (available as *Intercept X Advanced for Server*, *Intercept X Advanced for Server with XDR*, and *Intercept X Advanced for Server with MTR*) includes all Intercept X Advanced functionality with the addition of Application Lockdown, File Integrity Monitoring and visibility into organizations' wider cloud environments (e.g. serverless functions, S3 buckets and databases). It offers:

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

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

- *Cloud Workload Protection* – detect cloud workloads as well as critical cloud services including S3 buckets, databases and serverless functions, identify suspicious activity,

spot insecure deployments and close security gaps.

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

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

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

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

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

Sophos also offers **Sophos Mobile** and **Intercept X for Mobile** as separate add-ons. All Sophos solutions are managed via **Sophos Central**, an integrated cloud-based management console for all Sophos solutions. **Sophos Rapid Response** is an emergency incident response service for organizations experiencing an active cyberattack. It is available to existing Sophos customers, as well as non-customers (included in Sophos MTR service).

STRENGTHS

- Sophos 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, delivers protection and context reporting for customers who use Sophos Intercept X and the Sophos XG firewall.

- 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's Sandstorm sandboxing functionality.

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

- Customers we spoke with as part of this research, indicated that reporting features, while adequate, could be improved to offer greater customization.

MCAFEE

2821 Mission College Boulevard
Santa Clara, CA 95054
www.mcafee.com

McAfee Enterprise offers security solutions, threat intelligence and services that protect business endpoints, networks, servers, the Cloud and more. In July 2021, McAfee Enterprise was acquired by a consortium led by Symphony Technology Group (STG). In September 2021, STG also

announced the acquisition of FireEye products and its intent to combine McAfee Enterprise and FireEye products into a new pure play cybersecurity company.

SOLUTIONS

McAfee Endpoint Security, the company's endpoint protection platform (EPP), uses machine learning analysis, analytics for file-less attacks, dynamic application containment, and works with local and global threat intelligence to provide comprehensive insights across all threat vectors: file, web, message, and network. McAfee endpoint security solutions are compatible with Windows workstations and servers, macOS, VMware ESX, Linux, Citrix XenDesktop and XenServer, and other virtual platforms.

McAfee's **MVISION** portfolio of cloud-native security tools offers cloud-based MVISION EDR which provides automated, AI-guided investigations for security practitioners of any experience level. It works with McAfee Endpoint Security, as well as with third-party EPPs. All security solutions can be managed through **ePolicy Orchestrator (ePO)**, which is available with a choice of on-premise, virtual, or SaaS-based delivery which provides a single management system that offers centralized visibility across multiple security products and the entire threat defense lifecycle.

McAfee's MVISION portfolio is sold as a subscription service, with a choice of *MVISION Standard*, *MVISION Plus*, or *MVISION Protect Plus EDR for Endpoint*, which offer the following components to meet different customer needs at different price points:

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

- **McAfee Endpoint Security** – combines granular controls with layers of integrated capabilities like endpoint detection and response (EDR), machine learning analysis to provide full-stack protection for Windows, macOS, and Linux systems, and automatic rollback remediation capabilities. In-depth defenses collaborate to inform, analyze and automate responses.

- **McAfee MVISION Mobile** – 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.

- **McAfee MVISION EDR–** is McAfee's endpoint detection and response (EDR) solution, which offers AI-guided investigations and data visualization to enable security analysts to prioritize, investigate and remediate threats.

- **McAfee's ePolicy Orchestrator (ePO)** – offers centralized management to provide instant visibility into the state of security defenses. Insight into security events allows administrators to understand and target updates, changes, and installations to systems. McAfee ePO can be deployed on-premises, or as a cloud service through two options: McAfee ePO on Amazon Web Services (AWS), or a SaaS option called McAfee MVISION ePO.

- **McAfee MVISION Insights** – intelligently drives endpoint security to preempt attacks before they happen through a single console to speed threat assessment and response. It offers real-time intelligence gathered from one billion sensors to proactively identify potential threats, assess organization's security posture based on their configuration and unique risk profile, and actionable recommendations to proactively protect against threats.

- **McAfee XDR** – is McAfee's extended detection and response solution which aggregates all data necessary to analyze, evaluate and respond to threats across endpoint, network and cloud components. It delivers a simplified fully-integrated workflow to triage and orchestrate incident response with prescribed actionable intelligence.

McAfee's MVISION portfolio also offers *Device-to-Cloud suites* a three-tier solution bundle which combines McAfee Endpoint Security and MVISION Insights, as follows:

  - *MVISION Advanced* – McAfee Endpoint Security and MVISION Insights.

  - *MVISION Premium* – adds to Advanced, Endpoint Detection and Response (EDR), and Endpoint DLP capabilities.

  - *MVISION Complete* – adds to Premium, MVISION Unified Cloud Edge (UCE), to offer combined secure web gateway, advanced DLP, and Cloud Access Security Broker (CASB) capabilities.

STRENGTHS

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

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

- McAfee's MVISION 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.

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

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

WEAKNESSES

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

- McAfee solutions do not provide third party software patch assessment and remediation.

- Customers we spoke with as part of this research indicated that McAfee's EDR/XDR capabilities are still rather basic, and don't offer the depth and detail provided by competing solutions.

- McAfee does not offer its own email gateway solution, which may disappoint customers that want to source endpoint, email and web security from a single vendor.

- McAfee is undergoing a number of ownership transitions and management changes, first being spun off from McAfee as McAfee Enterprise, and more recently being united with

FireEye Products into a combined company. At the time of this writing, it is too early to know what effect this will have on the company's future direction.

SENTINELONE

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

SentinelOne, founded in 2013, delivers artificial intelligence powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single platform. SentinelOne is privately held.

SOLUTIONS

SentinelOne **Singularity,** is a security platform that consolidates endpoint protection, endpoint detection and response (EDR), IoT security, cloud security, and IT operations capabilities. It offers autonomous 'Sentinel' agents for Windows, Mac, Linux, and Kubernetes and supports a variety of form factors including physical, virtual, VDI, customer data centers, hybrid data centers, and cloud service providers. Sentinels are managed via a globally available multi-tenant SaaS designed for ease-of-use and flexible management. SentinelOne is available in the following tiered product offerings:

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

- **Singularity Control** – adds to the capabilities of Core a "security suite" of features for endpoint management which include: OS Firewall control with location awareness, USB

device control, Bluetooth controls, rogue visibility to uncover devices on the network that need Sentinel agent protection, and secure remote shell capabilities.

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

In addition, SentinelOne also offers the following functionality:

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

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

- **Singularity XDR** – empowers SOC analysts with end-to-end enterprise visibility, analytics, and automated response across the entire technology stack. It can automatically block sophisticated attacks against endpoints, IoT, cloud workloads, and secure access service edge (SASE) without analyst intervention.

- **Singularity XDR Power Tools** – are a set of tools which complement Singularity EDR and XDR capabilities with advanced investigative workflows and rich retrospective information to support comprehensive incident response.

- **Singularity Signal** – is a subscription service designed to supplement its endpoint security SaaS offerings. The Singularity MDR Team is the human side to the AI-based Singularity platform. It offers the expertise of an in-house, non-outsourced Team of cybersecurity

experts monitoring millions of endpoints.

- **SentinelOne Readiness Services –** is an offering designed around agent deployment and periodic health checks. It is designed to help customers accelerate SentinelOne agent rollout planning, installation execution, policy fine tuning, and to help handle in the short term any discovered infections.

STRENGTHS

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

- SentinelOne offers a fully converged Endpoint Protection Platform (EPP) and Endpoint Detection & Response (EDR) 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 also provides patented 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. The vendor is working to address this.

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

- SentinelOne does not offer application whitelisting.

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

- SentinelOne does not offer URL filtering or browser isolation.

- SentinelOne offers only basic mobile capabilities through a partnership with Lookout Security, however this is provided as an extra cost option. The vendor is working to address through further integrations on its nearterm roadmap.

- SentinelOne does not currently offer content-aware Data Loss Prevention capabilities.

F-SECURE

Tammasaarenkatu 7
P.O. Box 24
00181 Helsinki
Finland
www.f-secure.com

F-Secure, founded in 1988, offers cyber security products and services for enterprise and consumer customers. In the business space, the company offers cloud-based solutions for endpoint protection, detection and response, Microsoft 365 and Salesforce protection, advanced threat protection and vulnerability management, as well as security consulting services such as red teaming, security awareness training and cyber security assessments. F-Secure has a global presence, with headquarters in Finland, and is publicly traded.

SOLUTIONS

F-Secure's cloud-native endpoint protection is available with EDR, cloud protection for Microsoft 365 and vulnerability management with a single agent and cloud-based management, or as a managed service:

- **F-Secure 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 SharePoint and Exchange components, with application control, device control and fully integrated patch management.

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

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

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

  - *Threat hunting* – allows advanced search of events for hunting signs of threats or finding more context for incidents being investigated.

  - *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 expert service* – is available through F-Secure's managed detection and response team; the team can provide expert advice based on incident analysis and investigations, with a 2-hour response time.

  - *Clients* – are designed to work with any endpoint protection solution, and function with F-Secure's endpoint security solutions within a single-client and management infrastructure supporting Windows, macOS and Linux.

F-Secure Business Suite is an on-premise alternative for endpoint protection. **F-Secure Countercept** is F-Secure's MDR, managed advanced threat hunting and response service, which offers 24/7 protection against skilled cyber adversaries.

F-Secure Elements Endpoint Detection and Response is an XDR solution when it is combined with **F-Secure Elements for Microsoft 365**, a solution to protect cloud-based Office 365 email and collaboration from advanced threats like phishing, as well as detecting compromised Azure AD accounts. F-Secure Elements Security Center is a cloud native management platform, also managing **F-Secure Elements Vulnerability Management**, a solution which delivers extensive network- and host-based vulnerability scanning, prioritization and management.

STRENGTHS

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

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

- F-Secure uses a multi-layered architecture for malware detection and endpoint protection. Including DeepGuard, its advanced heuristic and behavioral analysis technology.

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

- The footprint of F-Secure 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.

WEAKNESSES

- F-Secure does not offer DLP capabilities.

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

- F-Secure's endpoint security only uses sandboxing to generate application reputation, while its full sandboxing capability is only included in its email security solution, F-Secure Elements for Microsoft 365.

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

- F-Secure only supports native Windows and macOS full disk encryption.

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

WATCHGUARD

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

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

SOLUTIONS

WatchGuard offers the cloud-native **Unified Security Platform (USP)**, a scalable platform for modern security delivery. Within the USP, **WatchGuard Cloud** is the centralized management interface, and the authority for security policy management, dissemination, and enforcement for security solutions for network, Wi-Fi, MFA and the WatchGuard Endpoint Security family of products. WatchGuard Endpoint Security includes advanced endpoint protection complemented by endpoint detection and response (EDR), and specialized security services. The solutions include:

- **WatchGuard EPP** – offers all the capabilities of Endpoint Protection, plus it adds web access control(URL filtering by category) and antispam and anti-malware protection for

Microsoft Exchange. It is available for Windows, macOS, Linux, and Android, however, web access control functionality is available for Windows only.

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

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

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

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

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

- *Essential Threat Hunting Service* – is a cloud based managed service which provides real-time intelligence on the events taking place on an organization's devices to discover threats that are cannot be identified using automated detection mechanisms, it also serves to investigate anomalous users, machines and application behavior. The information it provides helps security teams conduct improve remediation reduce the attack surface.

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

WatchGuard also offers the following complementary add-ons:

- **Advanced Reporting Tool (ART)** – is an optional module that can be used to augment Adaptive Defense and Adaptive Defense 360, to provide detailed information on applications and vulnerabilities. It provides pre-defined queries, dashboards, and alerts that provide insights into what is going on at the endpoints out-of-the-box. Managers can also create their own queries and alerts based on the endpoints telemetry.

- **WatchGuard Patch Management** – is an add-on to Panda Endpoint Protection, Panda Endpoint Protection Plus, Panda Adaptive Defense and Panda Adaptive Defense 360, which manages vulnerabilities in operating systems and third-party applications on Windows endpoints and servers. It provides a reduced attack surface, strengthening preventive capabilities and incident containment.

- **WatchGuard Data Control** – is an add-on to Panda Adaptive Defense and Panda Adaptive Defense 360, which discovers, audits and monitors unstructured sensitive or personal data on endpoints, from data-at-rest to data-in-use and data-in-motion. It can also run real time, free custom searches to find files with specific content.

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

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

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

In addition, WatchGuard's **Orion** platform (formerly Cytomic), is a cloud based multi-tenant platform which provides incident detection, hunting, investigation and response for security operations teams. It helps to proactively identify threats that have passed other security controls, blocking and responding in the early stages of the Cyber Kill Chain. In addition, it centralizes real-time and 365-day retrospective visibility for hunting and IOC searches, and supports in-depth investigations and playbooks through a native integration of the Jupyter Notebooks paradigm.

STRENGTHS

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

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

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

- WatchGuard solutions are attractively priced.

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

WEAKNESSES

- WatchGuard currently supports centralized management of full volume encryption with BitLocker for Windows devices. However, support for Apple FileVault in still on the vendor's roadmap.

- WatchGuard does not yet offer XDR capabilities, which have become common with vendors in this space.

- WatchGuard currently only provides basic MDM capabilities for Android. However, support for iOS is expected for early 2022.

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

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

MICROSOFT

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

Microsoft provides a broad range of products and services for businesses and consumers, through a portfolio of solutions for office productivity, messaging, collaboration, and more.

SOLUTIONS

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

- **Microsoft Defender For Endpoint (MDE, formerly Microsoft Defender ATP)** – is a cloud-based endpoint security solution that includes risk-based vulnerability assessment and management, attack surface reduction, behavior-based next generation protection, EDR, automatic investigation and remediation, managed hunting, and unified security management. It is available in two plans: Plan 1 (currently in preview) aimed at E3 license customers, or as Plan 2 (generally available) for E5 license customers or E3 customers with a E5 security extension. It uses technology built into Windows 10 and Microsoft cloud services to provide:

- *Endpoint behavioral sensors* – sensors embedded in Windows 10, collect and process behavioral signals from the operating system and send sensor data to private, cloud instances of MDE.

- *Cloud security analytics* – leverages machine-learning across the across the entire Microsoft Windows ecosystem to deliver insight, detection, and recommended responses to advanced threats.

- *Threat intelligence* – leverages threat intelligence collected by Microsoft, security teams, and augmented by threat intelligence provided by partners, to enable Windows Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are detected.

- *Managed Detection and Response* – as part of Microsoft Defender for Endpoint, Microsoft also offers **Microsoft Threat Experts**, a managed detection and response (MDR) service which combines targeted attack notification with on-demand SOC expert services. It is available as part of the Microsoft 365 E5 subscription plan.

Microsoft Defender for Endpoint is also available for macOS, Linux, Android and iOS platforms, although feature parity is not available across all platforms.

Microsoft Defender for Endpoint can be managed from the **Microsoft Security Center** console, which provides a unified control point across the entire enterprise environment encompassing Intune, Azure ATP, Office 365 ATP, Azure Security Center, Microsoft Cloud App Security, and more.

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

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

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

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

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

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

- **Secure Boot** – helps ensure that a device boots using only trusted software.

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

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

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

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

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

- **Microsoft System Center Endpoint Protection (SCEP)** – is Microsoft's solution for anti-malware and endpoint protection for traditional endpoint devices (laptops, desktops and servers). It provides real-time, policy-based protection from malware, spyware and other threats. It also provides file cleaning, where infected files are replaced with clean versions downloaded from a Microsoft cloud location, as well as the ability to configure Windows Firewall settings. SCEP is designed for Windows client workstations and servers, and is

included at no additional cost as part of the Microsoft Enterprise Client Access License and Core CAL programs. Separate security applications, however, are required for Mac and Linux platforms.

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

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

STRENGTHS

- 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 EDR solution.

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

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

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 sometimes difficult for customers to understand exactly what security features are included with what plans.

- In order to obtain Microsoft's full range of security solutions, including the Microsoft Defender for Endpoint (MDE) EDR component, customers must upgrade to Windows 10 or later and sign up for the high-end Microsoft 365 E5 enterprise plans. Microsoft is addressing this by introducing a new, reduced functionality MDE Plan 1 aimed at E3 customers.

- 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 System Center does not offer granular device control for removable media, CD/DVDs, and other common devices.

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

TREND MICRO

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

Founded in 1988, Trend Micro provides security solutions for organizations, service providers, and consumers. Trend Micro's cloud-based Smart Protection Network brings together threat

reporting and analysis based on a worldwide threat assessment infrastructure. Trend Micro is publicly traded.

SOLUTIONS

Trend Micro **Smart Protection Suites** brings together endpoint security, server security, email security, and web security. The vendor's XGen Endpoint Security, combines machine learning and other techniques, in order to protect against ransomware and advanced attacks.

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

Apex One can integrate with additional components which include:

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

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

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

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

Endpoint Encryption – encrypts data stored on endpoints including PCs, Macs, DVDs, and USB drives. It is available as a separate agent which provides full-disk encryption, folder and file

encryption as well as removable media encryption. Endpoint encryption is only available as an on-premises component and as a separate agent from Apex One single agent.

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

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

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

- **Trend Micro Apex One with XDR** – which adds XDR to the Apex One SaaS security solution.

- **Trend Micro XDR for Users** – which adds email and cloud file sharing security for Microsoft 365 and Google G Suite to Trend Micro Apex One with XDR.

STRENGTHS

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

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

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

WEAKNESSES

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

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

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

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

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

- Mobile Security is a separate add-on.

BLACKBERRY

2240 University Avenue, East
Waterloo, Ontario
Canada N2L 3W8
www.blackberry.com

BlackBerry, founded in 1984, provides security software and services aimed at businesses, car makers and government agencies. BlackBerry leverages artificial intelligence and machine learning, from its 2019 acquisition of Cylance, to deliver technology and services that offer protection against advanced threats. BlackBerry Limited is a publicly traded company.

SOLUTIONS

BlackBerry Unified Endpoint Security (UES) applies artificial intelligence and machine learning to deliver pre-execution threat prevention and automated detection and remediation against cyberattacks. BlackBerry UES comprises the following products:

- **BlackBerry Protect** – is the prevention-focused component, which delivers malware prevention powered by artificial intelligence, combined with application and script control, memory protection, and device policy enforcement to prevent cyberattacks. The solution delivers protection against malware, ransomware, file-less malware, malicious scripts, weaponized docs, and other attack vectors, without relying on signatures or streaming data to the cloud. Protect supports Windows (32bit or 64bit), macOS, and Linux environments. It is available as a cloud deployment, on-premises (as a virtual appliance), or as a hybrid deployment. It provides:

  - *Malware Execution Control* – rejects potentially unwanted programs, controls tools used in lateral movement, and more.

  - *Device Control* – provides control over the use of USB devices and prevents exfiltration of data through removable media.

  - *Applications Control* – offers device binary lockdown, prevents bad binaries, prevents modification of good binaries, and more.
  - *Script Control* – stops unauthorized PowerShell and Active Scripts, stops risky Visual Basic for Applications (VBA) macro methods, weaponized documents, and file-less attacks.

  - *Memory Protection* – stops memory misuse and exploitation, halts process injection and more.

- **BlackBerry Optics** – is the endpoint detection and response (EDR) component that enables easy root cause analysis, threat hunting and automated threat detection and response. It augments Protect's prevention capabilities without requiring organizations to make significant investments in on-premises infrastructure, stream data to the cloud continuously, or employ highly skilled security resources. It helps organizations automate threat detection and response tasks using existing resources, reducing the workload on security analysts. It also supports Remote Forensic Data Collection, to retrieve advanced sets of forensic data from endpoints, as well as execute scripts, or applications to capture critical information related to suspicious events or security incidents.

- **BlackBerry Persona** – is BlackBerry's endpoint user and entity behavior analytics (UEBA) solution, which reduces insider threats, stolen credentials and physical compromises by

providing continuous authentication and user behavior analytics to identify suspicious and malicious users in real-time.

- **BlackBerry Guard** – is a 24x7 Managed Detect and Response (MDR) offering which provides proactive threat hunting and actionable intelligence. It provides access to BlackBerry analysts to help investigate incidents, delivers regular updates on overall threat prevention status, and helps initiate actions in response to indicators of compromise (IOC).

- **BlackBerry Gateway** – is BlackBerry's Zero Trust Network Access (ZTNA) solution which protects systems and data while providing easy access, scalable VPN access to SaaS and on-premises applications.

BlackBerry also offers **BlackBerry Spark Suite** which combines **BlackBerry UES**, for endpoint protection, with **BlackBerry UEM**, for unified endpoint management (UEM), to deliver an integrated endpoint security and endpoint management solution.
BlackBerry also offers managed services to provide enterprises with pre-attack penetration and vulnerability testing, compromise assessments, and post-attack incident response.

STRENGTHS

- BlackBerry is a cloud-based security provider, however, all client data is stored locally removing the need for an always-on cloud connection. The vendor also supports on-premises and hybrid deployment options.

- BlackBerry Protect has a small and lightweight footprint compared to other security products.

- BlackBerry Optics is highly intuitive and does not require additional hardware or continuous streaming of data to the cloud, making it one of the more lightweight EDR solutions on the market. It is designed to detect threats and take responsive action, without human intervention.

- All BlackBerry products are managed through a single dashboard.

WEAKNESSES

- Customers we spoke with as part of this research, indicated a high degree of false positives.
- BlackBerry Optics can do patch assessment, however, it is not an automated process.
- BlackBerry Spark UES Suite offers basic DLP capabilities. Capabilities such as firewall are only available through partners.
- BlackBerry should make it easier for customers of its UES and UEM solutions to integrate with third party solutions (e.g. for SIEM and other forensic activities).
- BlackBerry has lost some mindshare in the endpoint security space since nearly all traditional endpoint protection vendors have now added the advanced next-generation capabilities which were once key differentiators of the Cylance solution.

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. In 2020, CrowdStrike acquired Preempt Security, a provider of zero trust and conditional access technology, and in 2021 it acquired Humio, a log management platform. CrowdStrike is publicly traded.

SOLUTIONS

CrowdStrike **Falcon Endpoint Protection** is a cloud-based endpoint protection solution which combines next-generation antivirus, endpoint detection and response (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 X* – is CrowdStrike's global threat feed providing customized reports and analysis to help predict and prevent zero-day attacks.

- *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 Insight* – is CrowdStrike's endpoint detection and response (EDR) solution. It relies on the CrowdStrike Threat Graph, an advanced graph data model, which collects and inspects event information in real time. It helps understand endpoint security posture and take recommended action.

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

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

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

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

Falcon Endpoint Protection is available in four bundles:

- **Falcon Pro** – includes Falcon Prevent. Falcon X, Falcon Device Control, and Falcon Firewall Management are optional add-ons.

- **Falcon Enterprise** – which includes Falcon Prevent, and Falcon Insight. Falcon X, Falcon Device Control, Falcon Firewall Management and Falcon OverWatch are optional add-ons.

- **Falcon Premium** – which offers all the protection of Enterprise, and adds Falcon Discover.

- **Falcon Complete** – offers fully managed endpoint protection as a service, powered by CrowdStrike experts and backed by a breach warranty guarantee of up to $1 million.

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

STRENGTHS

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

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

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

WEAKNESSES

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

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

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

- CrowdStrike is losing some mindshare, as almost all competing endpoint protection vendors have added advanced EDR/XDR, ATP and MDR capabilities.

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

VMWARE CARBON BLACK

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

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

SOLUTIONS

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

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

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

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

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

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

STRENGTHS

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

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

- VMware Carbon Black allows customers to choose which product modules are right for their organization. All modules are easily deployed through the same user interface and agent.

- VMware Carbon Black Cloud offers an extensible architecture based on open APIs, which allows partners and customers to easily extend and integrate with existing security components.

WEAKNESSES

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

- VMware Carbon Black Cloud does not provide device control.

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

- VMware Carbon Black has lost some mindshare following the VMware acquisition. The vendor is working to address this.

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**
- **Compliance**
- **Instant Messaging**
- **Unified Communications**
- **Mobility**
- **Web Technologies**

The company assists vendors to define their strategic product and business direction. It also assists corporate organizations in selecting the right products and technologies to support their business needs.

Our market research and industry analysis takes a global perspective, providing clients with valuable information necessary to compete on a global basis. We are an international firm with clients throughout the US, Europe and the Pacific Rim. The Radicati Group, Inc. was founded in 1993.

Consulting Services:

The Radicati Group, Inc. provides the following Consulting Services:

- Management Consulting
- Whitepapers
- Strategic Business Planning
- Product Selection Advice
- TCO/ROI Analysis
- Multi-Client Studies

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

MARKET RESEARCH PUBLICATIONS

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

Currently Released:

Title	Released	Price*
Microsoft SharePoint Market Analysis, 2021-2025	May 2021	$3,000.00
Email Market, 2021-2025	Apr. 2021	$3,000.00
Microsoft Office 365, Exchange and Outlook Market Analysis, 2021-2025	Apr. 2021	$3,000.00
Cloud Business Email Market, 2021-2025	Apr. 2021	$3,000.00
Corporate Web Security Market, 2021-2025	Apr. 2021	$3,000.00
APT Protection Market, 2021-2025	Apr. 2021	$3,000.00
Information Archiving Market, 2021-2025	Mar. 2021	$3,000.00
Email Statistics Report, 2021-2025	Feb. 2021	$3,000.00
Instant Messaging Statistics Report, 2021-2025	Feb. 2021	$3,000.00
Social Networking Statistics Report, 2021-2025	Jan. 2021	$3,000.00
Mobile Statistics Report, 2021-2025	Jan. 2021	$3,000.00
Endpoint Security Market, 2020-2024	Nov. 2020	$3,000.00
Secure Email Gateway Market, 2020-2024	Nov. 2020	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Secure Email Gateways Market, 2021-2025	Dec. 2021	$3,000.00
Endpoint Security Market, 2021-2025	Dec. 2021	$3,000.00
Enterprise DLP Market, 2021-2025	Dec. 2021	$3,000.00

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

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

