The Radicati Group, Inc.
www.radicati.com

THE RADICATI GROUP, INC.

Endpoint Security - Market Quadrant 2017

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

October 2017

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.

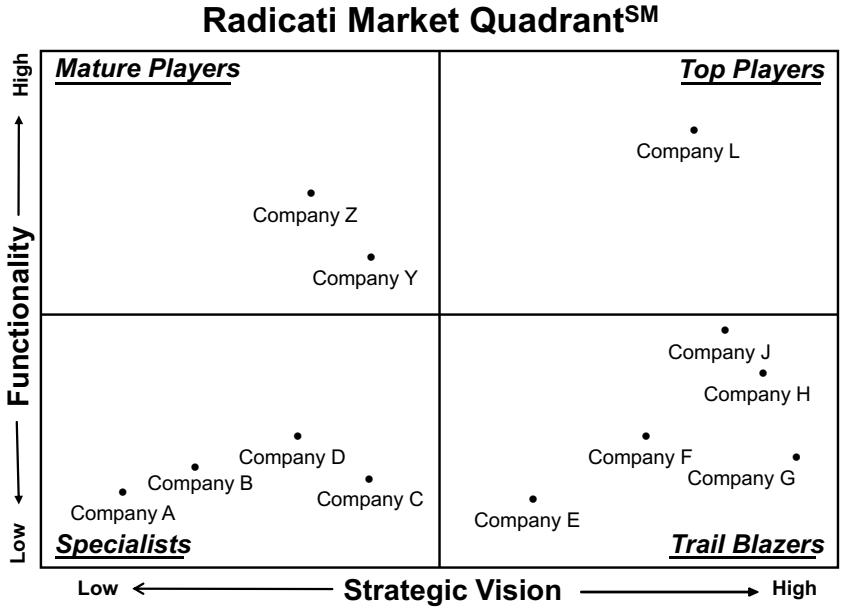

Figure 1: Sample Radicati Market Quadrant

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. The key features of endpoint security solutions are antivirus and malware protection, web security, email security, firewall functionality, and much more. Leading vendors in this market, include: *Avast, Bitdefender, Cisco, Comodo, Cylance, ESET, F-Secure, Kaspersky Lab, Malwarebytes, McAfee, Microsoft, Panda Security, Sophos, Symantec, Trend Micro,* and *Webroot*.

- Vendors in this market often target both consumer and business customers. However, this report deals only with solutions which address the needs of business customers, ranging from SMBs to very large organizations.

- Government organizations are considered "business/corporate organizations" for the purposes of this report.

- The market for endpoint security solutions continues to see strong growth as organizations of all sizes are investing heavily to protect against a growing landscape of threats and malicious attacks.

- The line between traditional endpoint solutions and next generation endpoint solutions is blurring as nearly all vendors now offer behavior-oriented solutions which include sandboxing, endpoint detection and response (EDR), advanced persistent threat (APT) protection and more. For organizations of all sizes, endpoint security is no longer an isolated discipline but is increasingly part of an organization-wide defense posture.

- Endpoint security solutions also increasingly include DLP, encryption, and MDM functionality to provide an efficient first line of defense against all types of data and information loss.

- Cloud-based endpoint security solutions continue to see strong growth as more organizations of all sizes look to leverage the benefits of cloud adoption. Cloud-based deployments are

particularly attractive in the security space because of the advantages they provide in terms of ensuring that updates and threat information are distributed quickly across the entire organization.

- The Endpoint Security market will top $5.2 billion in 2017, and grow to over $8.0 billion by 2021. Figure 1, shows the projected revenue growth from 2017 to 2021.

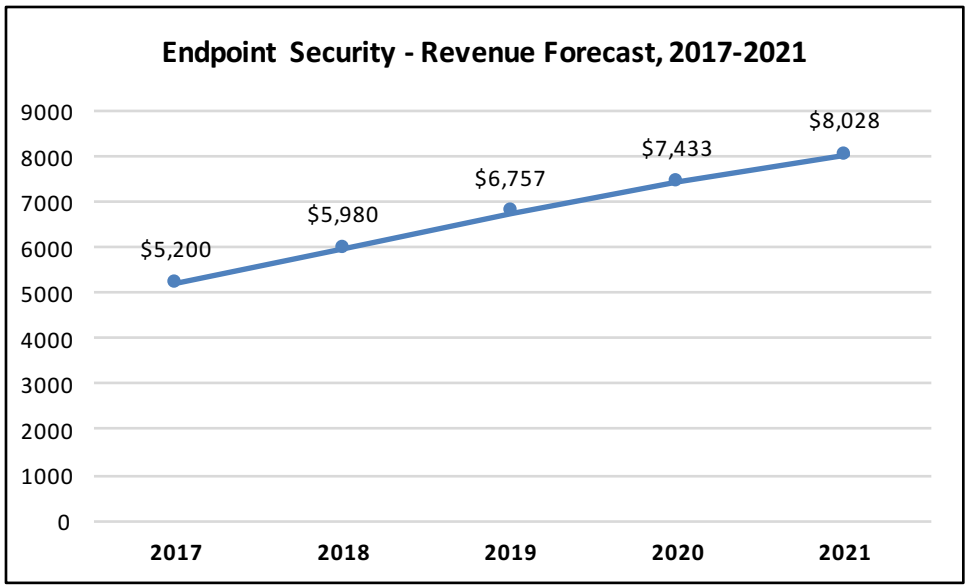

Figure 1: Endpoint Security Market Revenue Forecast, 2017-2021

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.

- ***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.

- ***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.

- ***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.

- ***Mobile device protection*** – a growing number of endpoint security vendors are starting to 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 a key differentiator.

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

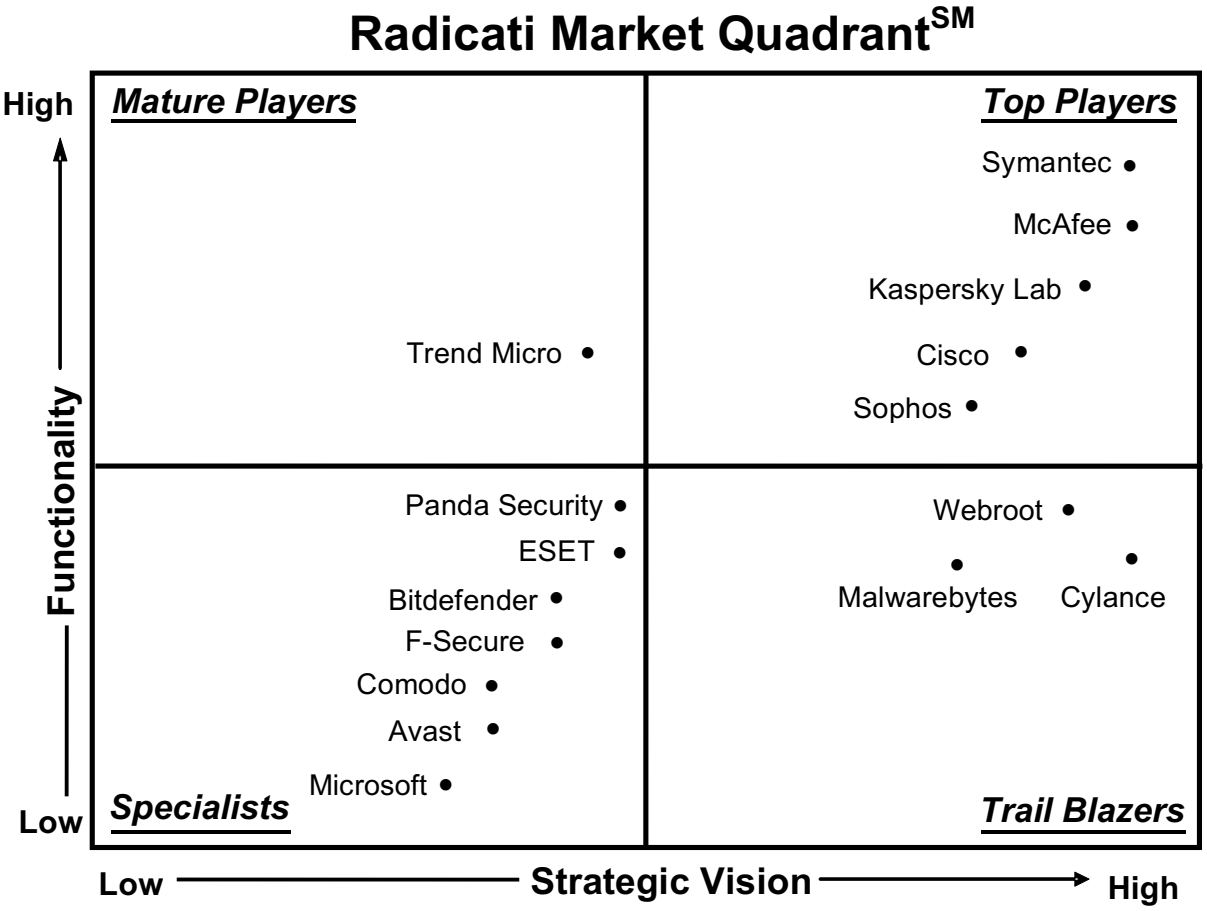

Figure 2: Endpoint Security Market Quadrant, 2017

* Radicati Market Quadrant℠ is copyrighted October 2017 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, Kaspersky Lab, Cisco* and *Sophos.*
- The **Trail Blazers** quadrant includes *Webroot, Cylance* and *Malwarebytes.*
- The **Specialists** in this market are *Panda, ESET, Bitdefender, F-Secure, Comodo, Avast,* and *Microsoft.*
- The **Mature Players** quadrant includes *Trend Micro*.

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 the enterprise and for consumers. Symantec operates one of the largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. In July 2017, Symantec acquired Skycure for its mobile threat protection technology.

SOLUTIONS

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

- **Symantec Endpoint Protection 14,** the latest version of its endpoint protection suite is compatible with the latest versions of Windows, macOS, Linux, VMware ESX, Citrix XenServer, and other virtual machines. It provides the following capabilities:

  - *Malware protection* – is provided through multiple layers that include advanced signature-less detection technologies as well as traditional signatures. Symantec's signature-less capabilities include advanced machine learning, behavior monitoring and memory exploit mitigation, which combine with reputation analysis, intrusion prevention and global intelligence network, to defend against advanced threats and zero-day attacks. A new cloud console provides insight into suspicious files and the ability to aggressively block new and emerging threats.

  - *Intensive Protection* – uses advanced machine learning, behavioral analysis, and reputation to discover and track suspicious files. The Intensive Protection policy can be tuned to proactively block more threats while minimizing false positives through efficient whitelisting and blacklisting.

  - *Exploit Protection* – is provided through new memory exploit mitigation technology to help prevent zero-day exploits of vulnerabilities in popular software (e.g. browsers, operating systems, enterprise software, and more).

  - *Email security* – is included in Symantec Endpoint Protection. The solution can scan all incoming and outgoing mail over POP3 or SMTP. Protection can be enabled for Microsoft Outlook, and IBM Notes.

  - *Web security* – is included to protect browsers from malicious activity, such as exploits designed to attack a browser vulnerability, drive-by downloads, and more.

  - *Firewall* – capabilities are built-in with features like denial of service detection, stealth web browsing to prevent websites from learning browser details, and more. Individual rules can also be created to block certain applications from accessing the Internet.

  - *Device control* – for USBs is included. Administrators can block files being written to these devices. Options are available to prohibit any software from an external device from running automatically. External storage devices can also be set to read-only.

Symantec Endpoint Protection supports a long list of devices that can be blocked, such as disk drives, FireWire, and more. SEP 14 added device control for managed Mac clients.

- *Antivirus removal tools* – are included to remove unwanted previous deployments of security solutions.

- *Recovery tools* – are included via the Symantec Endpoint Recovery Tool that can repair infected PCs by creating a rescue disk, or USB drive that can safely remove any malware.

- *Reporting* – for various levels of detail is available. Compliance, risk, application and device control, and others are among the different types of reports that can be generated. Frequency generation of reports can be scheduled.

- *REST APIs* – facilitate integration with Secure Web Gateway (from the Blue Coat acquisition) and other security infrastructure to orchestrate a response on the endpoint geared toward stopping the spread of infection.

- *Intelligent Threat Cloud* – are patented cloud lookup technologies to speed detection of suspicious files with high accuracy. This capability combined with the addition of Advanced Machine Learning on the endpoint enables the reduction in size and frequency of definition file updates, significantly reducing bandwidth usage.

- *Management* – is performed from one interface. Policies can be set with high levels of granularity in the centralized console.

Symantec also offers **Symantec Endpoint Protection Cloud (SEP Cloud),** which offers a simplified management console that is deployed as a cloud-based solution. SEP Cloud offers protection for traditional endpoints (Windows, macOS) and modern endpoints (iOS, Android) from a single solution. While the core security technologies for traditional endpoints remain the same, some of the advanced functionality has been removed, such as device and application control, limited virtual machine support, and others.

Symantec Endpoint Protection Mobile is available for iOS and Android devices. It uses predictive technology in a layered approach that leverages massive 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 Endpoint Protection enables Endpoint Detection and Response via **Symantec Advanced Threat Protection: Endpoint** with visibility into a file's static file attributes (e.g. has keylogging functionality, has a UI window, and more) and its full behavioral process trace in order of their observation. Event details from the Symantec Endpoint Protection client are analyzed for suspicious activities and prioritized incidents are created. The solution is integrated with an advanced cloud sandbox which can detect even 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 ATP supports searching for evidence or indicators of compromise (IOC's) on endpoint devices.

STRENGTHS

- Symantec offers a single management console across Windows, macOS, Linux, Embedded and Virtual machines, as well as a single integrated-client on the endpoint for more seamless management and performance.

- SEP offers multi-layered protection powered by artificial intelligence and advanced machine learning.

- Symantec Endpoint Protection has many features optimized for virtual environments and embedded machines, which reduce performance impact across both physical and virtual machines.

- 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 Insight network. It can also do behavioral analysis and apply application controls.

- Symantec's management console offers rich Directory Services integration, with policy-based protection.

- Symantec SEP 14 integrates with Symantec ATP platform, which includes ATP:Endpoint, ATP:Network and ATP:Email for full enterprise protection across all threat vectors.

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

WEAKNESSES

- SEP 14 offers mobile device protection as a separate option, available for separate purchase.

- Patch assessment and management, powered by Altiris, is delivered through Symantec Endpoint Management but is not integrated with Symantec Endpoint Protection.

- DLP capabilities require a separate add-on.

- SEP 14 offers encryption as a separate option, available for separate purchase.

MCAFEE

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

McAfee delivers security solutions and services for business organizations and consumers. The company provides security solutions, threat intelligence and services that protect endpoints, networks, servers, and more.

SOLUTIONS

McAfee security solutions are built on a security framework that leverages multiple defense layers. Advanced defenses like machine learning analysis and dynamic application containment work with local and global threat intelligence to provide comprehensive insights across all threat vectors—file, web, message, and network. McAfee solutions are managed through ePolicy Orchestrator (ePO), which delivers a centralized management experience for administrators.

McAfee endpoint protection solutions protect Windows, Macs, and Linux systems, as well as mobile devices, such as iPhone, iPad, and Android smartphones and tablets through partnerships with AirWatch and MobileIron.

McAfee endpoint security solutions are compatible with Microsoft Windows workstations and servers, Mac, VMware ESX, Linux, Citrix XenDesktop and XenServer, and other virtual platforms.

McAfee's endpoint portfolio includes the following solutions to meet different customer needs at different price points:

- **McAfee Dynamic Endpoint Threat Defense** – consists of two endpoint protection suites (McAfee Endpoint Threat Protection, McAfee Complete Endpoint Threat Protection) and optional add-ons that offer advanced threat defenses, and detection and response (EDR) capabilities.

- **McAfee Complete Endpoint Threat Protection** – is a security solution aimed at the advanced needs of large enterprises. In addition to the essential antivirus, antispam, web security, firewall, and intrusion prevention, it includes static code and behavioral machine learning analysis, dynamic application containment, behavioral anti-malware, and dynamic whitelisting. It is managed through a single endpoint management console which covers all platforms including: smartphones, tablets, Macs, Windows, Linux, UNIX, virtual systems, and servers. The suite includes McAfee Endpoint Security (ENS) which provides customers with an intelligent, collaborative framework that enables endpoint defenses to communicate, share intelligence, and act against advanced threats.

- **McAfee Complete Endpoint Protection - Business** – is an all-in-one solution that uses collaborative threat and global threat intelligence to defend against advanced threats, and offers encryption, dynamic application containment and machine learning for desktops and laptops to halt zero-day exploits. Phishing and multistage attacks are also blocked through its email, web, and collaborative endpoint defenses. It supports centralized, web-based administration.

- **McAfee Endpoint Threat Protection –** provides essential protection for customers that want the ability to change and grow as their business or environment changes. It includes

threat prevention, integrated firewall, web control, and more.

- **McAfee Endpoint Protection for SMB –** is designed for small and medium-size businesses and offers an all-in-one solution that addresses anti-malware, anti-spyware, data, and web security needs. It is available both on-premises and through the cloud. It also includes mobile security and mobile device management capabilities.

- **McAfee Endpoint Threat Defense** and **McAfee Endpoint Threat Defense and Response –** are available to McAfee endpoint suite customers who want to want to add advanced threat defenses or endpoint detection and response capabilities to their existing McAfee endpoint suite. Both leverage static and behavioral analysis and synthesized intelligence to protect, detect, correct, and adapt to combat emerging threats. Threat Defense adds Dynamic Application Containment and Real Protect Machine learning capabilities, while Threat Defense and Response also includes McAfee Active Response, which is McAfee's EDR capability.

- **Active Response –** is McAfee's endpoint detection and response (EDR) solution, which offers continuous visibility into endpoints, so organizations can identify breaches faster and gain more control over the threat defense lifecycle.

- **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.

STRENGTHS

- McAfee solutions are feature rich and include encryption, firewall, elements of DLP, HIPS and a variety of other features and capabilities, which are usually not present in competing endpoint solutions.

- McAfee machine learning technology includes both pre-execution and post-execution analysis.

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

- McAfee offers a broad range of endpoint solutions to fit the diverse needs of customers of different sizes and security requirements.

- 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 has retired its own mobile device protection solution and now relies on partnerships with best of breed vendors, such as AirWatch and MobileIron.

- McAfee solutions currently can only inventory endpoint software however, third party tools must be used to remediate/update software on endpoints.

KASPERSKY LAB

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

Kaspersky Lab is an international group, which provides a wide range of security products and solutions for consumers and enterprise business customers worldwide. The company's security portfolio includes endpoint protection, as well as specialized security solutions and services to combat evolving digital threats. The company has a global presence with offices in 32 different countries.

SOLUTIONS

Kaspersky Endpoint Security for Business (KESB) is a next generation integrated endpoint threat defense 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 Endpoint Security solutions offer support for a broad array of platforms, which include Windows, Linux, macOS, Android, iOS and Windows Phone.

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, Device Control, Application Control, Web Control, Mobile Device Management (MDM), and Security Management.

- *Advanced* – provides Next Generation Threat Prevention (for Windows, macOS and Linux) with Behavior Detection, Exploit Prevention, Host Intrusion Prevention, Remediation Engine, Device Control, Application Control, Web Control, Mobile Device Management (MDM), Data Protection (full disk and file-level Encryption), Systems Management (Patch Management), and Security Management.

- *Total* – provides Next Generation Threat Prevention (for Windows, macOS and Linux) with Behavior Detection, Exploit Prevention, Host Intrusion Prevention, Remediation Engine, Device Control, Application Control, Web Control, Mobile Device Management (MDM), Data Protection (full disk and file-level Encryption), Systems Management (Patch Management), Security for Collaboration, Security for Mail, Security for Internet Gateway, and Security Management.

All endpoint security products are managed by the **Kaspersky Security Center**, which delivers security management and control through a single administrative tool. Kaspersky's 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.

Kaspersky Endpoint Security Cloud, released in September 2016, is Kaspersky Lab's 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 endpoints, mobile devices and file servers.

In addition, **Kaspersky Security for Virtualization (KSV)** protects servers, desktops and data centers for VMware, Citrix, Microsoft Hyper-V and KVM virtual environments. KSV focuses on optimizing resource use and reducing infrastructure and equipment costs.

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

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

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

- *Post-execution behavioral analysis* – including System Watcher with exploit protection, host-based intrusion prevention/HIPS and reputation services.

- *Endpoint forensics data collection* – event logging and automated respond with active malware disinfection and malicious activities rollback.

Kaspersky Lab offers a full-scale Enterprise Security Platform comprising the following solutions: Endpoint Security (that also includes Kaspersky Embedded Systems Security for ATM and PoS protection), Mobile Security, Security for Data Centers, Virtualization Security, Anti-Targeted Attack solutions, Industrial CyberSecurity, Fraud Prevention, Security Intelligence Services, and DDoS Protection.

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 supports a broad range of systems, encompassing Windows, Linux, macOS, VMware, Citrix, KVM, IBM Notes/Domino, Microsoft Exchange, Android, iOS and Windows Phone.

- Kaspersky solutions rely on its own multi-layered technologies with pre-execution prevention and proactive detection technologies to provide fast, up to date real-time protection.

- The Kaspersky Security Center management console provides a comprehensive management tool that allows organizations to identify all endpoint assets (physical, virtual, and mobile), as well as conduct fast vulnerability assessments, achieve a real-time hardware and software inventory, and provide clear actionable administrator reporting.

- Kaspersky Systems Management can inventory and identify vulnerabilities, as well as automatically perform patch remediation.

- Application controls are very granular in Kaspersky's endpoint solutions, such as application privilege controls. Application Startup Controls support Default Deny mode with Dynamic Whitelisting.

- Kaspersky offers strong support for virtual environments. Kaspersky Security for Virtualization 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.

- Kaspersky lets administrators filter Web traffic by content, a feature that is typically not available in the Web security controls provided by other endpoint security solutions.

WEAKNESSES

- Kaspersky Lab's Endpoint Security Cloud, is currently aimed only at small-medium businesses (with less than 1,000 users), and MSPs. A cloud-based solution aimed at larger

customers is on the vendor's roadmap.

- 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.

- 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 has invested in a number of acquisitions over the last four years, including OpenDNS, Cloudlock, Sourcefire, Cognitive, and ThreatGrid. 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-managed endpoint security solution that can prevent attacks, as well as detect, contain, and remediate advanced threats if they get past front-line defenses. It offers coverage for PCs, Macs, Linux CentOS and RedHat, mobile devices (Android and iOS) and virtual systems. The following key capabilities are provided:

- *Malware Prevention* – is provided through a combination of file reputation, cloud-based sandboxing, and intelligence driven detection. Cisco's Talos Security Intelligence and Research group provides threat intelligence to the solution. Cisco AMP for Endpoints can automatically detect and block known and emerging threats in real time using both cloud-

and system-based technologies that include: big data analytics, machine-learning, fuzzy fingerprinting, a built-in antivirus engine, rootkit scanning, and more. It analyzes unknown files using built-in sandboxing technology and closes attack pathways and minimizes vulnerabilities with proactive protection capabilities.

- *Malware Detection* – AMP for Endpoints provides continuous monitoring and detection of files already on endpoints to identify malicious behavior and decrease time to detection. If malicious behavior is detected, it can automatically block the file across all endpoints, and show the security team the recorded history of the malware's behavior. This helps security teams understand the full scope of the compromise and respond appropriately.

- *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. Remediation capabilities come standard with AMP for Endpoints. If a threat is detected, AMP automatically contains and remediates across all of 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 AMP products via collective intelligence. If a file is determined to be malicious via AMP for Email or Web Security, that information is immediately shared across all AMP platforms, both for any future detection of the malicious file and retrospectively if the file was encountered by any of the other AMP platforms. 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 with no 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. Firepower and Cisco Identity Services Engine (ISE) are 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.

- *Reporting* – AMP for Endpoints offers static, dynamic, and historical reports. These include reporting on high-risk computers, overall security health, 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 larger, 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 AMP for Endpoints can be deployed on-premises, or as a cloud or private cloud form factor.

- AMP for Endpoints offers protection across PCs, Macs, Linux, mobile devices (Android and iOS) and virtual environments.

- Cisco offers a broad security portfolio, which encompasses threat intelligence, heuristics, behavioral analysis and sandboxing to prevent threats from entering the endpoint. The solution also detects threats that may have entered the network and provides response

capabilities to remediate across all protected endpoints.

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

- When integrated with Cisco AMP for Networks and other Cisco security solutions, AMP for Endpoints provides 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.

WEAKNESSES

- Cisco offers different management consoles which share and correlate threat data between them, however, Cisco could improve the management of its security solutions by offering a single, unified management console for all its security solutions.

- Cisco AMP for Endpoints does not integrate with Active Directory or LDAP to help enforce user policies.

- Cisco relies on partners to deliver MDM and EMM capabilities.

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

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

- Cisco AMP for Endpoints will appeal mostly to large and mid-size customers with complex endpoint protection needs, who wish to deploy endpoint protection as part of an enterprise-wide security architecture.

SOPHOS, LTD.
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 such as endpoint and mobile security, enterprise mobility management, encryption, server protection, secure email and web gateways, next-generation firewall, UTM and email phishing attack simulation and user training. In 2017, Sophos acquired Invincea, to bring artificial intelligence and deep learning to its portfolio.

SOLUTIONS

Sophos offers two endpoint security solutions which may be used together or separately:

- **Sophos Intercept X** – is a next-generation endpoint protection solution that combines signature-less exploit prevention, deep learning malware detection, and anti-ransomware techniques. Synchronized security automates incident response via constant and direct sharing of threat, security, and health information between endpoint and network. Intercept X is designed to augment existing endpoint security or antivirus software, delivering anti-exploit, anti-ransomware, root cause analysis, and advanced system cleaning technology. It is available for devices running Windows 7 and above. Intercept X can be used in conjunction with Sophos Endpoint Protection, as well as to augment endpoint security solutions from other vendors. Intercept X CryptoGuard technology prevents encryption of data by crypto-ransomware. It monitors remote computers and local processes that are modifying documents and other files, if it determines a process is not legitimate, it is terminated and files are restored to their pre-encryption state.

- **Sophos Endpoint Protection** – supports Microsoft Windows, Apple macOS, Linux, Unix, virtual machines, network storage, Microsoft SharePoint, Microsoft Exchange Server, and mobile devices (iOS, Android and Windows Phone 8). It includes the following capabilities:

- *Next Generation Endpoint Protection* – through Intercept X technology can block ransomware, provide signature-less exploit prevention and Root-Cause Analysis.

- *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.

- *Vulnerability scanning* – is available with patch assessment that can routinely check whether endpoints are missing any software patches or updates.

- *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.

- *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* – functionality to protect 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.

Sophos also offers **Sophos for Virtual Environments,** which is available separately and provides a centralized method for optimal security scanning performance in virtual environments.

STRENGTHS

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

- 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 functions.

- Sophos employs a single endpoint agent for Intercept X, AV, HIPS, Application Control, DLP, Device control, firewall, web protection and web filtering.

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

- Many features that are often only available as an add-on in competing endpoint security platforms are available standard in Sophos Endpoint Protection, such as DLP, encryption, and more.

WEAKNESSES

- Patch remediation is not yet available. Current features are limited to patch assessment.

- 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.

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

- Sophos Endpoint Protection is best suited for small and medium sized businesses, looking for ease of use and administration.

TRAIL BLAZERS

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

Webroot provides cybersecurity to consumers and businesses through a portfolio of endpoint security, network security, and threat intelligence solutions. Founded in 1997 and headquartered in Colorado, Webroot operates globally across North America, Europe and the Asia Pacific region.

SOLUTIONS

Webroot offers the **SecureAnywhere** suite of security products for endpoints and mobile devices. Powered by Webroot's cloud-based threat intelligence platform, Webroot solutions combine the latest real-time intelligence from Webroot BrightCloud services with advanced machine learning and behavior-based heuristics. Using up-to-date, cloud-based technology, Webroot can detect, analyze, categorize, score, and highly accurately predict the threats each endpoint is experiencing in real time.

- **Webroot SecureAnywhere 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* – designed to counter unknown 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 Protection* – is provided through a number of different shields within the Webroot solution. The Web Threat Shield uses Webroot's threat intelligence to block sites with poor reputations and known infected or malicious domains. Webroot's Real-Time Anti-Phishing service is also integrated to stop phishing and spear-phishing. The Identity/Privacy Shield isolates the browser (and any other application needed) from the rest of the endpoint. It protects the user and device, so even if there is malicious code already present, sensitive information such as access credentials cannot be stolen.

- *Enhanced Web Filtering* – is a web threat shield capability, where websites are validated using Webroot's web categorization and reputation threat intelligence data to ensure safer browsing for end users. Web sites are also checked using the BrightCloud Real Time Anti-Phishing service, which offers real-time site analysis for unknown sites.

- *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. While a file or process is undetermined, the firewall also monitors for data exfiltration.

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

- *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, full monitoring and journaling are automatically initiated. As soon as the endpoint reconnects to the Internet, any new 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 SecureAnywhere web-based management console. Policies can be set for an individual user or groups of users.

- *Global Site Manager* – is an Enterprise and MSP management console specifically designed to meet the needs for multi-location and multi-site management. It is designed to simplify and reduce the operational management overhead associated with complex endpoint deployments. It is also integrated with the Webroot Unity API, which allows MSPs to access real-time data to use within their own management, reporting, billing and workflow applications. The Global Site Manager also integrates the Webroot SecureAnywhere DNS protection service, and will include the Webroot Security Awareness Training service.

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

- *Windows 10 Support* – Webroot supports Windows 10, as well as covers Microsoft's Edge browser with web filtering and anti-Trojan protection (ID Shield).

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

- *GSM Dashboards* – offer full endpoint dashboard drill down capabilities, which allows administrators to quickly respond to events and investigate any anomalies or alerts on the dashboard.

- *Advanced Reporting* – provides reporting capabilities from a scheduled reporting engine that can generate reports based upon administrative preferences. The console allows the ability to schedule generation and emailing of reports.

- *Unity API* – is an API which lets Webroot SecureAnywhere solutions be easily integrated into other IT management platforms including RMMs, PSAs, bespoke billing platforms, and internal IS systems. Current integrations include Autotask, Atera, ConnectWise, Continuum, Kaseya, and Ninja. The UnityAPI is also available to MSPs for further automation of processes, reports and other endpoint services.

Webroot SecureAnywhere Business Mobile Protection is a separate solution for mobile devices, which currently supports Android and iOS devices (both iPad and iPhone). It can be

provisioned through the same web-based management console as the Webroot's endpoint security solution.

STRENGTHS

- Webroot SecureAnywhere Business Endpoint Protection offers a small install 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.

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

- Webroot SecureAnywhere Business Endpoint Protection is easy to manage, as it allows all endpoints to be kept up to date through cloud-based malware detection and the ability to automatically rollback and auto-remediate all infected endpoints.

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

WEAKNESSES

- DLP and encryption capabilities are not included in Webroot SecureAnywhere Business Endpoint Protection.

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

- Protection for mobile devices requires a separate product, however, Webroot provides a single management console for both computer endpoint and mobile device security.

- Webroot does not provide patch assessment and management.

CYLANCE, INC.
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. Cylance is privately held and is based in Irvine, California.

SOLUTIONS

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

- **CylancePROTECT** – is the prevention-focused component of the platform, and delivers malware prevention powered by artificial intelligence, combined with application and script control, memory protection, and device policy enforcement to prevent successful cyberattacks. Without using signatures or streaming data to the cloud, it delivers protection against common threats such as malware, ransomware, file-less malware, malicious scripts, weaponized docs, and other attack vectors. CylancePROTECT is available for Windows (32bit or 64bit), macOS, and Linux environments. 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 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.

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

STRENGTHS

- Cylance is a SaaS based security provider, however all client data is stored locally removing the need for an always-on cloud connection.

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

- Once set up, CylancePROTECT can run autonomously with minimal human intervention and can detect and block malware that did not even exist when the model was created and trained.

- 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.

- Cylance can do more to communicate to the market the breadth of threat prevention it offers for file-less attacks (application and script control, memory protection, and device usage policy enforcement).

- 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.

MALWAREBYTES

3979 Freedom Circle,
Santa Clara, CA 95054
www.malwarebytes.com

Malwarebytes, founded in 2008, offers solutions to proactively protect consumers and businesses against malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. Malwarebytes operates globally across North America, Europe, the Middle East, and Asia Pacific regions. The company is privately held.

SOLUTIONS

Malwarebytes offers both on-premises and cloud-based corporate solutions. Malwarebytes detection technologies are developed internally and do not rely on third party technology. Malwarebytes deep visibility into malware attacks and unique telemetry provides the foundation for Malwarebytes solutions. Malwarebytes protects against all stages of the attack chain and remediates advanced threats. It provides a multi layered detection approach consisting of behavior rules, signatures, and signature-less detection and blocking methods. Malwarebytes Endpoint Protection Detection capabilities include application hardening, Web protection,

Exploit mitigation (for both file-based and file-less malware), ransomware mitigation, application behavior, payload analysis, anomaly detection (machine learning), an incident response engine, and a Linking Engine that removes not only the malware itself but also all related artifacts to prevent reinfection.

Malwarebytes offers the following two main products through a cloud delivery and management platform:

- **Malwarebytes Incident Response** - provides automated endpoint remediation capabilities featuring persistent and non-persistent agent deployments options. Incident Response offers proactive malware sweeping with a forensic timeline view of events.

- **Malwarebytes Endpoint Protection -** provides real-time protection of the endpoint and can replace or augment traditional endpoint solutions. It offers a centralized cloud-management console and an ever-expanding set of signature & signature-less technologies (i.e. web blocking, application hardening, exploit mitigation, behavioral analysis, payload analysis, machine learning, and ransomware mitigation) on a single endpoint agent. It also includes endpoint remediation capabilities.

Malwarebytes Endpoint Security – is an on-premises solution that provides real-time protection of the endpoint via an on-premises management console. It offers similar capabilities to Endpoint Protection, but lacks the machine learning engine and does not leverage a single unified agent on the endpoint.

Malwarebytes products are designed to integrate into a customer's existing security workflow and co-exist with third-party antivirus software such as Symantec, McAfee, Microsoft, and others. Customers may use existing tools from traditional AV vendors or other third-parties like OPSWAT in parallel with Malwarebytes software.

Malwarebytes also offers Endpoint Detection and Response (EDR) detection technology which includes network sandboxing through its Saferbytes acquisition (which handles trojans, ransomware, viruses, and more), Big Data behavioral analysis, isolation, machine learning, and incident response. Malwarebytes relies on unique heuristic rules that can catch multiple hashes with a single rule, thus resulting in a light weight rules database. A single agent is used to deliver remediation, endpoint protection, and EDR capabilities.

STRENGTHS

- Malwarebytes offers both on-premises and cloud-based corporate solutions.

- Malwarebytes provides a single agent platform with the modularity to deliver a broad set of technologies (i.e. remediation, endpoint protection, and more).

- Malwarebytes' cloud management platform streamlines onboarding, scalability, and solution delivery while offering comprehensive visibility and reporting.

- Malwarebytes Endpoint Protection leverages a multi layered defense of web protection, application hardening, exploit mitigation, application behavior monitoring, payload analysis, machine learning, and behavioral monitoring (for ransomware) to protect against all stages of the infection chain, both pre- and post-execution.

- Malwarebytes products are designed to coexist on the same machine as a customer's existing endpoint security software and integrate into their existing security workflow.

WEAKNESSES

- Malwarebytes does not currently offer MDM or EMM capabilities, however, the company does offer security protection for Android-based mobile devices. The addition of MDM or EMM is under consideration as part of the vendor's mid-term roadmap.

- Malwarebytes does not currently offer DLP. However, this is under consideration as part of the vendor's mid-term roadmap.

- Malwarebytes is still best known for its consumer products. It lacks customer awareness within the business market. The company is working to address this.

- Malwarebytes has strong brand awareness with its remediation capabilities, but must shift this perception to being recognized for its endpoint protection capabilities.

SPECIALISTS

PANDA SECURITY

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

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 solutions are entirely cloud-based, endpoint security 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 browsing monitoring, url filtering by category, and antispam and anti-malware protection for Microsoft Exchange. It is available for Windows, macOS, Linux, and Android.

- **Adaptive Defense** – combines in a single agent all the features of Panda EP with Panda's Endpoint Detection and Response (EDR) solution, and managed services. 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 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 available for Windows.

- **Panda Adaptive Defense 360** – combines in a single agent all the capabilities of Panda EPP with all the capabilities of Adaptive Defense. It is available for Windows, macOS, Linux and Android.

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

- *Panda's 100% Attestation Service* – is a managed service that classifies all processes running on endpoints through machine learning techniques and the supervision of Panda Security's malware experts.

- *Panda Adaptive Defense's Threat Hunting and Investigation Service (THIS)* – provides real-time and retrospective intelligence on all the events taking place on an organization's systems to investigate known events, new proof-of-concept attacks and anomalous user, machine, application and tool behavior. The data helps investigators conduct forensic analyses 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.

- *Endpoint telemetry* – 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.

Advanced Reporting Tool (ART) is an optional module that can be used to augment Adaptive Defense and Adaptive Defense 360, to provide detailed information of vulnerable applications installed or running on protected endpoints. The module provides pre-defined queries, dashboards and alerts that provide security and IT insights of 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 Security also provides an easy to use, intuitive administration console, as well as a wide range of APIs and tools that make integration of their solution easy into organizations' existing applications and processes.

STRENGTHS

- Panda Security solutions are entirely cloud-based, making them an attractive choice for SMBs and cloud-ready organizations of all sizes looking for all the benefits of a cloud deployment.

- Panda Security Adaptive Defense 360 combines in a single solution the capabilities of Endpoint Protection Platforms (EPP) and 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 solutions are attractively priced.

WEAKNESSES

- Despite an attractive solution portfolio, Panda Security still lacks visibility in the business security space, particularly in North America.

- Panda Security offers limited DLP capabilities for data at rest through an optional add-on module. Additional capabilities and improved integration from the cloud-based management console are on the roadmap.

- No MDM or EMM capabilities are currently provided.

- Patch Assessment capabilities are currently provided through an its optional module called Advanced Reporting Tool (ART) which is not cloud-based. Vulnerability assessment and patch management from the cloud are on the roadmap for 2018.

ESET, SPOL. S.R.O.

Einsteinova 24
851 01 Bratislava
Slovak Republic
www.eset.com

ESET, founded in 1992, offers cybersecurity products and services for consumers and business users. The company is headquartered in Slovakia, with research, sales and distribution centers in over 200 countries. The company is privately held.

SOLUTIONS

ESET's Endpoint protection solutions include the following components:

- **ESET Remote Administrator** – is a web-based multi-tenant management console that manages all ESET Business Security products. It is available for Windows, Linux as a Virtual Appliance and as a Virtual Machine in Microsoft Azure.

- **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 behavior. It can detect policy violations, anomalies, and can provide detailed information and response options in the event of security incidents. ESET Enterprise Inspector helps discover correlations of otherwise safe processes, files or activities, evaluate them and detect any hidden threats or security weaknesses. It provides multiple options to respond to incidents or suspicious activities.

- **ESET's Threat Intelligence Service** – is ESET's threat reputation network. It uses information gathered from over 100 million sensors and sent to ESET's Cloud Malware Protection System via ESET LiveGrid. It shares actionable threat intelligence with customers by exposing and predicting the next steps of attackers. Additionally, it provides IOCs (IP, URL, file hash) and serves as an automated malware analysis portal. ESET Threat Intelligence Service also provides incident response management via SOCs. It does not require that ESET endpoint or server solutions be deployed on the user's network, which means that it can also be used by non-ESET customers as an additional layer of security to help alert them to imminent malware campaigns or targeted threats. The service can also be

used to provide additional information while investigating APTs and targeted attacks that have already been discovered.

- **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. It offers device control, anti-phishing technology with 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. 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 Remote Administrator which allows configuration of security settings for iOS devices. Administrators can enroll iPhones and iPads, as well as setup security profiles and adjusting device settings, such as: anti-theft, settings for Microsoft Exchange, Wi-Fi, VPN accounts, Passcode, iCloud and more.

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

- **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 (ESET Live Grid reputation technology, Anti-Phishing, Exploit Blocker, and Advanced Memory Scanner), a new antispam engine, and the ability of

selective database on-demand scanning. It features native local quarantine management, process exclusions, support for virtualization (Shared Local Cache, optional snapshot independence) and a Windows Management Instrumentation (WMI) connector.

- **ESET Virtualization Security for VMware vShield** – 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 appliance. It can be managed using ESET Remote Administrator, which allows complete endpoint security management.

STRENGTHS

- ESET Endpoint Security solutions 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 remote administration provides intuitive, easy to use management of all components of the ESET Endpoint Security suite.

- ESET has a global network of installed business solutions that feed information back into the ESET Live Grid Early Warning System, where ESET experts analyze and process the information, then add it to the ESET virus signature databases.

- 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. The administration console, ESET Remote Administrator, is available as a virtual machine in Windows Azure, as well as virtual appliances, for deployment in Private and Public clouds. A cloud-based version of ESET Cloud Administrator is on the vendor's near term roadmap.

- ESET does not provide its own DLP solution. However, it can offer DLP through the ESET Technology Alliance, its partner program of technology providers.

- ESET offers patch management through its ESET Technology Alliance partners.

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

- While ESET offers EDR functionality, through its Enterprise Inspector solution, it does not currently integrate into a common administration console with its endpoint solutions. This integration is on the vendor's roadmap for early 2018.

BITDEFENDER

24 Delea Veche St.
Offices Building A, floor 7, district 2
Bucharest, 024102
Romania
www.bitdefender.com

Bitdefender, founded in 2001, delivers a next-generation security solution through a network of value-added alliances, distributors and reseller partners. The company delivers solutions for businesses and consumers. Bitdefender targets government organizations, large enterprises, SMEs and consumers across more than 150 countries.

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 four GravityZone security packages, as follows:

- **GravityZone Business Security** – allows small customers to protect physical and virtual desktop and servers, combining security with simple centralized management. The solution is available as an on-premises installation, or as a cloud service.

- **GravityZone Advanced Business Security** – 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 also available as an on-premises installation, or as a cloud service.

- **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 as an on-premise installation, or as a cloud service.

- **GravityZone Enterprise Security** – 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. It is aimed at the needs of large enterprises and hybrid infrastructures.

Bitdefender also recently added a Full Disk Encryption module which can managed via the same 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.

Bitdefender also offers **GravityZone Security for MSSPs**, a solution portfolio tailored to meet the needs of Managed Security Service Providers. It offers a multi-tenant management console and simple monthly licensing, along with endpoint protection, threat detection and remediation.

Bitdefender has partnerships with diverse vertical MSP providers, such as Connect Wise, LabTech and Kaseya, to serve multiple segments in the MSP community.

STRENGTH

- Bitdefender's GravityZone Solution is available in all deployment options: on-premises, cloud and hybrid.

- 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.

- All Bitdefender anti-malware technologies are developed in-house. Bitdefender also licenses its technology to 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 provides dedicated solutions for mobile device, data protection and management, supporting Android and iOS platforms. However, mobile device protection is currently available only for 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.

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

F-SECURE

Tammasaarenkatu 7
PL 24
00181 Helsinki
Finland
www.f-secure.com

F-Secure, founded in 1988, offers cyber security products and services for enterprise and consumer customers. The company solutions offer endpoint protection, advanced threat protection and vulnerability management, as well as cyber security assessment, training and consultancy services. F-Secure is based in Finland, and is publicly traded in the country.

SOLUTIONS

F-Secure endpoint protection products are available in two flavors:

- **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 Mac and Windows workstations, including advanced behavior and heuristic analysis, 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 integrated mobile device management with anti-theft.
    - *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, 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.

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, no need for separate solutions with 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

- Reporting remains relatively basic compared to other solutions.

- Discovery of new agents in a network is a manual process for administrators.

- DLP is not included, and F-Secure does not offer any DLP add on.

- F-Secure's on-premises solution is fully integrated with Active Directory, however, integration of its cloud-based solution is still on the roadmap for future release.

- 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. However, these capabilities are on the vendor's near-term roadmap.

- Support for Microsoft Office 365 is not currently available, but is on the roadmap.

- Integration with sandboxing technologies is currently not available for either F-Secure's on-premises or cloud-based solution, but is on the vendor's near term roadmap.

COMODO SECURITY SOLUTIONS, INC.

1255 Broad Street,
Clifton, NJ 07013
www.EnterpriseSolutions@comodo.com

Comodo, well known as a leading SSL certificate authority, provides security solutions aimed at the needs of consumers and businesses. Comodo is headquartered in New Jersey, with offices in Silicon Valley, China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

SOLUTIONS

Comodo **Advanced Endpoint Protection**, offers a fully-integrated combination of Mobile Device, Endpoint Security, RMM, Patch Management, and Inventory Management solutions.

Advanced Endpoint Protection utilizes a lightweight, scalable Default Deny Platform to provide complete protection against zero-day threats. The platform blocks bad files and automatically contains unknown files in a virtual container. All untrusted processes and applications are automatically contained in a secure environment, allowing safe applications the freedom to run while denying malware system access. Comodo's automated containment technology is extremely lightweight, has no CPU dependencies, and is application agnostic. As a result, Advanced Endpoint Protection uses low CPU resources and requires an endpoint footprint of just about 20 MB. Advanced Endpoint Protection is available on a broad range of platforms including Windows, macOS, Linux, Android and iOS.

Comodo's Advanced Endpoint Protection integrates with Comodo's local and cloud-based **Specialized Threat Analysis and Protection (STAP)** engine. This process provides an Accelerated Verdict of unknown files as either known good, or known bad, keeping unknown files in containment for the shortest time necessary.

A variety of new device management capabilities are built into Comodo's **IT and Security Manager (ITSM)**. ITSM secures corporate data through comprehensive application management. ITSM Mobile Device Manager and Inventory Manager allow for the remote provisioning, configuration and control of android, iOS and Windows devices. Applications may also be permitted, blocked or allowed to run inside a secure container. Productivity increases by

disallowing non-critical business applications. ITSM may also perform tasks such as restrict what a user can do on a corporate owned mobile phone, determine which unknown applications are running in containment enterprise-wide, remote wipe a device or set of devices, or identify their geographic location.

A cloud-based engine identifies unknown software applications, quickly moving them to a verdict of known good or known bad. Comodo's local layers, including **VirusScope**, first analyze application behavior and actions running inside or outside of containment, and leverage multiple techniques to determine any malicious intent. **Valkyrie**, Comodo's cloud-based sandboxing technology which provides both static and dynamic analysis, correlates VirusScope's local view of the file's activity with a global view. All files that don't receive a classification from static or dynamic analysis are assigned to a human analyst who issues a definitive verdict within the shortest possible time. This helps reduce false positives and false negatives and while providing an Accelerated Verdict of malware at the endpoint.

Comodo Threat Research Lab (CTRL) leverages one of the largest caches of known bad files (blacklists from its worldwide installed base) helping enterprises to quickly identify known good and known bad applications. The service combines with other capabilities, including web filtering and firewall.

Comodo recently released its Endpoint Detection and Response (EDR) platform which will be offered as a free service to customers.

STRENGTHS

- Comodo's Advanced Endpoint Protection is a highly capable malware detection platforms with a low-footprint available for a broad range of endpoint computing environments.

- Comodo benefits from an extensive worldwide network which feeds threat intelligence in real time to quickly detect and block new threats.

- Comodo can offer enterprise customers a complete portfolio of security solutions comprising web security (Comodo cWatch), firewall (Comodo Dome), sandboxing (Valkyrie), EDR and more.

- Comodo offers full management of Android and iOS devices through in-house developed EMM at no extra charge.

- Comodo offers its own DLP technology.

WEAKNESSES

- Comodo lacks visibility in the enterprise security space. The vendor's strong brand identification with its SSL certificate business can divert attention away from its other IT Security products and services (including Advanced Endpoint Protection).

- While Comodo Advanced Endpoint Protection is available for a broad range of platforms (e.g. Windows, Linux, etc.) it does not currently offer feature parity across all platforms.

- Comodo's DLP technology is available through a separate console.

- Comodo's EDR capabilities are still relatively new and will benefit from more extensive real life tuning.

AVAST

Pikrtova 1737/1a,
Prague 4, Nusle, Postal Code 140 00
Czech Republic
www.avast.com

Avast Business is part of Avast, a provider of digital security products for both consumers and business users. The Avast Business portfolio includes Avast Business Endpoint Protection Solutions and Avast Business Managed Service Solutions.

SOLUTIONS

The Avast Business product portfolio provides a consolidated set of endpoint protection and managed service solutions to secure, simplify, and optimize the IT experience for small and medium-sized businesses (SMBs) worldwide. The Avast Business product portfolio also enables

service providers to deliver customized services that simplify security for SMBs and provides the tools and platforms to efficiently protect customers' networks, devices, data, and people. Avast solutions leverage the threat detection and protection of Avast's global threat detection network, which is fueled by over 400 million device and network endpoints and supported by machine learning and artificial intelligence technologies.

Avast Business Endpoint Protection Solutions include:

- **Avast Business Antivirus –** a full featured endpoint protection solution which includes a four-shield, real-time security defense with file, email, web and behavior shields, antispam, smart scan, sandbox, real site, WiFi Inspector features, and Avast's proprietary CyberCapture technology.

- **Avast Business Antivirus Pro –** includes all features of Avast Business Antivirus plus data protection services to secure Microsoft Exchange and Sharepoint servers, as well as Software Updater for third-party software updates and Data Shredder to permanently delete files.

- **Avast Business Antivirus Pro Plus –** Includes all features of Avast Business Antivirus Pro plus SecureLine VPN, which encrypts all communication, anonymizes browsing, privatizes uploads and downloads, and provides password management and secure browsing to keep employees safe.

- **Avast Business Management Console –** is available as a complement to the endpoint solutions, via cloud or on-premises, it provides a managed AV option that enables IT administrators to manage and set configurations on the AV clients being deployed for customers from a centralized console. The console also features user-defined device groups that enable IT administrators to logically group devices (e.g. 'servers', 'sales', 'PR') for improved display and settings. It also provides reporting on network activity (e.g. viruses found, quarantined, and more).

Avast Business Managed Service Solutions include:

- **Avast Business Managed Workplace –** provides a remote monitoring and management (RMM) platform that enables partners to automate tasks of deploying, managing and monitoring security services in IT environments. Other integrated services include Pro Plus antivirus protection, security assessment, patch management, network management, backup,

monitoring and alerting, reporting, and more.

- **Avast Business CloudCare –** enables Avast partners to remotely support their clients and deploy a robust portfolio of subscription-based cloud security solutions through a cloud-based administration platform. Advanced remote control capabilities, provided at no additional cost, enable administrators to support remote login of any device under management. Partners can implement and manage services such as Pro Plus antivirus, content filtering, online backup, email security services and secure sign on, as well as Pro Plus antivirus.

STRENGTHS

- Avast offers a strong set of high-performance products that are easy to use and meet the security needs of SMBs, as well as the business needs of channel partners.

- Avast leverages an advanced global threat detection network which uses machine learning and artificial intelligence technologies to identify and stop threats in real-time.

- Avast Business offers the same console for both cloud and on-premises solutions. Customers can easily migrate from on-premises to a cloud solution without redeployment and reconfiguration.

- Avast solutions are attractively priced to meet the needs of the SMB market.

WEAKNESSES

- Avast offers only limited separate tools for the removal tools to uninstall previously used security software on a user's machine.

- Patch assessment is currently available only for a limited number of third party applications. A full Windows and third party patch support capability is on the roadmap.

- Mobile device protection is not available in the Endpoint Protection suite of products. It is currently only provided as a service in Managed Workplace, but it is fairly basic and is limited to lock-wipe functionality for Android and iOS.

- Avast solutions do not provide DLP functionality.

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

MICROSOFT

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

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

SOLUTIONS

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 Enterprise Mobility Management (EMM) solution for mobile device management of Windows, Windows Phone, 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.

Starting with Windows 10 and Windows Server 2016 computers, Microsoft is folding most of the endpoint protection directly into the operating system. **Windows Defender Antivirus** is

loaded into the system directly at configuration time, to provide basic anti-malware protection and is complemented by a rich ecosystem of technologies which include (among others):

- **Microsoft SmartScreen** – phishing and malware filtering for Microsoft Edge browsers and Internet Explorer 11 in Windows 10.

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

- **Windows Defender ATP** – cloud-based analytics protection and response service designed to help detect, block and remediate zero-day threats.

Microsoft plans to continually adding new security features and technologies focusing primarily on Windows 10 customers.

STRENGTHS

- Microsoft strong set of security features delivered directly as part of the Windows 10 operating system makes it easier for users and administrators to deal with an ever-changing threat landscape.

- Microsoft System Center and Intune are among the least expensive endpoint security platforms on the market, and many Microsoft customers are able to get the solution at no additional cost as part of their existing licensing agreements.

- 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.

- 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.

WEAKNESSES

- Microsoft's malware detection capabilities are often cited by customers are less accurate than competing security solutions. Most customers tend to deploy System Center or the native Windows 10 anti-malware capabilities as a baseline, but also deploy additional security solution(s) from third party security vendors.

- 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 is focused on building security features into the Windows 10 platform. While this has advantages for Windows users it does little for non-Windows users and for organizations with heterogeneous platform environments.

- Microsoft offers endpoint protection for Mac and Linux as separate add-ons through a partnership with ESET, however, management of these clients is not integrated with System Center.

MATURE PLAYERS

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 multi-layered network and endpoint security solutions for businesses worldwide. Trend Micro offers email, web, and endpoint security platforms as software, appliances, and hosted solutions. 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.

SOLUTIONS

Trend Micro **Smart Protection for Endpoints** offers an integrated defense solution for desktops, laptops, servers and virtualized deployments, with a central management interface. The vendor's XGen Endpoint Security functionality is meant to address complex threats, through machine learning and other techniques to protect against ransomware and advanced attacks. Smart Protection for Endpoints comprises several products, as follows:

- **OfficeScan** – provides endpoint protection for file servers, desktops, laptops, and virtualized desktops. It supports Microsoft Windows, Apple macOS, Google Android, Apple iOS, Windows Mobile, Citrix XenServer, Citrix XenDesktop, and other virtualized endpoints. It delivers malware protection, web security, device control, application control, and reporting. The OfficeScan solution can also be extended with the following plug-ins:

    - *DLP* – content can be scanned for patterns, keywords, file attributes, such as name, size, and kind, and more. While basic device control is built-in to OfficeScan, the DLP plug-in adds more management granularity.

    - *Virtual Desktop infrastructure* – the OfficeScan client can recognize if an agent is running on a virtual or physical endpoint to improve protection methods.

    - *Intrusion Defense Firewall (IDF)* – brings advanced firewall capabilities. The IDF add-on also adds detailed network control for P2P, browsers, IM, streaming, and more.

    - *Mobile security* – management and malware protection is available for Apple iOS, Google Android, Blackberry, and offers capabilities such as provisioning, remote lock and wipe, password and encryption enforcement.

    - *Encryption* – is available as a separate solution offered by Trend Micro.

    - *Apple Mac OS X security* – the Mac protection agent includes pattern-based anti-malware and web reputation protection backed by the Smart Protection Network.

- **Worry-free Business Security Services** – is Trend Micro's cloud-based endpoint security suite aimed at small and mid-size organizations. The solution provides antivirus, anti-phishing, theft prevention and website controls for Windows and Mac workstations, servers,

tablets and mobile devices, Point of Sale (POS) devices, and USB drives.

- **Trend Micro Endpoint Encryption** – prevents data theft and accidental data loss, it can be integrated with OfficeScan and Control Manager.

- **Trend Micro Vulnerability Protection** – provides intelligent virtual patching, blocks exploits and zero-day threats.

- **Trend Micro Control Manager** – offers centralized, single pane of glass administration for endpoint, messaging, collaboration, web, and mobile security.

- **Trend Micro Mobile Security** – provides Mobile Device Management (MDM), Mobile Application Management, Application Reputation Services, and Device Antivirus for Android devices.

STRENGTHS

- Trend Micro offers a broad spectrum of endpoint protection modules that can be deployed together or separately to meet the diverse needs of customers of all sizes.

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

- Trend Micro uses a vulnerability patch block instead of patch remediation, which is faster and easier than deploying patches.

- Although offered as add-ons, Trend Micro offers solid support for virtual desktop infrastructures, encryption, DLP and MDM.

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.

- Device control only provides binary controls without an additional plug-in.
- Reporting only provides relatively basic information to the administrator.
- Encryption is only available as a separate add-on.
- DLP is only available as a separate add-on.
- MDM is a separate add-on.
- Some features, such as the IDF plug-in are not supported on Apple macOS.

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, 2017-2021	Jun. 2017	$3,000.00
Corporate Web Security Market, 2017-2021	Jun. 2017	$3,000.00
Email Market, 2017-2021	Jun. 2017	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2017-2021	Jun. 2017	$3,000.00
Cloud Business Email Market, 2017-2021	Jun. 2017	$3,000.00
Information Archiving Market, 2017-2021	May 2017	$3,000.00
Enterprise Mobility Management Market, 2017-2021	Apr. 2017	$3,000.00
Advanced Threat Protection Market, 2017-2021	Apr. 2017	$3,000.00
Mobile Statistics Report, 2017-2021	Apr. 2017	$3,000.00
Social Networking Statistics Report, 2017-2021	Feb. 2017	$3,000.00
Instant Messaging Market, 2017-2021	Feb. 2017	$3,000.00
Email Statistics Report, 2017-2021	Feb. 2017	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Endpoint Security Market, 2017-2021	Nov. 2017	$3,000.00
Secure Email Gateway Market, 2017-2021	Nov. 2017	$3,000.00
Enterprise Data Loss Prevention Market, 2017-2021	Nov. 2017	$3,000.00

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

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