The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Endpoint Security - Market Quadrant 2019

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

October 2019

TABLE OF CONTENTS

==========

==========

RADICATI MARKET QUADRANTS EXPLAINED

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

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

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

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

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

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

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

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

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

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

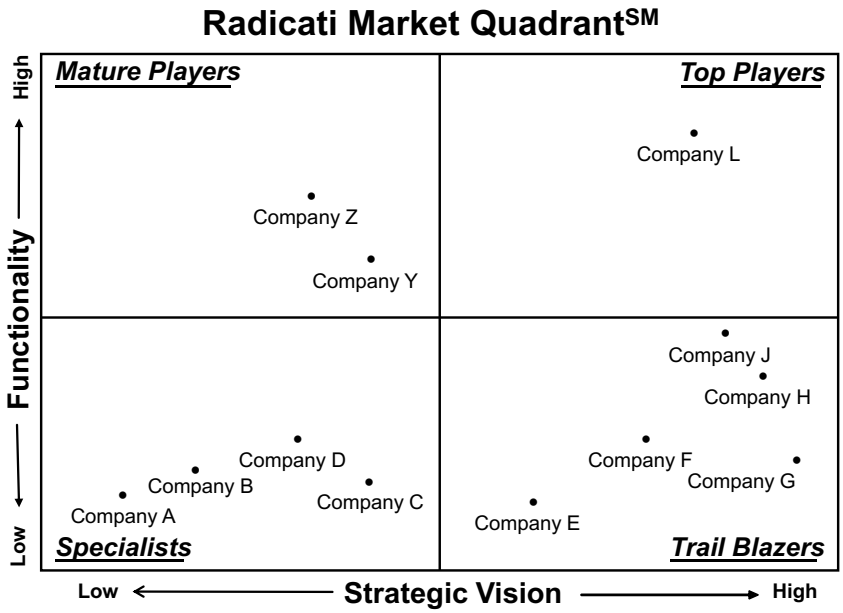

Figure 1: Sample Radicati Market Quadrant

INCLUSION CRITERIA

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

MARKET SEGMENTATION – ENDPOINT SECURITY

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

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

- 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 now offer behavior-oriented solutions which include endpoint detection and response (EDR), sandboxing, advanced persistent threat (APT) protection, managed detection and response (MDR), and more.

- Organizations of all sizes, 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 see strong growth as organizations of all sizes continue to invest in more sophisticated and feature-rich solutions to help protect against a multitude of threats and malicious attacks. The Endpoint Security market is expected to surpass $7.1 billion in 2019, and grow to over $13.3 billion by 2023. Figure 1, shows the projected revenue growth from 2019 to 2023.

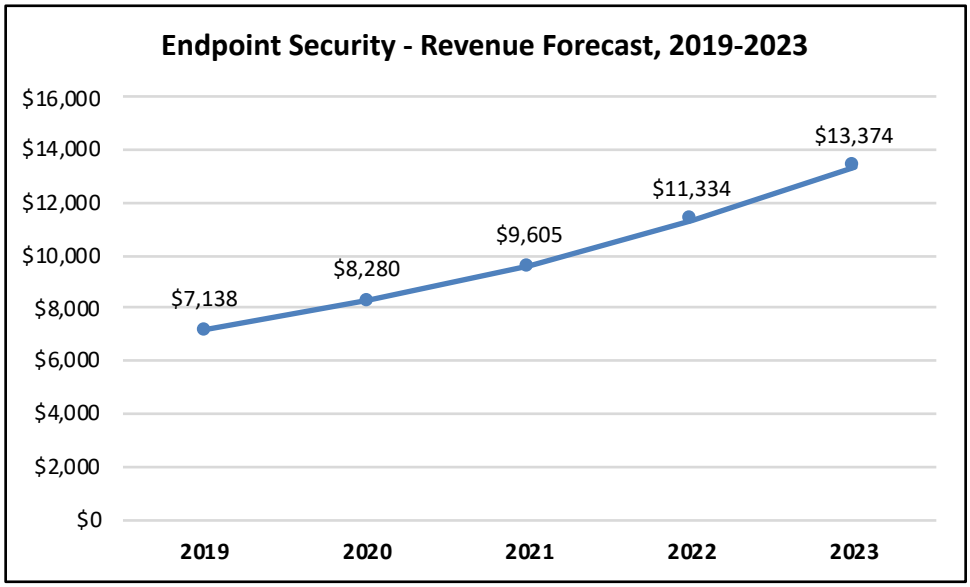

Figure 2: Endpoint Security Market Revenue Forecast, 2019-2023

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.

- ***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.

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

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

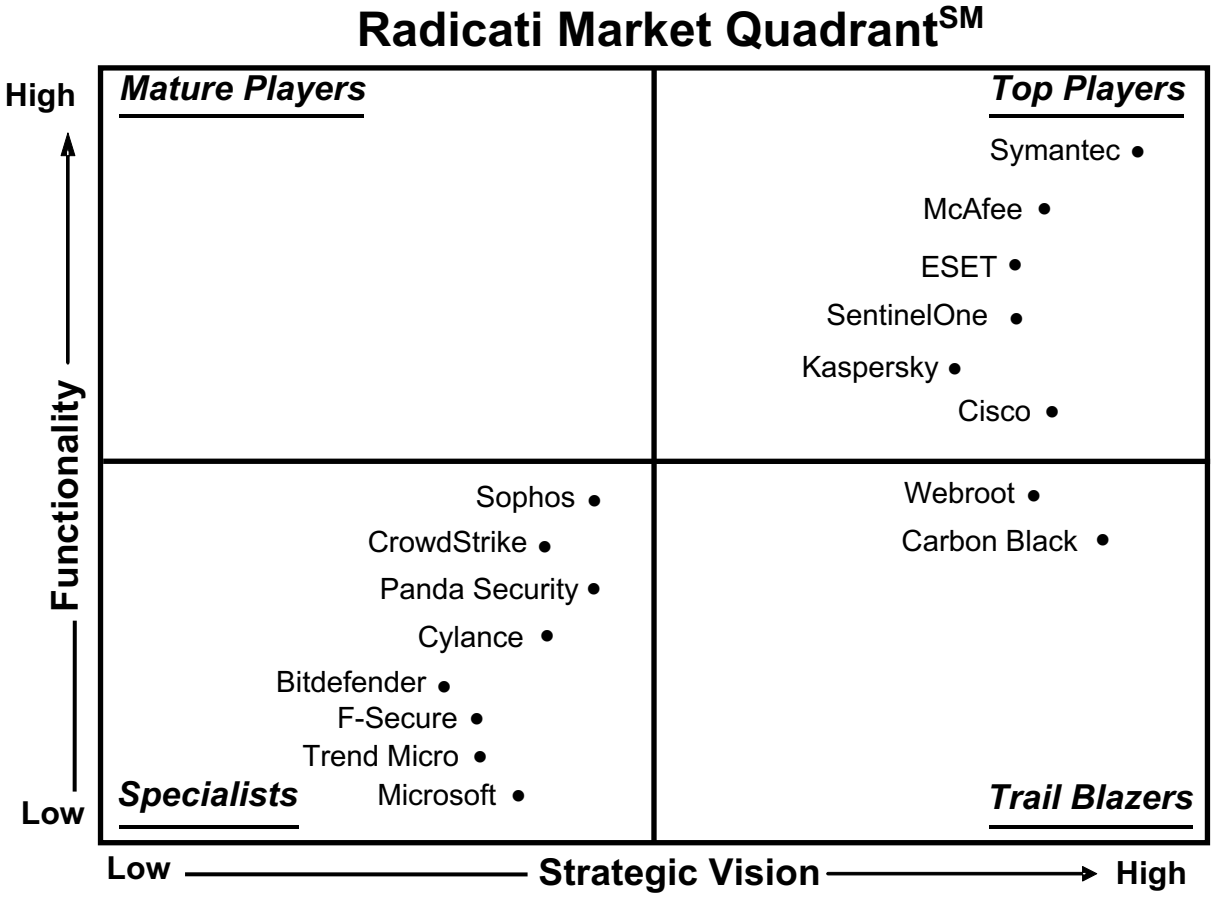

Figure 3: Endpoint Security Market Quadrant, 2019*

* Radicati Market Quadrant℠ is copyrighted October 2019 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 *Symantec, McAfee, ESET, SentinelOne, Kaspersky,* and *Cisco.*

- The **Trail Blazers** quadrant includes *Webroot,* and *Carbon Black.*

- The **Specialists** in this market are *Sophos*, *CrowdStrike, Panda Security, Cylance, Bitdefender, F-Secure, Trend Micro,* and *Microsoft.*

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

ENDPOINT SECURITY - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Symantec offers a wide range of security solutions for enterprises and consumers. Symantec operates one of the largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. In August 2019, Broadcom announced the acquisition of Symantec's enterprise security business.

SOLUTIONS

Symantec's security solutions are powered by the Symantec Global Intelligence Network that offers real-time updates. Symantec offers the following endpoint protection solutions:

- **Symantec Endpoint Security –** supports on-premises, cloud, and hybrid management, through a fully cloud managed option, which delivers artificial intelligence-guided security management, endpoint detection and response, protections against Active Directory exploits, smart application isolation and application control, and extended operating system

protections. It is compatible with the latest versions of Windows, macOS, Linux, Android, iOS, VMware ESX, Citrix XenServer, and other virtual machines. It combines malware protection, advanced machine learning, behavioral analysis, reputation filtering, exploit 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 is managed from a centralized console, which supports the definition of granular management policies.

- **Symantec Endpoint Protection Cloud (SEP Cloud)** – is an easy-to-use endpoint security solution designed for small and mid-size companies with limited security expertise. It delivers threat protection for traditional endpoints (Windows, macOS), mobile endpoints (iOS, Android), and Windows servers from a single cloud-managed console. While the core security technologies for traditional endpoints remain the same as in Symantec Endpoint Security, some functionality deemed less relevant to small and mid-sized customers has been removed, such as granular policy settings, device and application control, and Linux OS support.

- **Symantec Endpoint Protection Mobile (SEP Mobile)** – is advanced mobile threat defense for iOS and Android devices, also included in Symantec Endpoint Security. It uses predictive technology in a layered approach that leverages crowd-sourced threat intelligence, in addition to both device- and server-based analysis, to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits, with or without an Internet connection. Symantec has recently added integrations with its Web Security Service (WSS) and CloudSOC solutions to extend the capabilities of those solutions to mobile devices. It also integrates with Symantec Validation and ID Protection (VIP) to ensure multifactor authentication codes are only provided on low-risk devices.

- **Symantec Endpoint Detection and Response (EDR)** – enables visibility into a file's static file attributes (e.g. keylogging functionality, UI window, and more) and its full behavioral process trace (e.g. detection of fileless attack, PowerShell, Memory Exploit Mitigation, and more). Event details from the endpoint security client are analyzed for suspicious activities and prioritized incidents are created. The solution is integrated with an advanced cloud sandbox which can detect VM-aware malware and perform detonation on physical servers as needed. Remediation capabilities include endpoint quarantine, blacklisting and malware deletion to bring the endpoint back to the pre-infection state. Correlation with network and email events provides unified visibility and response across all threat vectors. Symantec EDR

supports searching for evidence or indicators of compromise (IOC's) on endpoint devices. EDR leverages the same Symantec endpoint agent, and does not require a separate agent.

- **Symantec Endpoint Application Isolation** – is an advanced protection add-on product to Symantec Endpoint Security using the same, single endpoint agent. It discovers applications running on endpoints and classifies apps (and their respective vulnerabilities) based on risk levels. It isolates suspicious applications to prevent them from executing privileged operations (e.g. changing the registry, downloading executables, and more) and it shields the vulnerabilities in commonly used applications (e.g. Browsers, Microsoft Office, Adobe) to prevent cyber attackers from exploiting them.

- **Symantec Endpoint Application Control** – is also an advanced protection add-on to Symantec Endpoint Security which uses the same, single endpoint agent. It discovers applications running on endpoints and classifies apps (and their respective vulnerabilities) based on risk levels. It generates smart allow and block lists to prevent unauthorized applications from running. The parameters used include reputation, certificates, publishers, hash, and more). In addition, Application Control offers a simple workflow to manage drift by addressing new applications and handling exceptions.

- **Symantec Endpoint Threat Defense for Active Directory** – protects Active Directory environments from malicious use by attackers. It automatically learns an organization's entire Active Directory structure and creates an obfuscation to prevent attackers from stealing credentials and move laterally in the organization.

STRENGTHS

- Symantec offers a single management console across Windows, macOS, Linux, Embedded and Virtual machines, as well as a single integrated agent on the endpoint for seamless management and performance. Hybrid management options (on-premises and cloud) offer additional flexibility to customers.

- 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, application isolation, and application control.

- The level of granularity and flexibility in the management console is higher than many other 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.

- The level of integration with the Symantec product portfolio (web and email security gateways, threat analytics, multifactor authentication and more) and third-party solutions (e.g. orchestration, automation, SIEM, and others) is higher than most other solutions on the market.

- Symantec Endpoint Security has built-in Endpoint Detection and Response (EDR) capabilities. In addition, Symantec offers Managed EDR, with 24x7 triage, incident response, proactive threat hunting and containment response.

- Given the rich functionality of Symantec's endpoint security platform, it is priced very competitively.

WEAKNESSES

- The Endpoint management (ITMS), powered by Altiris, is available primarily as an on-premise managed solution currently, and only some features like vulnerability remediation are available on the cloud console.

- DLP capabilities require a separate add-on.

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

MCAFEE

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

McAfee is the device-to-cloud cybersecurity company, which delivers solutions for businesses and consumers. Its business solutions are based on a holistic, automated open security platform which provides orchestrated security to protect the entire infrastructure, including endpoints, network, web, mobile, IoT devices, and cloud. The company is privately held.

SOLUTIONS

McAfee Endpoint Security uses advanced defenses like machine learning analysis, analytics for fileless 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'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, the company's endpoint protection platform (EPP), as well as with third-party EPPs. McAfee offers an open security platform that allows multiple McAfee and third-party products to co-exist and share threat intelligence. All security solutions are managed through ePolicy Orchestrator (ePO), which is available as an on-premise, virtual, or SaaS-based solution which provides a single management system for centralized visibility across multiple security products and the entire threat defense lifecycle. McAfee endpoint protection solutions protect Windows, Macs, and Linux systems, as well as iOS and Android mobile devices.
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 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), and machine learning analysis to provide full-stack protection for Windows, macOS, and Linux systems. 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.

STRENGTHS

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

- 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 fileless-based attacks.

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

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

WEAKNESSES

- Full DLP capabilities are only offered as a separate add-on.

- McAfee solutions are a bit pricier than offerings from competing vendors, but typically offer more features and functionality.

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

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. It offers device control, anti-phishing technology and additional capabilities, such as firewall, web control, botnet protection and more.

- **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. It offers integrated device control and anti-phishing with additional capabilities, such as firewall, web control, and more.

- **ESET Endpoint Security for Android –** offers reputation-based malware protection, anti-phishing, app control, anti-theft, SMS/call filtering and device security.

- **ESET Mobile Device Management for iOS** – is an integration of the Apple iOS MDM framework with ESET Security Management Center 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 File 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. It pays special attention to ensure that servers are stable and conflict-free to keep maintenance and restarts to a minimum.

- **ESET Mail Security for Microsoft Exchange Server** – combines server malware protection, spam filtering and email scanning. 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), new proprietary antispam engine, and selective database on-demand scanning. It features native local quarantine management, process exclusions, support for virtualization (e.g. optional snapshot independence, hybrid Office365 scanning, clustering support) and a Windows Management Instrumentation (WMI) connector.

- **ESET Virtualization Security for VMware** – is an agentless scanning solution for VMware environments. It streamlines the protection of all virtual machines on the same host by automatically connecting to the vShield and NSX appliance. It can be managed using the ESET Security Management Center.

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

- **ESET Security Management Center** – is a web-based single pane of glass multi-tenant management console for all ESET business security products. It can be installed on Windows, Linux or as a Virtual Appliance in Microsoft Azure. It supports Mobile Device Management (MDM) for Android and iOS devices. ESMC allows single click incident remediation, features a customizable notification system, automated VDI support and comes with over 170 built-in reports, as well as the ability to create custom reports.

In addition, ESET provides the following services and solutions:

- **ESET Enterprise Inspector** – is ESET's EDR solution. It combines ESET's detection and protection technologies, threat intelligence and cloud malware protection system with other advanced techniques to monitor and evaluate suspicious processes and behaviors. It can detect policy violations, anomalies, and can provide detailed information and response options in the event of security incidents. It provides multiple options to respond to incidents or suspicious activities.

- **ESET Dynamic Threat Defense (EDTD)** – is ESET's managed cloud sandboxing solution, which provides another layer of protection for ESET Endpoint and Server security solutions. It provides static and dynamic analysis and reputation data, to detect zero-day threats. It is managed by the ESET Security Management Center and integrates directly with ESET Enterprise Inspector, ESET Mail Security solutions and ESET Endpoint solutions.

- **ESET's Threat Intelligence Service** – is ESET's threat reputation network. It uses information gathered from over 110 million sensors that is sent to ESET's Cloud Malware Protection System via ESET LiveGrid®. It shares actionable threat intelligence with customers. Additionally, it provides IOCs (IP, URL, file hash) and serves as an automated malware analysis portal.

- **ESET Threat Hunting** – is a security service delivered by ESET cybersecurity experts who perform an on-demand investigation of data, events and alarms generated by the ESET Enterprise Inspector. This may include root cause analysis, forensic investigations, as well as actionable mitigation advice.

- **ESET Threat Monitoring** – is a security service delivered by ESET cybersecurity experts who continuously monitor customer network and endpoint security data to provide alerts in real time if suspicious activity requires attention. It also provides actionable advice on risk mitigation.

- **ESET Manual Malware Analysis** – is an ESET security service which provides full examination and reverse engineering of submitted files. It also provides detailed reports on malicious code behavior with recommendations for prevention, removal and mitigation of attack impact.

- **Forensic Analysis & Consulting** – is a service which provides manual examination of submitted hardware and investigation by ESET Malware Research experts to provide mitigation suggestions and minimize breach aftermath.

- **ESET Initial Assessment and Optimization** – is a service designed for customers utilizing ESET's Enterprise Inspector (EEI) EDR solution, which further improves protection and detection capabilities based on an initial assessment which results in the optimization of settings, rules and exclusions specifically tailored to a customer's environment.

- **ESET Cloud Administrator** – is a cloud-based console, offered as a service, for the remote management of customer networks of up to 250 seats.

- **ESET Secure Authentication** – is a mobile-based multi-factor authentication (MFA) solution that protects organizations from weak passwords and unauthorized access. It provides support for iOS, and Android.

STRENGTHS

- ESET Endpoint Security solutions are generally 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 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 products are deployed on-premises. However, the cloud-based administration is available through two solutions: ESET Security Management Center, available as a virtual machine in Windows Azure or as virtual appliances; and ESET Cloud Administrator, for remote management of organizations with up to 250 seats. A cloud-based management console for larger enterprise customers is on the vendor's roadmap.

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

- The ESET Endpoint Security for macOS does not currently integrate with its ESET Enterprise Inspector, EDR solution. The vendor is working to address this in future releases.

- ESET endpoint solutions are licensed by device, whereas most competitors now license by user (making it easier for users to deploy on multiple devices).

- ESET still lacks market visibility, particularly in North America. The vendor is working to address this.

SENTINELONE

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

SentinelOne, founded in 2013, develops software to secure endpoint devices and provide forensics to understand targeted attacks. SentinelOne delivers autonomous endpoint protection through a single agent that prevents, detects, and responds to attacks across all major threat vectors. SentinelOne is privately held.

SOLUTIONS

The **SentinelOne Endpoint Protection Platform (EPP)** is a fully converged Endpoint Protection Platform (EPP) and Endpoint Detection & Response (EDR) offering in a single agent, which autonomously prevents, detects, and responds to threats in real-time for both on-premises and cloud environments. The SentinelOne platform protects against all threat vectors pre-execution, on-execution and post-execution, and since it is powered by AI and machine learning, it does not require any prior knowledge of an attack to detect and remediate. SentinelOne's endpoint protection capabilities are integrated with its EDR capabilities, in the same agent and codebase. This delivers an integrated, automated approach which meets the needs of large enterprises and SMBs for threat protection and response capabilities in a simple, automated fashion. SentinelOne can be used as a standalone solution on an endpoint or run beside other legacy or next-generation AV engines.

SentinelOne supports cloud (including SaaS or PaaS), on-premises or hybrid deployments. It supports all leading platforms, including Windows, macOS, Linux, all leading virtualization platforms, as well as leading container platforms, such as Docker and Kubernetes.

SentinelOne provides the following capabilities:

- *Malware prevention and detection* – SentinelOne uses proprietary static and behavioral AI engines to prevent, detect, and automatically respond to malware and advanced threats including true unknown zero days, ram only malware, and others. The engines work when the agent is online or offline.

- *Directory integration* – SentinelOne automatically integrates with Active Directory for dynamic grouping of agents. It also leverages SAML v2 for administrative logins.

- *Firewall integration* – The SentinelOne behavioral AI functions much like a next-generation HIPS, it monitors network traffic and how that traffic interacts with processes on the endpoint. If malicious behavior is observed, the agent can take action in real time to kill and mitigate the threat. SentinelOne also has integration with the native firewalls on Windows, macOS, and Linux to allow for custom blocking rules via policies.

- *Device Control* - SentinelOne provided USB and Bluetooth device control on Windows and macOS. This works on all supported OS and hardware types including Virtual Machines.

- *Encrypted traffic and URL detection* – SentinelOne provides visibility into encrypted TLS traffic without certificates or proxies. It provides full threat hunting visibility of encrypted traffic directly from the endpoint, with no need to decrypt and re-encrypt traffic as it travels across the network. SentinelOne also monitors all URLs (including TLS / SSL ones) in use on all endpoints in real time and can autonomously kill and mitigate any detected threat.

- *Sandboxing* – The SentinelOne behavior engine provides all the functionality of a sandbox in real time on the endpoint. SentinelOne also provides integrations into on-premises and cloud based sandboxes, such as FireEye and Wildfire.

- *Patch assessment* – the SentinelOne agents keep real-time inventory of all software installed on all managed agents including install path, version, and patch level. The admin can run a report to compare the software inventory to known vulnerabilities as published by MITRE.

- *Web and email security* – SentinelOne monitors all paths that web or email could use to launch an attack via its Behavioral Engine.

- *Mobile security* – SentinelOne partners with Lookout Security to offer mobile security, as an add-on component at an extra charge. The solution is seamlessly integrated into the SentinelOne management console.

- *Reporting* – the SentinelOne Reporting engine can be customized to return reports in a dynamic fashion. The management server also supports access to all data via API, and publishes an EXCEL plugin for further customized reporting.

- *Alerts* – when a new threat is detected, endpoints are autonomously able to notify other agents, so that all other endpoint devices become immune to the threat.

- *Remediation* – SentinelOne provides one-click automated on-device threat remediation, which can forensically remove any malware that the behavioral AI sees without end user impact. The agent can also see inside TLS and SSL traffic without certificates or network changes. SentinelOne offers the same level of efficacy regardless of whether the agent is online or offline.

SentinelOne also offers more than 350 APIs that enable its partners and end customers to seamlessly integrate and unify security and IT assets within their existing architectures.

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 improve in-product workflows, as well as the quality of integration with partner technology solutions. The vendor is working to address this in future releases.

- 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 partners with Lookout Security for mobile security capabilities, however this is provided as an extra cost option.

- SentinelOne does not currently offer content-aware Data Loss Prevention, however, the vendor is considering adding this in the future.

KASPERSKY

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

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

SOLUTIONS

Kaspersky offers Endpoint Security with built-in Automated Endpoint Detection & Response (Automated EDR), which leverages Machine Learning (ML) techniques to complement and enhance security efficiency levels while combating threats.

Kaspersky Endpoint Security for Business (KESB) is a multi-layered endpoint protection platform, which delivers a broad array of capabilities and technologies to enable companies to see, control and protect all endpoint devices. It provides comprehensive security, visibility and manageability of all endpoints, including physical and virtual machines, mobile devices, and file servers. Kaspersky offers support for a broad array of platforms, which include Windows, Linux, macOS, Android, and iOS.

Kaspersky Endpoint Security for Business is available in three different tiers, each of which adds its own layer of protection against cyber-threats, as follows:

- *Select* – provides Next Generation 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, it adds Application Control for servers, Automated EDR with Adaptive Anomaly Control, Data Protection (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, it protects enterprise perimeter including Email and Web Traffic.

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 also be deployed on public cloud or hosted environments and accessed through a web-interface.

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

Kaspersky Endpoint Security Cloud is a cloud-based endpoint security solution, aimed at small and medium-sized businesses, as well as MSP partners. It offers a cloud-based management solution for securing Windows and macOS endpoints, file servers, iOS and Android devices. It integrates with Remote Monitoring and Management (RMM) and Professional Services Automation (PSA) systems from ConnectWise, Automate, Autotask, Tigerpaw and SolarWinds.

In addition, **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.

Kaspersky Endpoint Security can be extended with **Kaspersky Security for Microsoft Office 365**, and with **Kaspersky Web Traffic Security**, providing corporate IT network protection at a web gateway level.

Kaspersky Sandbox is tightly integrated with KESB, to provide automated detection and prevention of previously unknown malware, new viruses and ransomware, zero-day exploits, and others.

Kaspersky Endpoint Security solutions provide a multi-layered protection approach which includes:

- *Exposure reduction* – with web and email traffic filtering through white and black-listing, as well as rapid cloud lookups.

- *Pre-execution prevention* – endpoint hardening (with patch management and application control), and heuristic analysis based on emulator and machine learning technologies.

- *Automated EDR* – including behavior detection, exploit protection, adaptive anomaly control, automatic rollback, malicious action blocker for shared folders, fileless threat protection, host-based intrusion prevention (HIPS), and reputation services.

- *Endpoint forensics data collection* – event logging with active malware disinfection.

- *Automated Sandbox* – complements Endpoint Security with advanced emulation, shared verdict cache and automated response scenarios.

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

STRENGTHS

- All Kaspersky solutions leverage the Kaspersky Security Network, a real-time intelligence network that collects tens of millions of threat samples daily on a worldwide basis to ensure accurate, up-to-date protection.

- Kaspersky Endpoint Security adapts to any IT environment and 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 solutions rely on its own low footprint, high-performance security technologies. Behavior Detection technology implements a Memory Protection mechanism, which guards system-critical processes and prevents leaking user and administrator credentials.

- Kaspersky supports an Adaptive Anomaly Control approach which collects statistics about triggered control rules to create a normal activity model for users, and then activate only rules that block what appears to be anomalous behavior.

- On premises or cloud-hosted Kaspersky Security Center management console 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, provide a real-time hardware and software inventory, and offer actionable administrator reporting.

- Through the use of Dynamic Whitelisting, Application Control reduces exposure to zero-day attacks by providing control over what software is allowed to run on desktops and servers.

- 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's Endpoint Security Cloud, is currently aimed only at small-medium businesses (with less than 1,000 users), and MSPs.

- While Kaspersky Endpoint Security for Business is available for macOS, Linux, and Windows platforms, full feature parity is not always available so customers should check carefully what features are provided on each platform.

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

- 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).

- 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.

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 Security Intelligence and Research Group (Talos), made up of leading threat researchers.

SOLUTIONS

Cisco Advanced Malware Protection (AMP) for Endpoints is a cloud-based endpoint security solution designed to detect, prevent, and remediate advanced threats. It provides a holistic view of servers and endpoints running Windows, Mac, Android, iOS, Linux (CentOS and RedHat), as well as virtual systems. It is available through a public or on-premise private cloud deployment.

AMP for Endpoints comprises the following key capabilities:

- *Malware Prevention* – is provided through a combination of technologies including file reputation, traditional anti-virus, cloud-based sandboxing, file-less in-memory exploit prevention, system process protection and behavior-based ransomware protection. Cisco AMP for Endpoints can automatically detect and block known and emerging threats through real time technologies that include: big data analytics, machine-learning, and fuzzy fingerprinting. Malicious verdicts from the detonation of unknown files in the sandbox are automatically added to the file reputation in the AMP's collective threat intelligence cloud and can close attack pathways across the AMP Ecosystem of security control points. File analysis reports provide detailed behavioral indicators of compromise with mappings to applicable MITRE ATT&CK framework. Cisco's Talos Security Intelligence and Research group further augments this threat intelligence dynamically through the cloud or content updates to the various engines.

- *Malware Detection* – AMP for Endpoints 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, AMP for Endpoints captures all command line activity on the endpoint and is able to analyze command line arguments associations with malicious file

attributes, file and network activity. This helps scale detections from a single file conviction to multiple file convictions using analytics through telemetry from other Cisco security products, not just endpoint. If malicious behavior is detected, it can automatically block the file across all endpoints and the AMP Ecosystem of security control points, and provide security teams with a recorded history of the malware's behavior and trajectory.

- *Malware Response* – AMP for Endpoints provides a suite of response capabilities to contain and eliminate threats across all endpoints. Administrators can search across endpoints using a simple, web-browser based management console using OpenIOC queries for known indicators of compromise and/or more advanced live searches of endpoint telemetry using osquery. A Cisco-curated catalog of queries mapped to the MITRE ATT&CK TTP detection is provided for ease of use, including the ability to query for an endpoint forensic snapshot. If a threat is detected, AMP automatically contains and remediates across all endpoints including PCs, Macs, Linux, and mobile devices (Android and iOS).

- *Email and Web security* – all file disposition and dynamic analysis information is shared across the AMP Ecosystem via collective intelligence. If a file is determined to be malicious via AMP for Email or Web Security, that information is shared across all AMP platforms, both for future detection as well as retrospectively if the file was encountered by any of the other AMP platforms; including Endpoint. Native integration between AMP for Endpoints and the AMP Ecosystem provides global outbreak control, threat context enrichment and global trajectory view of malware ingress across key attack vectors. AMP for Endpoints also inspects web proxy logs from a compatible web proxy, and allows administrators to uncover file-less or memory-only malware, see infections that live only in a web browser, catch malware before it compromises the OS-level, and get visibility into devices that don't have the AMP for Endpoints connector installed.

- *Firewall* – AMP for Endpoints integrates with AMP for Networks. All detection information is sent to the Firepower management platform and can be used to correlate against other network threat activity. Native integration between AMP for Endpoints and the AMP Ecosystem provides global outbreak control, threat context enrichment and global trajectory of malware traversal on the network. Firepower and Cisco Identity Services Engine (ISE) can be tightly integrated, which allows AMP for Endpoint events to trigger policy responses and enforcement in ISE.

- *Patch Assessment* – AMP for Endpoints uses a feature called Vulnerable Software that identifies if the installed software is up to date according to the vendor, or if the installed version has an exploitable vulnerability. Additionally, the advanced live search in AMP for Endpoints using osquery provides cataloged queries to identify Windows hotfixes and/or patch levels of the endpoint.

- *Reporting* – AMP for Endpoints 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* – AMP for Endpoints comes with its own management console and can also integrate with the Firepower console (for Cisco NGIPS or Cisco Firewall deployments) for tighter management across all deployed Cisco security solutions.

- *Integrations* – AMP for Endpoints has an API that allows customers to sync AMP for Endpoints with other security tools or SIEMs. AMP for Endpoints is also part of Cisco's integrated security ecosystem that helps share and correlate information across endpoints, network IPS, firewalls, web and email gateways, and more.

Cisco AnyConnect Secure Mobility Client offers VPN access through Secure Sockets Layer (SSL), endpoint posture enforcement and integration with Cisco Web Security for comprehensive secure mobility. It assists with the deployment of AMP for Endpoints, 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 to prevent threats from entering the endpoint. Cisco has also integrated unified access security and multi-factor authentication capabilities from its Duo Security acquisition.

- Cisco AMP for Endpoints delivers Endpoint Protection and Endpoint Detection and Response capabilities in a single agent.

- Cisco AMP for Endpoint threat response delivers automatic threat context enrichment and unified threat response capabilities across the AMP Ecosystem, including Endpoints, Network, Email, DNS, and more.

- AMP for Endpoints is a unified agent for security services, which provides remote access functionality, posture enforcement, and web security features.

- AMP for Endpoints offers rich native integrations to Cisco NGFW/NGIPS, Email Security, Umbrella DNS Security other Cisco security solutions to provide a thorough network edge to endpoint visibility.

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

- Customers report that AMP for Endpoints is easy to use, and highly efficient in dealing with prevention and remediation.

WEAKNESSES

- Cisco AMP for Endpoints does not provide features to help uninstall previous security software.

- Cisco AMP for Endpoints currently offers third party software patch assessment, but does not offer third party patch software remediation.

- Cisco AMP for Endpoints does not provide content-aware DLP functionality.

- Cisco AMP for Endpoints will appeal mostly to customers with complex endpoint protection needs, who are already vested in Cisco solutions.

TRAIL BLAZERS

WEBROOT

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

Webroot, a Carbonite company, delivers endpoint and network protection, security awareness training and threat intelligence services to businesses and consumers worldwide. In 2019, Webroot was acquired by Carbonite, an endpoint and server backup and recovery provider serving customers ranging from small businesses to enterprises.

SOLUTIONS

Webroot offers the Webroot suite of three SMB/MSP business security products for endpoint, internet DNS filtering and security awareness training. All are powered by the **Webroot Threat Intelligence Platform**, a security intelligence platform that continuously collects, analyzes and correlates security information, such as file behavior and reputation, URL and IP reputation, real-time anti-phishing, mobile app reputation and more.

- **Webroot Business Endpoint Protection** is a real-time, cloud-based approach to detecting and preventing malware. It is compatible with Microsoft Windows PCs, Laptops 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 features the following capabilities:

    - *Real-Time Anti-malware* – uses Webroot's correlated threat intelligence to perform continuous file and process analysis, and provides malware detection and prevention, in combination with a lightweight, high performance endpoint agent. By moving intensive malware discovery processing to the cloud, it significantly increases system performance and minimizes local endpoint resource usage and impact on user productivity. Webroot requires zero signatures or definition updating of the endpoint as the Webroot Threat Intelligence Platform makes collective file and process security intelligence instantly available to all customers in real time.

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

- *The Identity/Privacy Shield* – secures and isolates the browser (and any other application needed) from the rest of the endpoint. It protects both the user and device.

- *Web search results annotations and safety ratings* – are provided for the main search engines and share why a site was blocked and possible actions for the user.

- *Real-time anti-phishing* – is activated when a user clicks on an email link or attachment that tries to reach the internet. It then relies on machine learning models to determine if access needs to be blocked.

- *Outbound Firewall* – ensures that all outbound TCP/UDP requests and destinations are checked against the Webroot Threat Intelligence Platform so automatic decisions can be made on the users' behalf whether to block or allow the traffic. If a file or process is undetermined, the firewall monitors for data exfiltration.

- *Endpoint Restore and Remediation* – by closely monitoring unknown files and journaling any changes made, the endpoint can be restored to its last known good state.

- *Offline Protection* – uses separate file execution policies to stop attacks when endpoints are not connected to the internet. If an unknown file or process runs when the endpoint is offline, monitoring and journaling are automatically initiated. Upon reconnecting to the internet, any unknown or changed files are analyzed, and if found to be malicious, the endpoint is rolled back to its last known good state.

- *Device control* – using adjustable heuristics settings administrators can lock down common devices, such as USBs and DVDs.

- *Centralized remote management* – available via the Webroot web-based management console. Policies can be set for individual users, or groups of users.

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

- *Automation Ecosystem Integrations* – expanded integrations for MSPs include support for Remote Management and Monitoring (RMM) and Professional Services Automation (PSA) platforms.

- *Dwell Time* **–** Webroot reports and alerts on the dwell-time of infections and gives administrators high visibility into infections and details about infection type.

- *Windows 10 and ELAM Support* – Webroot supports Windows 10, and also covers Microsoft's Edge browser with web filtering and anti-Trojan protection (ID Shield). Webroot also recently added Early Launch Anti-Malware protection (ELAM).

- *Advanced Whitelisting* – offers flexibility in creating file overrides through an enhanced Whitelisting and Blacklisting interface that simplifies the management of application overrides.

- *Fully integrated customer support system* – Webroot offers integrated support within the management console, which makes complex support and ticket number referencing easy.

- *Global Management Dashboards* – offer full endpoint dashboard drill down capabilities, allowing administrators to respond to events and investigate anomalies or alerts on the dashboard.

- *Advanced Reporting* – a scheduled reporting engine provides administrators flexibility in generating reports based on their preferences. The Webroot Unity API can also be used to provide highly customized reporting.

- *Unity API* – allows for easy 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

- Webroot Business Endpoint Protection has a small installation footprint, since it doesn't require a local threat database.

- 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 can work with any browser.

- Management is fully cloud-based, which means there is no need for an on-premises management server.

- Webroot Business Endpoint Protection is easy to manage, and offers built-in automatic rollback and auto-remediation of infected endpoints.

- 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

- Webroot Business Endpoint Protection does not include encryption capabilities.

- Webroot Business Endpoint Protection does not provide DLP functionality or ICAP support for integration with third party DLP solutions.

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

- Webroot does not provide protection for mobile devices.

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

CARBON BLACK

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

Carbon Black is a developer of next-generation endpoint security. The company leverages its big data and analytics cloud platform, the CB Predictive Security Cloud, to enable customers to defend against advanced cyber threats, including malware, ransomware, and non-malware attacks. In August 2019, VMware announced its intent to acquire Carbon Black.

SOLUTIONS

CB Predictive Security Cloud is a next generation endpoint protection platform that consolidates security in the cloud, making it easy to prevent, investigate, remediate, and hunt for threats from a single endpoint agent, console, and data set. It offers the following modules which can be managed through the same user interface, with a single login:

- **CB Defense** – delivers next-generation antivirus (NGAV), and endpoint detection and response (EDR) functionality.

- **CB ThreatHunter** – is a threat hunting and incident response solution delivering unfiltered visibility for security operations center (SOC) and incident response (IR) teams. The CB Predictive Security Cloud captures and stores all OS events across every individual endpoint. Leveraging this unfiltered data, CB ThreatHunter provides immediate access to a complete picture of an attack at all times, reducing investigation time. CB ThreatHunter enables teams to proactively hunt for threats, as well as uncover suspicious and stealthy behavior, disrupt active attacks and address potential defense gaps. It allows organizations to respond and remediate in real-time, stopping active attacks and quickly repairing damage.

- **CB LiveOps** – is a real-time security operations solution that enables organizations to ask questions of all endpoints and take action to instantly remediate issues. It closes the gap between security analysis and IT operations by giving administrators visibility into precise details about the current state of all endpoints, enabling them to make fast decisions to reduce risk.

- **CB ThreatSight** – is a managed service for CB Defense that provides a team of Carbon

Black security experts who work side-by-side with customer organizations to help validate and prioritize alerts, uncover new threats, and accelerate investigations.

- **CB Defense for VMware** – is a cloud-delivered security solution for protecting applications deployed in virtualized data centers.

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

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

- Carbon Black 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.

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

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

WEAKNESSES

- Carbon Black Predictive Security Cloud does not currently offer some traditional endpoint protection functionality, such as firewalls, mobile security, or DLP. However, provision of a managed OS firewall is on the vendor's roadmap, and custom integrations are possible through the platform's open APIs.

- Carbon Black Predictive Security Cloud does not currently provide device control. This is on the vendor's roadmap.

- The Carbon Black Predictive Security Cloud platform does not yet provide application control capabilities. Carbon Black currently offers this through its on-premises application control product, CB Protection.

SPECIALISTS

SOPHOS

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

Sophos provides IT security and data protection products for businesses on a worldwide basis. Sophos offers security solutions for endpoint and mobile security, endpoint detection & response (EDR), managed detection and response (MDR), enterprise mobility management, encryption, server protection, secure email and web gateways, next-generation firewall, UTM and email phishing attack simulation and user training. In October 2019, Thoma Bravo announced the acquisition of Sophos.

SOLUTIONS

Sophos offers three endpoint security solutions, **Intercept X Advanced**, **Intercept X Advanced with EDR**, and **Managed Threat Response**. The EDR version contains all the traditional and modern protection of Intercept X Advanced, but also includes additional endpoint detection and response (EDR) functionality on the same agent. 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 EDR.

- **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 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.

- **Sophos Intercept X Advanced with EDR** – also includes integrated endpoint detection and response capabilities using the same agent. The solution is centrally managed by Sophos Central. It is available for devices running Windows 7 and above, as well as MacOS (without anti-exploit and deep learning). Intercept X can be deployed on its own, or it can augment endpoint security solutions from other vendors. It includes CryptoGuard technology, which prevents encryption of data by crypto-ransomware. It monitors remote computers and local processes that are modifying documents and other files, and if it determines a process is not legitimate, it is terminated and files are restored to their pre-encryption state. **Intercept X for Servers** also features deep learning, anti-exploit, CryptoGuard, anti-ransomware, and other server specific protections.

  Intercept X includes the following capabilities:

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

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

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

  - *WipeGuard* – behavior-based ransomware protection that stops master boot record, or wiper, ransomware.

  - *EDR* – detect, investigate, and respond to potential security incidents.

  - *Managed Threat Response* – offers 24/7 threat hunting, detection, and response delivered by an expert team as a fully-managed service.

- *Endpoint Antivirus* – detects viruses, suspicious files and behavior, adware, and other malware. Real-time antivirus lookups help ensure up-to-date information.

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

- *Server Lockdown/ whitelisting* – integrates anti-malware capabilities with the ability to lock down applications.

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

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

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

- *Full Disk Encryption* – is available for Microsoft Windows and Apple macOS systems. System files, hibernation files, and temp files can all be protected with full disk encryption. Sophos can also manage native Bitlocker or FileVault 2 encryption within the operating system. Data recovery and repair tools are included in the solution.

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

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

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

- *Antivirus product removal* – features let administrators scan managed machines for previous versions of security software that may cause conflicts. Any conflicting software can be automatically removed during deployment.

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

The following solutions are also available as separate add-ons:

- *Mobile Device Management (MDM) and Enterprise Mobility Management (EMM)* – handles all mobile devices, from the initial setup and enrollment, through device decommissioning. It includes a fully featured web-based console allowing administration from any location on any device.

- *Mobile Antivirus* – protects Android devices using up-to-the-minute intelligence from Sophos Labs. Apps can be scanned on installation, on demand or on a schedule.

Sophos solutions can be managed through two solutions: **Sophos Central**, a web console that can monitor the status of all machines on a network, regardless of platform; and **Sophos Enterprise Console**, an on-premises management platform that provides role-based administration and an SQL-based reporting interface. The Intercept X features only available via Sophos Central.

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.

- Intercept X can be deployed alongside non-Sophos antivirus products, layering anti-exploit and anti-ransomware on top of existing deployments, or it can replace existing antivirus products.

- 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 does not support patch assessment and remediation of third party software running on the endpoint (e.g. old versions of Adobe).

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

- For the on-premises solution, management of mobile devices is accessible from the Endpoint Management Console, but runs in a separate management console. This is not an issue in the cloud-based Sophos Central solution.

- 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).

- Reporting features, while adequate, could be improved to support greater customization.

- Sophos MDR services are still relatively new and provide fairly basic threat hunting capabilities. The vendor is working to enhance this service in future releases.

CROWDSTRIKE

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

CrowdStrike, Inc., a wholly owned subsidiary of CrowdSrike Holdings, Inc., delivers endpoint protection, threat intelligence, incident response, and cyberattack response services to customers in over 170 countries. The company 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. Falcon combines artificial intelligence and machine learning techniques to protect against known and unknown threats.

It comprises the following components:

- *Falcon Prevent* – is CrowdStrike's next-generation antivirus (NGAV) solution which delivers protection based on machine learning, as well as exploit blocking, indicator of attack (IOA) behavioral analysis, and more.

- *Falcon Insight* – is its 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.

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

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

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

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

- CrowStrike solutions are based on a lightweight agent and managed services cloud architecture, which delivers a uniform set of protection features across Windows, macOS, and Linux platforms.
- CrowdStrike offers an advanced set of next-generation endpoint protection capabilities which combine AV, EDR, advanced threat protection (ATP), with Managed Detection and Response (MDR), at an attractive price point, 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 focuses mainly on OverWatch, its Managed Detection and Response (MDR) solution for threat hunting and post incident response, as opposed to its product based solutions for attack prevention.

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

- CrowdStrike has lost some mindshare over the past year, as almost all competing endpoint protection vendors have added advanced EDR, ATP and MDR capabilities.

- CrowdStrike solutions tend to be more expensive than many competing next generation endpoint solutions.

PANDA SECURITY

C/ Santiago de Compostela 12, 1ª Planta
48003 Bilbao
Spain
www.pandasecurity.com/business

Panda Security, founded in 1990, is well known for its antivirus software and delivers security solutions for consumers and businesses. Panda Security, headquartered in Spain, has a presence in more than 80 countries and is privately held.

SOLUTIONS

Panda Security offers a cloud-native approach for endpoint security, which includes traditional endpoint protection (EPP), as well as advanced endpoint protection complemented by endpoint detection and response (EDR), and specialized security services. The solutions include:

- **Panda Endpoint Protection (EP)** – provides anti-malware, anti-spyware, anti-phishing protection, protection against zero-day exploits, email and web protection, firewall, IDS/HIDS, device control, disinfection and remediation tools, and more. It is available for Windows, macOS, Linux, and Android.

- **Panda Endpoint Protection Plus (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 (the web access control functionality is only available for Windows).

- **Panda Adaptive Defense** – is Panda Security's Endpoint Detection and Response (EDR) solution, complemented by their 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, and carry out detailed forensic analysis to determine the root cause of breaches, as well as implement mechanisms to avoid future incidents. It is currently available for Windows, while MacOS and Linux are on the roadmap.

- **Panda Adaptive Defense 360** – 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 100% Attestation Service and the Threat Hunting and Investigation Service (THIS) at no extra charge.

Panda Adaptive Defense and Panda Adaptive Defense 360, both leverage the following services:

- *The 100% Attestation Service* – is Panda Security's executable classification service, which monitors and prevents the execution of malicious applications and processes on endpoints.

- *Threat Hunting and Investigation Service (THIS)* – is a managed service which provides real-time and retrospective intelligence on all the events taking place on an organization's systems to discover unknown threats by investigating anomalous users, machines and application behavior. The data helps investigators conduct forensic analysis that make remediation processes more efficient and help reduce the attack surface. In addition, any new

indicators of compromise feed the solution's technologies and automate detection in the early attack phases without human intervention.

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

Panda Security 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.

- **Panda 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.

- **Panda 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.

- **Panda 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.

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

Recently, Panda Security launched Cytomic, a new business unit with its own identity and exclusive portfolio, focused on addressing the needs of organizations with mature security operations centers, and on MSSPs expanding into Managed Detection and Response services. Its first offering is **Cytomic Orion**, a cloud-based Threat Hunting Platform, which allows to query and analyze real-time events and 12 months of enriched events for hunting, conducting IOC searches, and conducting automated template-based investigations through integration with the Jupyter Notebooks platform. It can also take direct remediation and containment actions from the console. Cytomic Orion leverages the 100% Attestation Service from Panda Security, and it can coexist and complement any incumbent EPP and EDR solution on the endpoints.

STRENGTHS

- Panda Security Adaptive Defense 360 combines 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 deliver prevention, detection and response capabilities.

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

- Panda Security 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 Panda Adaptive Defense 360 agent.

- Panda Patch Management is a fully integrated module available for any Endpoint Protection Solutions, included Panda Adaptive Defense 360. It manages vulnerabilities, patches, updates and end-of-life application in both operating systems and third-party applications on Windows endpoints and servers.

- Panda Security solutions are attractively priced.

- The Cytomic ORION solution, which integrates with the Jupyter Notebooks platform to adapt it to threat hunting use cases, is highly innovative.

WEAKNESSES

- Panda Security's EDR and 100% Attestation Service capabilities are currently available only for Windows platforms. The vendor is planning to add support for macOS and Linux in the future.

- Panda Security 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.

- Panda currently provides basic MDM capabilities for Android, however, support for iOS devices is not provided.

- Panda Security currently provides only basic DLP capabilities, through its Data Control module. However, the vendor plans to enhance this with future releases.

- Despite an attractive portfolio of solutions, Panda Security still lacks visibility in the enterprise security space, particularly in North America.

CYLANCE

18201 Von Karman Avenue, Suite 700
Irvine, CA 92612
www.cylance.com

Cylance, founded in 2012, uses artificial intelligence, algorithmic science and machine learning to provide technology and services that offer predictive and preventive protection against advanced threats. In 2019, Cylance was acquired by BlackBerry Limited.

SOLUTIONS

Cylance offers a prevention-first security platform that combines artificial intelligence for predictive prevention, with dynamic threat detection and response, to deliver full threat prevention and visibility across enterprises.

- **CylancePROTECT** – is the prevention-focused component of the platform, 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. CylancePROTECT supports Windows (32bit or 64bit), macOS, and Linux environments. It is available as a cloud deployment, on-premises (as a virtual appliance), or hybrid. 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.

- **CylanceOPTICS** – is the endpoint detection and response (EDR) component of the Cylance Security Platform that enables easy root cause analysis, threat hunting and automated threat detection and response. It augments CylancePROTECT prevention 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.

- **CylanceGUARD** – is Cylance's 24x7 Managed Detect and Response (MDR) offering which provides proactive threat hunting based on its AI platform. It provides access to Cylance analysts to help navigate incidents, delivers regular updates on overall threat prevention status, and helps initiate actions in response to indicators of compromise (IOC).

Cylance also offers managed services to provide enterprises with pre-attack penetration and vulnerability testing, compromise assessments, and post-attack incident response.

STRENGTHS

- Cylance 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.

- CylancePROTECT has a small footprint compared to other security products.

- CylanceOPTICS (i.e. EDR) 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 as well take responsive action, without human intervention.

- All Cylance products are managed through a single dashboard.

WEAKNESSES

- Capabilities such as firewall, DLP and Mobile Device Management are only available through partners.

- CylanceOPTICS can do patch assessment, however, it is not an automated process.

- Customers we spoke with as part of this research, indicated a high degree of false positives.

- Cylance could improve market awareness of its security partnerships, as well as make it easier for customers to integrate its products with third party solutions.

- Cylance has lost some visibility and mindshare, as nearly all traditional endpoint protection vendors have now added advanced next-generation capabilities (e.g. AI, Machine Learning, EDR, and more).

BITDEFENDER

24 Delea Veche St.
Offices Building A, floor 7, district 2
Bucharest, 024102
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 business solution that can be installed on-premises or as a cloud solution hosted by Bitdefender, and can provide security for physical, virtual, hybrid cloud and mobile enterprise networks.

The Bitdefender Business Portfolio includes a number of GravityZone security packages, as follows:

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

- **GravityZone Advanced Business Security** – 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 also 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. However, the mobile security (MDM) component is only available for on-premises deployment.

- **GravityZone Elite Suite** – offers the same services as Advanced Business Security but adds two new pre-execution detection layers - HyperDetect and Sandbox Analyzer. Hyperdetect uses specialized local machine 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, repots 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. However, the mobile security (MDM) component is only available for on-premises deployment.

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

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

Bitdefender also offers a Full Disk Encryption module which can managed via the GravityZone console.

GravityZone Security for Virtualized Environments (SVE) – is the security flagship 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 Hypervisor Introspection (HVI) – is aimed at protecting virtual workloads, enabling data centers and organizations to increase their security posture across their entire infrastructure. It is a security layer complementary to existing security tools, which helps monitor memory space, to discover network intrusions even if no security alarms are triggered within the operating system.

Bitdefender also offers **GravityZone Security for MSPs**, 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 has partnerships with diverse vertical MSP providers, such as Connect Wise, LabTech and Kaseya, to serve multiple segments in the MSP community.

Bitdefender also offers the **GravityZone Managed Endpoint Detection and Response (MEDR)** service, which delivers 24x7 security monitoring, bringing together security experts, telemetry and threat intelligence feeds to detect and respond to malicious attacks.

STRENGTH

- 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 endpoint protection and EDR solution, which can be easily deployed by organizations of all sizes.

- 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.

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.

- GravityZone Endpoint Security currently provides only basic DLP-like functionality which allows Administrators to define patterns to be checked against scanned SMTP and HTTP traffic.

- While offering highly accurate malware and threat detection solutions, Bitdefender lacks advanced analysis and response capabilities, such as integration with third-party SIEM and/or SOAR tools.

- Bitdefender has been somewhat late to add Managed Detection and Response (MDR) capabilities, compared to many competing vendors.

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

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 solutions for endpoint protection, detection and response, advanced threat protection and vulnerability management, as well as red

teaming, cyber security assessment, training and consultancy services. In 2018, F-Secure acquired MWR InfoSecurity, a provider of cybersecurity services including managed threat hunting and managed phishing protection. F-Secure is based in Finland, and is publicly traded in the country.

SOLUTIONS

F-Secure endpoint protection products are available in two flavors, with EDR detection and response capabilities available on top of both either as a product, or as a managed service:

- **F-Secure Protection Service for Business** (cloud service) – includes the following key features:

  - *Management Portal (cloud)* – central management portal for deployment, management and monitoring, with integrated mobile fleet management.

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

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

  - *Server protection* – comprehensive server security for Windows, Linux and Citrix. Additional SharePoint and Exchange components, with fully integrated patch management.

- **F-Secure Business Suite** (on-premises) – includes the following key features:

  - *Central Management* – management of all IT security in one place, including monitoring and enforcing security policies.

  - *Client Security* – multi-layered security for desktops and laptops which provides complete endpoint protection. Includes advanced behavior, heuristic analysis, ransomware protection, and fully integrated patch management.

- *Server Security* – real-time protection for Microsoft Windows servers, Citrix and Microsoft servers.

- *Communication & Collaboration* – spam and malware protection for Microsoft Exchange and Microsoft SharePoint.

- *Linux Security* – multilayered security for Linux workstations and servers.

- *Virtual Security* – offers optimized performance for public and private virtual environments by offloading scanning to a dedicated server.

- *Web Filtering* – protection for email, browsing and file transfer traffic.

- *Automatic Patch Management* – up-to-date patching of operating system and third party applications.

- **F-Secure Rapid Detection & Response** (cloud service) – includes the following key features:

  - Advanced threat protection with real-time behavioral, reputational and big data analysis with machine learning.

  - Endpoint clients allow the execution of remote response actions, like host isolation, on both Windows and macOS.

  - Automated response actions are available to contain attacks whenever high risk levels are identified.

  - On-demand access is available to F-Secure's managed detection and response team for incident analysis and investigations.

  - The clients are designed to work with any endpoint protection solution, and function with F-Secure's endpoint security solutions in a single-client and management infrastructure.

F-Secure also offers **F-Secure Countercept** a 24/7 managed threat hunting service to detect and respond to even advanced live, hands-on keyboard attacks in minutes.

STRENGTHS

- F-Secure offers both a cloud-based solution, as well as an on-premises solution to fit different customer needs.
- F-Secure uses a multi-layered architecture for malware detection and endpoint protection. Including DeepGuard, its advanced behavioral analytics engine.
- Real-time threat intelligence from F-Secure Security Cloud ensures up-to-date protection. Updates are transparent and delivered constantly, without disrupting employee productivity.
- Fully integrated patch management and EDR capabilities, which do not require additional client agents.
- 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 a very easy, simple process.

WEAKNESSES

- F-Secure does not offer DLP capabilities.
- F-Secure's Business Suite on-premises offering lags somewhat behind its cloud-based offering in a number of areas, including: VPN support, iOS, and Android support.
- Support for Microsoft Office 365 is not currently available, but is on the near term roadmap.
- F-Secure has improved its market visibility, but still needs to make progress in this area particularly in North America.

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. Its solutions are powered by the cloud-based Trend Micro Smart Protection Network, which brings together threat reporting and analysis based on a worldwide threat assessment infrastructure. The company is publicly traded.

SOLUTIONS

Trend Micro **Smart Protection Suites** offers an integrated defense solution for desktops, laptops, servers and virtualized deployments, with a central management interface. The vendor's XGen Endpoint Security functionality, combines machine learning and other techniques, in order to protect against ransomware and advanced attacks.

The endpoint component of Smart Protection Suites is **Apex One**, Trend Micro's flagship enterprise product which combines traditional endpoint protection with endpoint detection and response (EDR) and managed detection and response (MDR) capabilities. It replaces OfficeScan which was Trend Micro's previous solution. OfficeScan customers are able to obtain Apex One as a regular upgrade, although access to some functionality, such as the EDR component, requires an appropriate license entitlement. 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 a number of additional components which include:

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

Endpoint 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), 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.

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.

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, EDR and MDR 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 endpoints.

WEAKNESSES

- Trend Micro has been slow to innovate its portfolio, particularly as it pertains to the addition of advanced threat detection technologies. Its XGen machine learning functionality was a late addition and is still only keeping pace with competing solutions.

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

- 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.

MICROSOFT

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

Microsoft develops products and services for businesses and consumers, and delivers an extensive portfolio of solutions which include office productivity, messaging, collaboration, and more.

SOLUTIONS

Microsoft has folded much of its endpoint protection directly into the operating system, starting with Windows 10 and Windows Server 2016 computers. The solutions are branded under the **Windows Defender** umbrella name, as follows:

- **Windows Defender Antivirus (AV)** – 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 11 in Windows 10.

- **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 upgrade 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.

- **Microsoft Defender Advanced Threat Protection ATP** – is a cloud-based EDR analytics protection and response service designed to help detect, block and remediate zero-day threats. It provides protection against phishing, malware and spam attacks. It can offer near real-time protection against high-volume spam campaigns, with DKIM and DMARC support. It also adds protection against “zero-day” attachments and harmful URL links, through real-time behavioral analysis and sandboxing. Microsoft Defender ATP is also available for Mac platforms, while support for Linux platforms is currently available only through partners.

Microsoft Defender Advanced Threat Protection ATP can be managed from the Microsoft Security Center console, which provides a unified control point across the entire enterprise environment encompassing Azure ATP, Office 365 ATP, Azure Active Directory, SQL Server, Microsoft Cloud App Security, and more.

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 a single administration console, **Microsoft System Center Configuration Manager (System Center)**, which unifies policy management and device management.

As part of Microsoft Defender ATP, 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.

STRENGTHS

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

- SCEP is included at no additional cost as part of the Microsoft Enterprise Client Access License and Core CAL programs. Microsoft Intune is available as a component of Microsoft's Enterprise Mobility Suite (EMS), which includes Microsoft Azure Active Directory Premium, and Microsoft Azure Information Protection. This makes SCEP and Intune some of the least expensive endpoint security solutions on the market, as many customers are able to get the solutions at no additional cost as part of 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 continues to invest heavily in security, delivering 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 advanced protection.

- In order to benefit from the more advanced security features, customers have to upgrade to Windows 10.

- In order to obtain Microsoft's full range of security solutions, including the EDR component, Microsoft Defender Advanced Threat Protection (ATP), customers must upgrade to the high-end Microsoft 365 E5 enterprise license.

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

- 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 Linux, as a separate add-on through third-party partners, however, management of these clients is not integrated with System Center.

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, 2019-2023	Apr. 2019	$3,000.00
Microsoft Office 365, Exchange Server and Outlook Market Analysis, 2019-2023	Apr. 2019	$3,000.00
Email Market, 2019-2023	Apr. 2019	$3,000.00
Cloud Business Email Market, 2019-2023	Mar. 2019	$3,000.00
Corporate Web Security Market, 2019-2023	Mar. 2019	$3,000.00
Unified Endpoint Management Market, 2019-2023	Mar. 2019	$3,000.00
Information Archiving Market, 2019-2023	Mar. 2019	$3,000.00
Advanced Persistent Threat (APT) Protection Market, 2019-2023	Mar. 2019	$3,000.00
Email Statistics Report, 2019-2023	Feb. 2019	$3,000.00
Social Networking Statistics Report, 2019-2023	Feb. 2019	$3,000.00
Instant Messaging Statistics Report, 2019-2023	Jan. 2019	$3,000.00
Mobile Statistics Report, 2019-2023	Jan. 2019	$3,000.00
Endpoint Security Market, 2018-2022	Nov. 2018	$3,000.00
Secure Email Gateway Market, 2018-2022	Nov. 2018	$3,000.00
Cloud Access Security Broker (CASB) Market, 2018-2022	Nov. 2018	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Information Archiving Market, 2020-2024	Mar. 2020	$3,000.00
Email Statistics Report, 2020-2024	Feb. 2020	$3,000.00

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

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