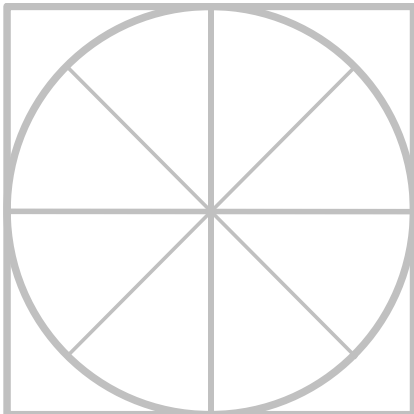


THE RADICATI GROUP, INC.

Endpoint Security - Market Quadrant 2018

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

November 2018



* Radicati Market QuadrantSM is copyrighted November 2018 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 QuadrantsSM 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 QuadrantsSM are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED	3
MARKET SEGMENTATION – ENDPOINT SECURITY	5
EVALUATION CRITERIA.....	7
MARKET QUADRANT – ENDPOINT SECURITY	11
<i>KEY MARKET QUADRANT TRENDS</i>	12
ENDPOINT SECURITY - VENDOR ANALYSIS	12
<i>TOP PLAYERS</i>	12
<i>TRAIL BLAZERS</i>	34
<i>SPECIALISTS</i>	44
<i>MATURE PLAYERS</i>	65

Please note that this report comes with a 1-5 user license. If you wish to distribute the report to more than 5 individuals, you will need to purchase an internal site license for an additional fee. Please contact us at admin@radicati.com if you wish to purchase a site license.

Companies are never permitted to post reports on their external web sites or distribute by other means outside of their organization without explicit written prior consent from The Radicati Group, Inc. If you post this report on your external website or release it to anyone outside of your company without permission, you and your company will be liable for damages. Please contact us with any questions about our policies.

RADICATI MARKET QUADRANTS EXPLAINED

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

1. **Top Players** – These are the current market leaders with products that offer, both breadth and depth of functionality, as well as possess a solid vision for the future. Top Players shape the market with their technology and strategic vision. Vendors don't become Top Players overnight. Most of the companies in this quadrant were first Specialists or Trail Blazers (some were both). As companies reach this stage, they must fight complacency and continue to innovate.
2. **Trail Blazers** – These vendors offer advanced, best of breed technology, in some areas of their solutions, but don't necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for “disrupting” the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.
3. **Specialists** – This group is made up of two types of companies:
 - a. Emerging players that are new to the industry and still have to develop some aspects of their solutions. These companies are still developing their strategy and technology.
 - b. Established vendors that offer very good solutions for their customer base, and have a loyal customer base that is totally satisfied with the functionality they are deploying.
4. **Mature Players** – These vendors are large, established vendors that may offer strong features and functionality, but have slowed down innovation and are no longer considered “movers and shakers” in this market as they once were.
 - a. In some cases, this is by design. If a vendor has made a strategic decision to move in a new direction, they may choose to slow development on existing products.

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

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

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

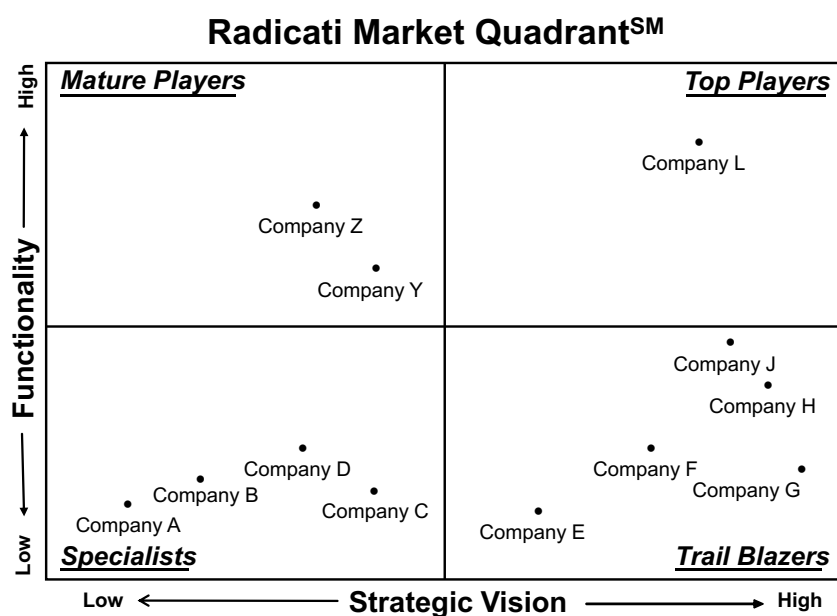


Figure 1: Sample Radicati Market Quadrant

INCLUSION CRITERIA

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

MARKET SEGMENTATION – ENDPOINT SECURITY

This edition of Radicati Market QuadrantsSM 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: *Bitdefender, Carbon Black, Cisco, CrowdStrike, Cylance, ESET, F-Secure, Kaspersky Lab, Matrix42, McAfee, Microsoft, Panda Security, SentinelOne, Sophos, Symantec, Trend Micro, and Webroot.*
- Vendors in this market often target both consumer and business customers. However, this report deals only with solutions aimed at businesses, ranging from SMBs to very large organizations. Government organizations are considered “business/corporate organizations” for the purposes of this report.
- The line between traditional endpoint solutions and next generation endpoint solutions no longer exists as nearly all vendors now offer behavior-oriented solutions which include endpoint detection and response (EDR), sandboxing, advanced persistent threat (APT) protection and more. Increasingly many vendors also offer managed professional services for in-depth threat hunting, forensics and remediation activities.
- Organizations of all sizes, no longer view endpoint security as an isolated discipline affecting only the endpoint but as an integral part of an organization-wide defense posture, where endpoint security shares threat intelligence feeds and policy controls with all other major security components, including firewalls, secure web gateways, secure email gateways, data loss prevention (DLP), and more.
- Adoption of 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 Endpoint Security market is expected to surpass \$6.4 billion in 2018, and grow to over \$13.1 billion by 2022. Figure 1, shows the projected revenue growth from 2018 to 2022.

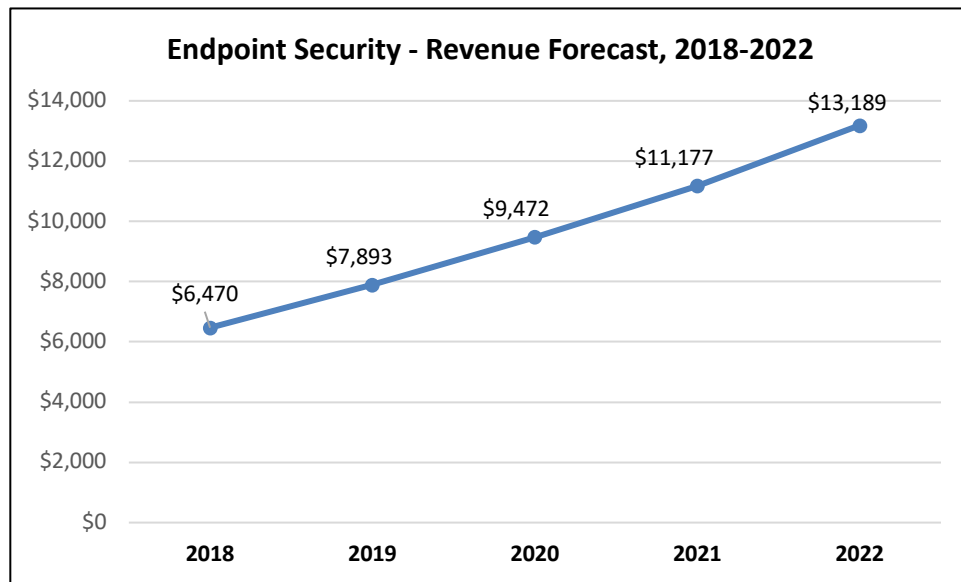


Figure 2: Endpoint Security Market Revenue Forecast, 2018-2022

EVALUATION CRITERIA

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

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

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

Vendors in the *Endpoint Security* space are evaluated according to the following key features and capabilities:

- ***Deployment Options*** – availability of the solution in different form factors, such as on-premises, appliance and/or virtual appliance, cloud-based services, or hybrid.
- ***Platform Support*** – the range of computing platforms supported, e.g. Windows, macOS, Linux, iOS, Android, and others.
- ***Malware detection*** – is usually based on signature files, reputation filtering (proactive blocking of malware based on its behavior, and a subsequent assigned reputation score), and proprietary heuristics. The typical set up usually includes multiple filters, one or more best-of-breed signature-based engines as well as the vendor's own proprietary technology. Malware engines are typically updated multiple times a day. Malware can include spyware, viruses, worms, rootkits, and much more.
- ***Antivirus Removal Tools*** – serve to uninstall previously used security software on a user's machine. Running multiple security solutions on one device can cause conflicts on the endpoints, which can result in downtime.

- **Directory integration** – can be obtained via Active Directory or a variety of other protocols, such as LDAP. By integrating with a corporate directory, organizations can more easily manage and enforce user policies.
- **Firewall** – functionality typically comes with most endpoint security solutions, and offers a more granular approach to network protection, such as blocking a unique IP address. Intrusion prevention systems are also commonly included as a feature in firewalls. Intrusion detection and prevention systems protect against incoming attacks on a network.
- **URL Filtering** – enables organizations to manage and control the websites their employees are allowed to visit. Solutions can block particular websites, or define categories of websites (e.g. gambling) to block, as well as integrate with sandboxing and or threat intelligence feeds to detect and stop malicious URLs.
- **Patch Assessment** – is a common feature included in many endpoint security solutions. It serves to inventory software on protected endpoints to determine if any of the software on the endpoint is out-of-date. It is meant to alert administrators about important software updates that have not yet been deployed.
- **Patch remediation** – lets administrators deploy a missing software update discovered during the patch assessment phase. It should be possible for administrators to deploy software updates directly from the management console.
- **Reporting** – lets administrators view activity that happens on the network. Endpoint Security solutions should offer real-time interactive reports on user activity. Summary views to give an overall view of the state of the network should also be available. Most solutions allow organizations to run reports for events that occurred over the past 12 months, as well as to archive event logs for longer-term access.
- **Web and Email Security** – features enable organizations to block malware that originates from web browsing or emails with malicious intent. These features are compatible with applications for web and email, such as browsers, email clients, and others. These features also help block blended attacks that often arrive via email or web browsing.
- **Device control** – allows control on the use of devices on endpoints, such as USB drives, CD/DVDS, and more. Some solutions provide only basic binary control policies (i.e.

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

- **Encryption** – support for full-disk encryption (FDE) to lock an entire drive, or file-based encryption to lock specific files.
- **Network access control (NAC)** – lets administrators block network access to certain endpoints for various reasons. It is commonly used to bar new endpoints from joining the network that have yet to deploy the organization's security policies.
- **Mobile device protection** – 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.
- **Sandboxing** – does the solution include sandboxing capabilities, or integrate with a third party sandboxing solution for pre- or post-execution malware detection.
- **Advanced Persistent Threat (APT)** – endpoint protection solutions should integrate with APT solutions for real-time threat correlation across the entire customer environment.
- **EDR** – endpoint protection solutions should include Endpoint Detection and Response (EDR) solutions, or integrate with third party EDR solutions.

In addition, for all vendors we consider the following aspects:

- *Pricing* – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a “good value”.
- *Customer Support* – is customer support adequate and in line with customer needs and response requirements.
- *Professional Services* – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

***Note:** On occasion, we may place a vendor in the Top Player or Trail Blazer category even if they are missing one or more features listed above, if we feel that some other aspect(s) of their solution is particularly unique and innovative.*

MARKET QUADRANT – ENDPOINT SECURITY

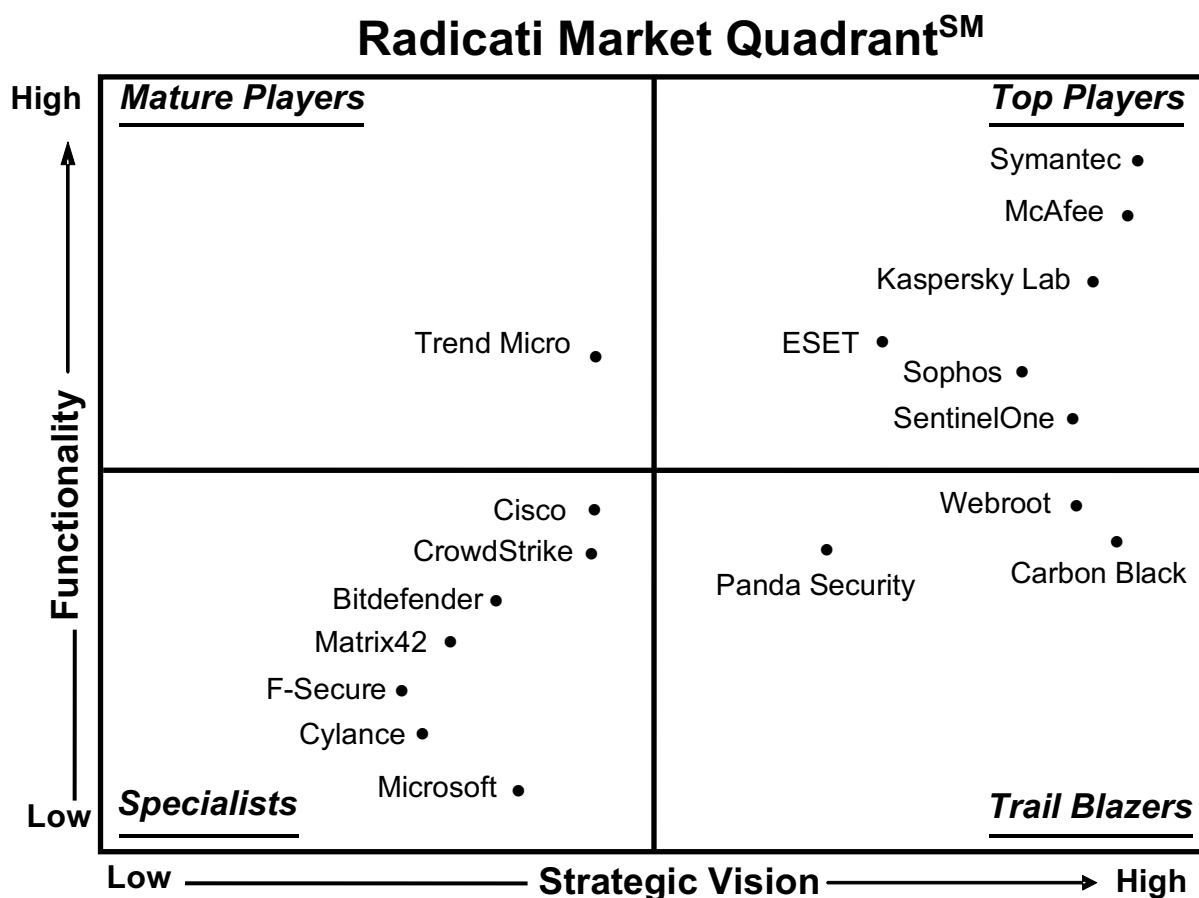


Figure 3: Endpoint Security Market Quadrant, 2018*

* Radicati Market QuadrantSM is copyrighted November 2018 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 QuadrantsSM 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 QuadrantsSM 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, ESET, Sophos, and SentinelOne*.
- The **Trail Blazers** quadrant includes *Webroot, Carbon Black, and Panda Security*.
- The **Specialists** in this market are *Cisco, CrowdStrike, Bitdefender, Matrix42, F-Secure, Cylance, 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 enterprises and consumers. Symantec operates one of the largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. In 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 offers the following endpoint protection solutions:

- **Symantec Endpoint Protection (SEP) 14.2 (On-Premise & Cloud)** – is the latest version of its endpoint protection suite, compatible with the latest versions of Windows, macOS, Linux, VMware ESX, Citrix XenServer, and other virtual machines. It combines the

following capabilities: malware protection, advanced machine learning, behavioral analysis, reputation filtering, exploit prevention, deception, mail security, web security, firewall, device control, antivirus removal tools, recovery tools, reporting, REST APIs, and integration with its intelligent threat cloud capabilities. The solution is managed from a centralized console, which supports the definition of highly granular management policies. Symantec supports hybrid management options (on-premise and cloud) and plans to launch a new fully cloud managed offering, which will deliver artificial intelligence-guided security management, smart application isolation & application control, and extended operating system protections.

- **Symantec Endpoint Protection Cloud (SEP Cloud)** – is an easy-to-use endpoint security solution designed for small and mid-size companies with limited security expertise. It delivers threat protection for traditional endpoints (Windows, macOS), mobile endpoints (iOS, Android), and Windows servers from a single cloud-managed console. While the core security technologies for traditional endpoints remain the same as in SEP, some functionality that is less relevant to small and mid-sized customers has been removed, such as granular policy settings, device and application control, and Linux OS support.
- **Symantec Endpoint Protection Mobile (SEP Mobile)** – is an advanced mobile threat defense solution for iOS and Android devices. It uses predictive technology in a layered approach that leverages crowd-sourced threat intelligence, in addition to both device- and server-based analysis, to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits, with or without an Internet connection. Symantec has recently added integrations with its Web Security Service (WSS) and CloudSOC solutions to extend the full value of those solutions to mobile devices, and also with Symantec Validation and ID Protection (VIP) to ensure multifactor authentication codes are only provided on low-risk devices.
- **Symantec Advanced Threat Protection: Endpoint (ATP:Endpoint)** – enables Endpoint Detection and Response (EDR) with visibility into a file's static file attributes (e.g. keylogging functionality, UI window, and more) and its full behavioral process trace (e.g. detection of fileless attack, PowerShell, Memory Exploit Mitigation, and more). Event details from the 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 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. ATP leverages the SEP agent, and does not require a separate agent.

- **Symantec Endpoint Application Isolation** – is an advanced protection add-on product to SEP using the same, single SEP agent. It discovers applications running on endpoints and classifies apps (and their respective vulnerabilities) based on risk levels. It isolates suspicious applications to prevent them from executing privileged operations (e.g. changing the registry, downloading executables, and more) and it shields the vulnerabilities in commonly used applications (e.g., Browsers, Microsoft Office, Adobe) to prevent cyber attackers from exploiting them.
- **Symantec Endpoint Application Control** – is also an advanced protection add-on to SEP using the same, single SEP agent. It also discovers applications running on endpoints and classifies apps (and their respective vulnerabilities) based on risk levels. It generates smart allow and block lists to prevent unauthorized applications from running. The parameters used include reputation, certificates, publishers, hash, and more). In addition, Application Control offers a simple workflow to manage drift by addressing new applications and handling exceptions.

STRENGTHS

- Symantec offers a single management console across Windows, macOS, Linux, Embedded and Virtual machines, as well as a single integrated agent on the endpoint for seamless management and performance. Hybrid management options (on-premise and cloud) offer additional flexibility to customers.
- SEP offers multi-layered protection powered by artificial intelligence and advanced machine learning to provide prevention, detection and response, as well as deception, application isolation, and application control.
- The level of granularity and flexibility in the management console is higher than many other solutions in the market.

- The firewall functionality included can block unique IP addresses and leverages reputation analysis from Symantec's Global Intelligence Network. It can also do behavioral analysis and apply application controls.
- The level of integration with the Symantec product portfolio (web and email security gateways, threat analytics, multifactor authentication and more) and third-party solutions (e.g. orchestration, automation, SIEM, and others) is higher than most solutions in the market.
- Symantec SEP 14 has built-in Endpoint Detection and Response (EDR) capabilities which are part of the Symantec ATP platform. In addition, Symantec offers Managed EDR, with 24x7 triage, incident response, proactive threat hunting and containment response.
- Given the rich functionality of Symantec's endpoint security platform, it is priced very competitively.

WEAKNESSES

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

SOLUTIONS

McAfee security solutions are built on a security framework that leverages multiple defense layers. Advanced defenses like machine learning analysis, analytics for fileless attacks 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 offers an open security platform that allows multiple McAfee and third-party products to co-exist and share threat intelligence. All security solutions are managed through ePolicy Orchestrator (ePO), which provides a single management system which offers centralized visibility across multiple security products and the entire threat defense lifecycle. McAfee endpoint protection solutions protect Windows, Macs, and Linux systems, as well as iOS and Android mobile devices.

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

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

- **McAfee MVISION Endpoint** – extends the base security built into Windows 10 with enhanced detection for fileless and zero-day threats. It utilizes a lightweight agent and combined policy management, to deliver advanced behavioral analytics for collective defense through a single console.
- **McAfee Endpoint Security** – combines granular controls with layers of integrated capabilities like endpoint detection and response (EDR), and machine learning analysis to provide full-stack protection for Windows, macOS, and Linux systems. In-depth defenses collaborate to inform, analyze and automate responses.
- **McAfee MVISION Mobile** – offers on-device threat detection and protection for iOS and Android mobile devices. It protects against application and network threats, using machine learning algorithms to help identify malicious behavior.
- **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 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. McAfee ePO can be deployed on-premises, or as a cloud service through two options: McAfee ePO on Amazon Web Services (AWS), or a SaaS option called McAfee MVISION ePO.

STRENGTHS

- McAfee offers on-premise, cloud and SaaS management options while retaining a centralized management experience.
- McAfee's Device Security portfolio delivers a broad range of defenses, including advanced defense capabilities needed for zero-day threats, while also integrating and working with third party solutions and native OS security controls.
- McAfee provides advanced threat defenses, like pre-execution and post-execution machine learning analysis and advanced analytics for fileless-based attacks.
- McAfee's Endpoint Security provides a framework which enables IT to easily view, respond to, and manage the threat defense lifecycle.
- McAfee's ePolicy Orchestrator is a powerful, single management console that allows administrators to create and manage policies across most McAfee security solutions.

WEAKNESSES

- Full DLP capabilities are only offered as a separate add-on.
- McAfee solutions are a bit pricier than offerings from competing vendors, but typically offer more features and functionality.
- McAfee solutions currently can only inventory endpoint software however, third party tools must be used to remediate/update software on endpoints.

- Active Response lacks some of the more granular information available with other EDR solutions, however McAfee plans to address this through future releases on its product roadmap.

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 and is privately held.

SOLUTIONS

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

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

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

servers.

- *Total* – in addition to all Select and Advanced capabilities, it protects enterprise perimeter including Email and Web Traffic.

All endpoint security products are managed by the **Kaspersky Security Center**, 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 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 Windows and macOS endpoints, file servers, iOS and Android devices. Kaspersky Endpoint Security Cloud can be extended with Next Generation protection for Microsoft Office 365 email.

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

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

- *Exposure reduction* – with web and email traffic filtering through white and black-listing, as well as rapid cloud lookups.
- *Pre-execution prevention* – endpoint hardening (with patch management and application control), and heuristic analysis based on emulator and machine learning technologies.
- *Post-execution analysis* – including behavior detection, exploit protection, host-based intrusion prevention (HIPS), and reputation services.

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

Kaspersky Lab offers a full-scale Enterprise Security Platform comprising the following products: Endpoint Security, Endpoint Detection and Response, Embedded Systems Security for ATM and PoS protection, Anti-Targeted Attack Platform, Private Security Network, 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 adapts to any IT environment and supports a broad range of systems, encompassing Windows, Linux, macOS, VMware, Citrix, KVM, Microsoft Exchange, Android, iOS.
- Kaspersky solutions rely on its own low footprint, high-performance security technologies. Behavior Detection technology implements a Memory Protection mechanism, which guards system-critical processes and prevents leaking user and administrator credentials.
- The Kaspersky Security Center management console provides a comprehensive management tool that allows organizations to identify all endpoint assets (e.g. physical, virtual, and mobile), as well as conduct fast vulnerability assessments. It can also automatically perform patch remediation, provide a real-time hardware and software inventory, and offers actionable administrator reporting.
- Through the use of Dynamic Whitelisting, Application Control reduces exposure to zero-day attacks by providing control over what software is allowed to run on desktops and servers.
- Kaspersky offers strong support for virtual environments. Kaspersky Hybrid Cloud Security offloads resource intensive anti-malware scans onto a specialized virtual appliance, an approach which places less load on computing resources and helps businesses maintain high virtualization densities and performance.

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

WEAKNESSES

- Kaspersky 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.
- Kaspersky Endpoint Security for Business does not provide content-aware DLP, or support ICAP for integration with third-party DLP solutions.
- Kaspersky Endpoint Security for Business does not support network access control, which prevents administrators from blocking network access to certain endpoints (e.g. new endpoints that have not yet deployed the organization's security policies).
- While the Kaspersky Security Center console currently allows monitoring of Kaspersky's Secure Email Gateway (thus helping integrate visibility across endpoints and email security), management of email security currently requires a separate console. Integration of email security management capabilities is on the roadmap for future releases.

ESET

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

ESET, founded in 1992, offers cybersecurity products and services for enterprises, small and medium businesses and consumers. The company is privately held.

SOLUTIONS

ESET's Endpoint protection solutions include the following components:

- **ESET Endpoint Security for Windows** – is ESET's flagship endpoint security product for Windows. It offers a low footprint, support for virtual environments, and combines reputation-based malware protection with advanced detection techniques enhanced by ESET's machine learning engine, Augur. It offers device control, anti-phishing technology and additional capabilities, such as firewall, web control, botnet protection and more.
- **ESET Endpoint Security for macOS** – is ESET's security product for macOS platforms. Similarly, to its Windows counterpart, it offers a low footprint, support for virtual environments, cross-platform protection, and combines reputation-based malware protection with advanced detection techniques enhanced by ESET's machine learning engine Augur. It offers integrated device control and anti-phishing with additional capabilities, such as firewall, web control, and more.
- **ESET Endpoint Security for Android** – offers reputation-based malware protection, anti-phishing, app control, anti-theft, SMS/call filtering and device security.
- **ESET Mobile Device Management for iOS** – is an integration of the Apple iOS MDM framework with ESET Security Management Center which supports the configuration of security settings for iOS devices. Administrators can enroll iPhones and iPads, as well as setup security profiles and adjust device settings, such as: anti-theft, settings for Microsoft Exchange, 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 LiveGrid® reputation technology for advanced detection techniques. It features support for virtualization (e.g. optional snapshot independence, process exclusions, clustering support), Hyper-V and Network Attached Storage scanning, and a Windows Management Instrumentation (WMI) connector. The product is also available as a VM Extension in Microsoft Azure.
- **ESET Security for Microsoft SharePoint Server** – provides advanced protection for SharePoint servers to protect against malicious uploads and unwanted files. It pays special

attention to ensure the servers are stable and conflict-free to keep maintenance and restarts to a minimum.

- **ESET Mail Security for Microsoft Exchange Server** – combines server malware protection, spam filtering and email scanning. It includes the malware protection technology included in ESET Endpoint solutions (ESET LiveGrid reputation technology, ESET machine learning engine Augur, Anti-Phishing, Exploit Blocker, and Advanced Memory Scanner), new proprietary antispam engine, and the ability of selective database on-demand scanning. It features native local quarantine management, process exclusions, support for virtualization (e.g. optional snapshot independence, hybrid Office365 scanning, clustering support) and a Windows Management Instrumentation (WMI) connector.
- **ESET Virtualization Security for VMware** – is an agentless scanning solution for VMware environments. It streamlines the protection of all virtual machines on the same host by automatically connecting to the vShield and NSX appliance. It can be managed using the ESET Security Management Center.
- **ESET Endpoint Encryption** – provides data encryption, including full-disk encryption (FDE), as well as files, removable media, and email.
- **ESET Security Management Center (ESMC)** – is a web-based single pane of glass multi-tenant management console for all ESET business security products. It runs on Windows, Linux, or as a Virtual Appliance, in Microsoft Azure. It also supports Mobile Device Management (MDM) of Android and iOS devices. ESMC allows single click incident remediation, provides a customizable notification system, automated VDI support, and comes with over 170 built-in reports, as well as the ability to create custom reports.

In addition, ESET provides the following services and solutions:

- **ESET Enterprise Inspector** – is ESET's EDR solution. It combines ESET's detection and protection technologies, threat intelligence and cloud malware protection with other advanced techniques, to monitor and evaluate suspicious processes and behavior. It provides multiple options to respond to incidents or suspicious activities. Monitoring of ESET Enterprise Inspector can be managed via the ESET Security Management Center.
- **ESET Dynamic Threat Defense (EDTD)** – is ESET's managed cloud sandboxing solution,

which provides another layer of protection of ESET Endpoint & Server security solutions. It provides static and dynamic analysis and reputation data, to detect zero-day threats. It is managed by and reports to ESET Security Management Center and directly integrates with ESET Enterprise Inspector, ESET Mail Security solutions and ESET Endpoint solutions.

- **ESET's Threat Intelligence Service** – is ESET's threat reputation network. It relies on information gathered from over 110 million sensors that is sent to ESET LiveGrid. It shares actionable threat intelligence with customers. Additionally, it provides IOCs (IP, URL, file hash) and serves as an automated malware analysis portal. The Threat Intelligence Service is also available standalone.
- **ESET Threat Hunting** – is a security service delivered by ESET cybersecurity experts who perform an on-demand investigation of data, events and alarms generated by the ESET Enterprise Inspector. This may include root cause analysis, forensic investigations and provides actionable mitigation advice.
- **ESET Threat Monitoring** – is a security service delivered by ESET cybersecurity experts who continuously monitor customer network and endpoint security data to provide alerts in real time if suspicious activity requires attention, as well as provides actionable advice on risk mitigation.
- **ESET Manual Malware Analysis** – is an ESET security service which provides full examination and reverse engineering of submitted files. It also provides detailed reports on malicious code behavior with recommendations for prevention, removal and mitigation of attack impact.
- **Forensic Analysis & Consulting** – is a service which provides manual examination of submitted hardware and investigation by ESET Malware Research experts to provide mitigation suggestions and minimize breach aftermath.
- **ESET Cloud Administrator** – is a cloud-based console, offered as a service, for the remote management of customer networks of up to 250 seats.
- **ESET Secure Authentication** – is a mobile-based multi-factor authentication (MFA) solution that protects organizations from weak passwords and unauthorized access. It provides support for iOS, Android and Windows 10 Mobile.

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 management console provides real-time visibility for on-premise and off-premise endpoints as well as full reporting for ESET enterprise-grade solutions from a single pane of glass securely deployed on-premise or in the cloud. It covers desktops, servers, agentless virtual machines and managed mobile devices.
- ESET has a global network of installed business solutions that feed information back into the ESET LiveGrid, its cloud-based reputation system.
- ESET Endpoint Security is well suited to offer protection for companies with heterogeneous environments, e.g. Windows, macOS, Linux, and more.

WEAKNESSES

- ESET products are deployed on-premises. However, the cloud-based administration is available through two solutions: ESET Security Management Center, available as a virtual machine in Windows Azure or as virtual appliances; and ESET Cloud Administrator, for the remote management of organizations with up to 250 seats.
- ESET does not provide its own DLP solution. However, it offers DLP through the ESET Technology Alliance, its partner program.
- The ESET Endpoint Security for macOS does not currently integrate with its ESET Enterprise Inspector, EDR solution. The vendor is working to address this in future releases.
- ESET endpoint solutions are licensed by device, whereas most competitors now license by user (making it easier for users to deploy on multiple devices).
- ESET still lacks market visibility, particularly in North America. The vendor is working to address this.

SOPHOS

The Pentagon Abingdon Science Park

Abingdon

OX14 3YP

United Kingdom

www.sophos.com

Sophos provides IT security and data protection products for businesses on a worldwide basis. Sophos offers security solutions 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. The company is headquartered in Oxford, U.K., and is publicly traded on the London Stock Exchange.

SOLUTIONS

Sophos offers two endpoint security solutions, Intercept X and Sophos Endpoint Protection. They can be deployed separately or combined into a single product and agent, as Intercept X Advanced:

- **Sophos Intercept X Advanced** – combines traditional protection and next-generation endpoint protection into a single solution, with a single agent. It provides signature-less exploit prevention, antivirus, deep learning malware detection, anti-ransomware, HIPS, whitelisting, web security, application control, DLP and all features contained in Sophos Endpoint Protection. Synchronized Security automates incident response and application visibility, via on-going direct sharing of threat, security, and health information between endpoints and the network. Other features include root cause analysis, and advanced system cleaning technology. Sophos Intercept X Advanced with EDR also includes an integrated endpoint detection and response product using the same agent. The solution is centrally managed by Sophos Central. It is available for devices running Windows 7 and above, as well as MacOS (without anti-exploit and deep learning). Intercept X can be deployed on its own, or it can augment endpoint security solutions from other vendors. The included CryptoGuard technology prevents encryption of data by crypto-ransomware. It monitors remote computers and local processes that are modifying documents and other files, and if it determines a process is not legitimate, it is terminated and files are restored to their pre-encryption state. Intercept X for Servers also features deep learning, anti-exploit,

CryptoGuard, anti-ransomware, and more.

- **SophosEndpoint 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:
 - *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. Intercept X Advanced is only available via Sophos Central.

STRENGTHS

- Intercept X can be deployed alongside non-Sophos antivirus products, layering anti-exploit and anti-ransomware on top of existing deployments, or it can replace existing antivirus products.
- Sophos' CryptoGuard technology supports file roll-back capabilities in the event of a ransomware incident.
- Sophos Synchronized Security, delivers protection and context reporting for customers who use Sophos Intercept X and the Sophos XG firewall.
- Sophos solutions are easy to deploy and manage, and don't require extensive training to take advantage of all features and functions.
- Sophos Intercept X Advanced employs a single endpoint agent for combined traditional and next-generation protection, which delivers AV, deep learning, anti-exploit, anti-ransomware, 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 such as DLP, encryption, and more, that are often only available as add-ons in competing endpoint security platforms are standard in Sophos Endpoint Protection.

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.
- Sophos Synchronized Security and EDR technology, would both benefit from further depth of capabilities. Sophos is aware of this and is investing in augmenting both technologies.

- Sophos no longer supports network access control, which prevents administrators from blocking network access to certain endpoints (e.g. new endpoints that have not yet deployed the organization's security policies).
- Reporting features, while adequate, could be improved to support greater customization.
- Sophos Intercept X Advanced is best suited for small and medium sized businesses, looking for ease of use and administration.

SENTINELONE

605 Fairchild Dr.

Mountain View, CA 94043

www.sentinelone.com

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

SOLUTIONS

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

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

SentinelOne provides the following capabilities:

- *Malware detection* – SentinelOne uses proprietary static and behavioral AI engines to prevent, detect, and automatically respond to malware and advanced threats like zero days, ram only malware, and others. The engines work when the agent is online or offline.
- *Directory integration* – SentinelOne automatically integrates with Active Directory for dynamic grouping of agents. It also leverages SAML v2 for administrative logins.
- *Firewall integration* – the SentinelOne behavioral AI functions much like a next-generation HIPS, it monitors network traffic and how that traffic interacts with processes on the endpoint. If malicious behavior is observed, the agent can take action in real time to kill and mitigate the threat. Integration with the native firewalls on Windows, macOS, and Linux to allow for customer blocking rules, is also on the roadmap.
- *Encrypted traffic and URL detection* – SentinelOne provides visibility into encrypted TLS traffic without certificates or proxies. It provides full threat hunting visibility of encrypted traffic directly from the endpoint, with no need to decrypt and re-encrypt traffic as it travels across the network. SentinelOne also monitors all URLs (including TLS / SSL ones) in use on all endpoints in real time and can autonomously kill and mitigate any detected threat.
- *Sandboxing* – the SentinelOne behavior engine provides all the functionality of a sandbox in real time on the endpoint.
- *Patch assessment* – the SentinelOne agents keep real-time inventory of all software installed on all managed agents including install path, version, and patch level. The admin can run a report to compare the software inventory to known vulnerabilities as published by MITRE.
- *Web and email security* – SentinelOne monitors all paths that web or email could use to launch an attack via its Behavioral Engine.

- *Mobile security* – SentinelOne partners with Lookout Security to offer mobile security, as an add-on component at an extra charge. The solution is seamlessly integrated into the SentinelOne management console.
- *Reporting* – the SentinelOne Reporting engine can be customized to return reports in a dynamic fashion. The management server also supports access to all data via API, and publishes an EXCEL plugin for further customized reporting.
- *Alerts* – when a new threat is detected, endpoints are autonomously able to notify other agents, so that all other endpoint devices become immune to the threat.
- *Remediation* – SentinelOne provides one-click automated threat remediation, which can forensically remove any malware that the behavioral AI sees without end user impact. The agent can also see inside TLS and SSL traffic without certificates or network changes. SentinelOne offers the same level of efficacy regardless of whether the agent is online or offline.

SentinelOne also offers more than 300 APIs, that enable its partners and end customers to seamlessly integrate and unify security and IT assets within their existing architectures.

STRENGTHS

- Unlike other next-generation endpoint protection platforms, SentinelOne can be deployed both in the cloud and on-premises.
- SentinelOne offers a fully converged Endpoint Protection Platform (EPP) and Endpoint Detection & Response (EDR) platform in a single lightweight agent. It can run on its own or complement existing AV solutions from other vendors.
- SentinelOne's autonomous endpoint agent provides prevention, detection, and response without any reliance on cloud systems or look up. This allows for faster detection and response to advanced attacks at machine speed.
- SentinelOne's autonomous agent also provides patented remediation technology. This allows the agent to automatically return a system to its pre-threat state without any end user impact

or system downtime.

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

WEAKNESSES

- While SentinelOne has solid integrations and performance, it needs to improve in-product workflows, as well as the quality of integration with partner technology solutions. The vendor is working to address this in future releases.
- While SentinelOne provides patch assessment, it does not currently provide patch remediation (i.e. deployment of missing updates discovered during the patch assessment phase).
- SentinelOne does not offer application whitelisting.
- SentinelOne partners with Lookout Security for mobile security capabilities, however this is provided as an extra cost option.
- SentinelOne does not currently offer content-aware Data Loss Prevention, however, the vendor is considering adding this in the future.

TRAIL BLAZERS

WEBROOT

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

Webroot, founded in 1997, delivers threat intelligence and protection for endpoint networks, for businesses and individuals worldwide, based on cloud and artificial intelligence to stop zero-day threats in real time. The company is headquartered in Colorado, and operates globally across North America, Europe and the Asia Pacific region.

SOLUTIONS

Webroot offers the **SecureAnywhere** suite of business security products for endpoint, mobile, internet DNS filtering, security awareness training and mobile devices. Powered by the **Webroot Threat Intelligence Platform**, a security intelligence platform which continuously collects, analyzes and correlates security information, such as file behavior and reputation, URL and IP reputation, real-time anti-phishing, mobile app reputation and more.

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

- *Web Reputation Protection & Filtering* – is provided through a number of different shields within the Webroot endpoint security solution. The Web Threat Shield uses Webroot's BrightCloud Threat Intelligence Services to block sites with poor reputations and known infected (or malicious) domains.
- *The Identity/Privacy Shield* - secures and isolates the browser (and any other application needed) from the rest of the endpoint. It protects both the user and device.
- *Web search results annotations and safety ratings* - are provided for the main search engines and share why a site was blocked and possible actions for the user.
- *Real-time anti-phishing* - is activated when a user clicks on an email link or attachment that tries to reach the internet. It then relies on machine learning models to determine if access needs to be blocked.
- *Outbound Firewall* – ensures that all outbound TCP/UDP requests and destinations are checked against the Webroot Threat Intelligence Platform so automatic decisions can be made on the users' behalf whether to block or allow the traffic. If a file or process is undetermined, the firewall monitors for data exfiltration.
- *Endpoint Restore and Remediation* – by closely monitoring unknown files and journaling any changes made, the endpoint can be restored to its last known good state.
- *Offline Protection* – uses separate file execution policies to stop attacks when endpoints are not connected to the internet. If an unknown file or process runs when the endpoint is offline, monitoring and journaling are automatically initiated. Upon reconnecting to the internet, any unknown or changed files are analyzed, and if found to be malicious, the endpoint is rolled back to its last known good state.
- *Device control* – using adjustable heuristics settings administrators can lock down common devices, such as USBs and DVDs.
- *Centralized remote management* – available via the Webroot SecureAnywhere web-based management console. Policies can be set for individual users, or groups of users.

- *Global Site Manager* – is MSP-focused , specifically designed to meet the needs of multi-location and multi-site management. It securely integrates with the Webroot Unity API, which allows MSPs to access on-demand real-time threat and other endpoint data to use within their own management, reporting, billing and workflow applications.
- *Automation Ecosystem Integrations* – expanded integrations for MSPs include support for Remote Management and Monitoring (RMM) and Professional Services Automation (PSA) platforms.
- *Dwell Time* – Webroot reports and alerts on the dwell-time of infections, and gives administrators high visibility into infections and details about infection type.
- *Windows 10 Support* – Webroot supports Windows 10, and also covers Microsoft’s Edge browser with web filtering and anti-Trojan protection (ID Shield).
- *Advanced Whitelisting* – offers flexibility in creating file overrides through an enhanced Whitelisting and Blacklisting interface that simplifies the management of application overrides.
- *Fully integrated customer support system* – Webroot offers integrated support within the management console, which makes complex support and ticket number referencing easy.
- *GSM Dashboards* – offer full endpoint dashboard drill down capabilities, allowing administrators to respond to events and investigate anomalies or alerts on the dashboard.
- *Advanced Reporting* – a scheduled reporting engine provides administrators flexibility in generating reports based on their preferences. The Webroot Unity API can also be used to provide highly customized reporting.
- *Unity API* – allows for easy integration into other IT management platforms, including Remote Monitoring and Management (RMM), Professional Services Automation (PSA), customized billing platforms, and internal IS systems. It also can be deployed by MSPs for custom automation of processes, reports and other services.

Webroot SecureAnywhere Business Mobile Protection is a separate solution for mobile devices using Android or iOS. It can be provisioned through the same web-based management console as the Webroot's endpoint security solution.

STRENGTHS

- Webroot SecureAnywhere Business Endpoint Protection has a small installation footprint, since it doesn't require a local threat database.
- System performance requirements are light, allowing the standard agent to be used in both older machines (where less processing power is available), as well as virtual environments, where system resources are also defined.
- Webroot can coexist in an environment with other endpoint security platforms, whereas most other solutions have difficulty operating on a machine with other security software.
- Webroot can work with any browser.
- Management is fully cloud-based, which means there is no need for an on-premises management server.
- Webroot SecureAnywhere Business Endpoint Protection is easy to manage, and offers built-in automatic rollback and auto-remediation of infected endpoints.
- Webroot offers Infection Dwell Time reporting, which alerts and informs administrators of the precise time an endpoint was infected and how long it has taken for Webroot to fully remediate the infection. This can be coupled with forensics and data auditing.

WEAKNESSES

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

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

CARBON BLACK

1100 Winter St.

Waltham, MA 02451

www.carbonblack.com

Carbon Black is a provider of next-generation endpoint security. The company leverages its big data and analytics cloud platform, the Cb Predictive Security Cloud, to enable customers to defend against advanced cyber threats, including malware, ransomware, and non-malware attacks. Carbon Black is publicly traded.

SOLUTIONS

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

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

- **Cb LiveOps** – is a real-time security operations solution that enables organizations to ask questions of all endpoints and take action to instantly remediate issues. It closes the gap between security analysis and IT operations by giving administrators visibility into precise details about the current state of all endpoints, enabling them to make fast decisions to reduce risk.
- **Cb ThreatSight** – is a managed service for Cb Defense that provides a team of Carbon Black security experts who work side-by-side with customer organizations to help validate and prioritize alerts, uncover new threats, and accelerate investigations.
- **Cb Defense for VMware** – is a cloud-delivered security solution for protecting applications deployed in virtualized data centers.

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

STRENGTHS

- Carbon Black offers its solution through a multi-tenant cloud platform, which makes it easier for customers to consume its services while benefiting from broad real-time threat analysis across a wide number of endpoints.
- Carbon Black offers strong prevention based on streams of activity delivered via unfiltered data collection, which enables the Predictive Security Cloud to perform well-informed analysis to detect new attack patterns and deploy new logic to stop malicious activity.
- Carbon Black Predictive Security Cloud, allows customers to choose which product modules are right for their organization. All modules are easily deployed through the same user interface and agent.
- Carbon Black offers an extensible architecture based on open APIs, which allows partners and customers to easily extend and integrate with existing security components.

WEAKNESSES

- Carbon Black Predictive Security Cloud does not currently offer some traditional endpoint protection functionality, such as firewalls, mobile security, or DLP. However, provision of a managed OS firewall is on the vendor's roadmap, and custom integrations are possible through the platform's open APIs.
- Carbon Black Predictive Security Cloud does not currently provide device control. This is on the vendor's roadmap.
- Customers reported that administrative capabilities could be improved through more granular role based access controls to enable different teams within an organization to have access to different capabilities with the Predictive Security Cloud platform.
- The Carbon Black Predictive Security Cloud platform does not yet provide application whitelisting capabilities. Carbon Black currently offers this through its on-premises application control product, Cb Protection.

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 offers a cloud-first approach for endpoint security, which includes traditional endpoint protection (EPP), as well as comprehensive endpoint protection (EPP) complemented by endpoint detection and response (EDR) and managed services for Threat Hunting and Investigation Service. The solutions include:

- **Panda Endpoint Protection (EP)** – provides anti-malware, anti-spyware, anti-phishing protection, protection against zero-day exploits, email and web protection, firewall, IDS/HIDS, device control, disinfection and remediation tools, and more. It is available for Windows, macOS, Linux, and Android.
- **Panda Endpoint Protection Plus (EPP)** – offers all the capabilities of Endpoint Protection, plus it adds web browsing monitoring, URL filtering by category, and antispam and anti-malware protection for Microsoft Exchange. It is available for Windows, macOS, Linux, and Android.
- **Panda Adaptive Defense** – is Panda’s Endpoint Detection and Response (EDR) solution, which is included in their managed service offering. It provides protection against unknown malware and targeted attacks through visibility at the endpoint of users, files, processes, registry, memory and network behavior. This visibility serves to block attacks using 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 EPP capabilities with EDR capabilities, and managed services. It offers protection for desktops, laptops, and servers, delivered from the cloud. It automates the prevention, detection, containment and response against advanced attacks, zero-day malware, ransomware, phishing, memory exploits, and malwareless attacks, inside and outside the corporate network. It includes the 100% Attestation Service and the Threat Hunting and Investigation Service (THIS) at no extra charge.

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

- *The 100% Attestation Service* – is Panda Security’s sandbox service, which monitors and prevents the execution of malicious applications and processes on endpoints.
- *Threat Hunting and Investigation Service (THIS)* – is a managed service which provides real-time and retrospective intelligence on all the events taking place on an organization’s systems to discover unknown threats by investigating anomalous users, machines and applications 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.

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

Panda Security also offers the following complementary add-ons:

- **Advanced Reporting Tool (ART)** – is an optional module that can be used to augment Adaptive Defense and Adaptive Defense 360, to provide detailed information on applications and vulnerabilities. It provides pre-defined queries, dashboards, and alerts that provide insights into what is going on at the endpoints out-of-the-box. Managers can also create their own queries and alerts based on the endpoints telemetry.
- **Panda Patch Management** – is an add-on to Panda Endpoint Protection, Panda Endpoint Protection Plus, Panda Adaptive Defense and Panda Adaptive Defense 360, which manages vulnerabilities in operating systems and third-party applications on Windows endpoints and servers. It provides a reduced attack surface, strengthening preventive capabilities and incident containment.
- **Panda Data Control** – is an add-on to Panda Adaptive Defense and Panda Adaptive Defense 360, which discovers, audits and monitors unstructured sensitive or personal data on endpoints, from data-at-rest to data-in-use and data-in-motion. It can also run real time, free custom searches to find files with specific content.
- **SIEMFeeder** – is a module that sends in real time, events collected on endpoints and enriched with security intelligence, to integrate into SIEM solutions.
- **Aether** – is Panda Security's new, recently redesigned intuitive cloud-based administration console. It provides a wide range of APIs and tools to help integrate 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, Endpoint Detection & Response (EDR) and managed services. The solution is delivered in a light agent connected through cloud-based technologies to deliver prevention, detection and response capabilities.
- Panda Security delivers an easy to use, intuitive administration console with rich, actionable reporting.
- Panda Security offers a Data Control module, which provides an unattended solution to control, monitor and search sensitive data and Personal Information at the endpoints. It doesn't require any additional agent, and its capabilities are integrated into the Panda Adaptive Defense 360 agent.
- Panda Patch Management is a fully integrated module available for any Endpoint Protection Solutions, included Panda Adaptive Defense 360. It manages vulnerabilities, patches, updates and end-of-life application in both operating systems and third-party applications on Windows endpoints and servers.
- Panda Security solutions are attractively priced.

WEAKNESSES

- Panda Security's EDR and 100% Attestation Service capabilities are currently available only for Windows platforms. The vendor is planning to add support for macOS and Linux in the future.
- Panda Security Adaptive Defense 360 does not currently provide encryption capabilities. The vendor has this on its roadmap.

- Panda Security solutions do not support network access control, which prevents administrators from blocking network access to certain endpoints (e.g. new endpoints that have not yet deployed the organization's security policies).
- No MDM or EMM capabilities are currently provided in Panda's Endpoint Security Solutions. The vendor has this on its future roadmap.
- Panda Security currently provides only basic DLP capabilities, through its Data Control module. The vendor plans to enhance this in future releases.
- Despite an attractive portfolio of solutions, Panda Security still lacks visibility in the enterprise security space, particularly in North America.

SPECIALISTS

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, ThreatGrid. In August 2018, Cisco announced the acquisition of Duo Security, a provider of unified access security and multi-factor authentication. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), made up of leading threat researchers.

SOLUTIONS

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

AMP for Endpoints comprises the following key capabilities:

- *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 can close attack pathways and minimize vulnerabilities through proactive protection capabilities.
- *Malware Detection* – AMP for Endpoints provides continuous monitoring and detection of files already on endpoints to help identify malicious behavior and decrease time to detection. If any malicious behavior is detected, it can automatically block the file across all endpoints, and show the security team a 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 is available as a public or private cloud deployment.
- Cisco offers a broad security portfolio, which encompasses threat intelligence, heuristics, behavioral analysis and sandboxing to prevent threats from entering the endpoint. Cisco also recently acquired Duo Security and is in the process of also integrating its unified access security and multi-factor authentication capabilities with its existing portfolio.

- AMP for Endpoints is not merely focused on threat detection, but also provides response capabilities to remediate against threats 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 a thorough network edge to endpoint visibility.
- Cisco offers APIs for their endpoint solutions (as well as Threat Grid and Cisco Umbrella solutions) to integrate with a customer's existing security architecture, as well as other security tools or SIEMs.
- Customers report that AMP for Endpoints is easy to use, and highly efficient in dealing with prevention and remediation.

WEAKNESSES

- Cisco 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.

CROWDSTRIKE

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

CrowdStrike, Inc., a wholly owned subsidiary of CrowdStrike Holdings, Inc., delivers endpoint protection, next-generation antivirus, threat intelligence, incident response, ransomware, and endpoint detection and response (EDR) services to customers in over 170 countries. The company is privately held.

SOLUTIONS

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

It comprises the following components:

- *Falcon Prevent* – which delivers next generation antivirus protection, based on machine learning, as well as exploit blocking, indicator of attack (IOA) behavioral analysis, and more.
- *Falcon Insight* – is its endpoint detection and response (EDR) solution.
- *Falcon Discover* – offers IT hygiene and asset inventory, to help identify unauthorized systems and applications in real-time, as well as remediate issues to improve security posture.

Falcon Endpoint Protection is available in three bundles:

- **Endpoint Detection and Response (EDR)** – which includes Insight and Discover, to deliver comprehensive endpoint visibility that spans detection, response, forensics and IT hygiene. to
- **Endpoint Protection Platform (EPP) Standard Bundle** – which includes Insight and Prevent, and provides detection and response workflows through a unified management

console.

- **Endpoint Protection Platform (EPP) Advanced Bundle** – includes Prevent, Insight, and Discover, to deliver complete endpoint protection that combines prevention, detection and response and IT hygiene through a unified management console and associated workflows.

These solutions can be augmented with **Falcon OverWatch**, a 24/7 managed service dedicated to pro-active threat hunting and detection and response (MDR), and **CrowdStrike Threat Intelligence** its global threat feed providing customized reports and analysis to help predict and prevent zero-day attacks.

STRENGTHS

- CrowdStrike solutions are based on a lightweight agent and managed services cloud architecture, which delivers a uniform set of protection features across Windows, macOS, and Linux platforms.
- CrowdStrike offers an advanced set of next-generation endpoint protection capabilities which combine AV, EDR, advanced threat protection (ATP), with experienced managed services, at an attractive price point, which makes this functionality accessible to organizations which may have the necessary IT resources to run this type of capabilities on their own.
- CrowdStrike solutions are managed through a unified management console which provides workflows for detection and response.

WEAKNESSES

- Customers we spoke with as part of this research, indicated a high rate of false positives. CrowdStrike tends not to participate in third party malware testing, making it difficult to assess its efficacy.
- CrowdStrike does not offer content-aware DLP functionality, or support ICAP for integration with third party DLP vendors.
- CrowdStrike does not provide protection for mobile platforms (i.e. iOS, Android).

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

BITDEFENDER

24 Delea Veche St.

Offices Building A, floor 7, district 2

Bucharest, 024102

Romania

www.bitdefender.com

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

SOLUTIONS

Bitdefender's **GravityZone**, is a business solution that can be installed on-premises or as a cloud solution hosted by Bitdefender, and can provide security for physical, virtual, hybrid cloud and mobile enterprise networks.

The Bitdefender Business Portfolio includes four GravityZone security packages, as follows:

- **GravityZone Business Security** – is aimed at small businesses. It provides protection for physical and virtual desktops and servers, combining security with simple centralized management. It is available as an on-premises installation, or as a cloud service.
- **GravityZone Advanced Business Security** – is aimed at the needs of medium sized businesses. It offers the same services as Business Security, but adds security services for protecting Microsoft Exchange servers and mobile devices. It also includes a feature called Smart Central Scan, which allows Security administrators to offload anti-malware processes to a centralized scanning server, thus lowering the resource consumption on protected systems. The solution is available on-premises or as a cloud service, and can protect

desktops, servers and Microsoft Exchange mailboxes. However, the mobile security (MDM) component is only available for on-premises deployment.

- **GravityZone Elite Suite** – offers the same services as Advanced Business Security but adds two new pre-execution detection layers - HyperDetect and Sandbox Analyzer. Hyperdetect uses specialized local machine models and behavior analysis techniques to detect hacking tools, exploits and malware obfuscation techniques. Sandbox analyzer detonates payloads in a contained virtual environment, analyzes their behavior, reports malicious intent and provides actionable insight. The solution is available on-premises or as a cloud service, and can protect desktops, servers and Microsoft Exchange mailboxes. However, the mobile security (MDM) component is only available for on-premises deployment.
- **GravityZone Ultra Suite** – offers an easy-to-use integrated endpoint protection and EDR solution, which offers prevention, automated detection, investigation and response tools in a single agent, which can be managed through a single console. It provides real-time visibility into endpoints, insight into suspicious activity, alert triage and incident analysis visualization, one-click investigation, IOC lookup, helps track live attacks and lateral movements and enables rapid response for containment and remediation. It is available only as a cloud solution and can protect desktops, servers and Microsoft Exchange mailboxes.
- **GravityZone Enterprise Security** – is aimed at the needs of large enterprises and hybrid infrastructures. It is available only as an on-premise solution and provides security services for protecting physical and virtual desktops and servers, Microsoft Exchange servers and mobile devices.

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

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

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

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

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

STRENGTH

- Bitdefender's GravityZone Solution is available multiple 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.
- Bitdefender's GravityZone Ultra Suite is an integrated endpoint protection and EDR solution, which can be easily deployed by organizations of all sizes.
- Bitdefender tends to receive very high scores in third-party AV testing.
- All Bitdefender anti-malware technologies are developed in-house. Bitdefender 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 offers a Mobile Security (MDM) solution for Android and iOS platforms. However, it is currently available only for its GravityZone on-premises solutions.
- GravityZone Endpoint Security currently provides only basic DLP-like functionality which allows Administrators to define patterns to be checked against scanned SMTP and HTTP traffic.
- While offering highly accurate malware and threat detection solutions, Bitdefender lacks advanced analysis and response capabilities, such as integration with third-party SIEM and/or SOAR tools.
- Bitdefender is still best known for its consumer products and lacks greater visibility in the larger enterprise market. The company is working to address this.

MATRIX42

Elbinger Strasse 7
60487 Frankfurt am Main
Germany
www.matrix42.com
www.egosecure.com

Matrix42, founded in 1992, is a German-based developer of workspace management integration solutions across physical, virtual, mobile and cloud-based environments. In 2018, Matrix42 acquired EgoSecure, a data security company with a broad range of data security products aimed at businesses and consumers. Matrix42 is a privately held company.

SOLUTIONS

Matrix42 Endpoint Security is a modular solution with 20 different data security components available through mix-and-match options, which allows customers to choose only the components they need. Endpoint Security supports Windows and macOS platforms.

It comprises the following key components:

- **Antivirus** – protects endpoints from viruses, trojans, and other malicious software. In addition to traditional signatures, it utilizes advanced detection technologies including heuristics, behavior analysis, updatable behavior patterns, and anti-rootkit technologies. It relies on antivirus technology licensed from BitDefender. The Endpoint Security Management Console can also manage the standard Avira antivirus product.
- **EDR** – through a partnership with EnSilo, a provider of infection detection and remediation technology, Matrix42 offers post infection protection against malware activities. Unwanted harmful behavior, such as suspicious encryption activity or network access can be detected and prevented. A cloud-based machine learning forensic engine ensures malicious behavior prevention. EnSilo supports Windows, macOS X, Linux and a variety of virtual desktop scenarios.
- **Application Control** – offers policy-based restrictions and controls which applications may be executed on an endpoint and which may not. It supports both blacklist and whitelist approaches. Trusted objects can be added based on digital signatures, storage location, hashes, and more.
- **Device Control** – determines the scope of use of devices (e.g. USB sticks, external hard drives, CDs) or interfaces (e.g. Wi-Fi, Firewire, USB, Bluetooth), to prevent data loss and protect against malware intrusion.
- **Secure Audit** – helps visualize data flows and surfaces possible weaknesses in the protection settings. In addition, it can provide forensic information.
- **Full Disk Encryption, Removable Device Encryption, Cloud Storage Encryption** – Full Disk Encryption is provides to safeguard data in case of physical device loss or theft or unauthorized access. It allows encryption of an entire drive, or only sector level encryption. Pre-boot authentication can be strengthened with 2-factor authentication (i.e. through

smartcards, e-tokens, etc.). Local folder Encryption and Network Share encryption act as an additional layer of data protection from unauthorized access in enterprise environments. Removable Device Encryption applies encryption policies to all types of removable media. Cloud Storage Encryption is available to provide on-the-fly encryption of data transfers to DropBox, OneDrive, Google drive, Box, or OwnCloud/NextCloud.

STRENGTHS

- Endpoint Security components are available as modular solutions, with mix-and-match options where customers can choose only the required components.
- The Matrix42 Endpoint Security provides a single agent for protection from internal threats through device control, DLP filtering, and encryption, as well as external threats through antivirus and application control components.
- Matrix42 Endpoint Security delivers strong device control protection capabilities.
- Matrix42 Endpoint Security offers fully integrated incident, change management and remediation processes.
- The Endpoint Security management server can be installed on-premises or in the cloud, hybrid deployment is also available.

WEAKNESSES

- The Matrix42 Endpoint Security macOS client currently offers only basic functionality.
- The Matrix42 Endpoint Security antimalware capabilities are not the vendor's own, but are licensed from Bitdefender.
- Matrix42 currently offers mobile device protection through its Silverback product, but this must be purchased as a separate product. EDR for mobile platforms is on the vendor's roadmap.
- Endpoint Security currently offers a data monitoring component called Insight, which provides a dashboard view on data movement, but it is not currently integrated with the

enSilo EDR functionality.

- Matrix42 Endpoint Security currently only offers post-execution sandboxing functionality.
- URL filtering functionality is not currently available, but is under development for future release.
- Matrix42 lacks market visibility, particularly in North America. The vendor is working to address this.

F-SECURE

Tammasaarencatu 7

P.O. Box 24

00181 Helsinki

Finland

www.f-secure.com

F-Secure, founded in 1988, offers cyber security products and services for enterprise and consumer customers. In the business space, the company offers solutions for endpoint protection, detection and response, advanced threat protection and vulnerability management, as well as red teaming, cyber security assessment, training and consultancy services. In 2018, F-Secure acquired MWR InfoSecurity, a provider of cybersecurity services including managed threat hunting and managed phishing protection. F-Secure is based in Finland, and is publicly traded in the country.

SOLUTIONS

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

- **F-Secure Protection Service for Business** (cloud service) – includes the following key features:
 - *Management Portal (cloud)* – central management portal for deployment, management and monitoring, with integrated mobile fleet management.

- *Computer protection* – security for macOS and Windows workstations, including advanced behavior and heuristic analysis, 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.

F-Secure also offers **F-Secure Rapid Detection & Response** its EDR solution that provides companies lacking large IT or security teams with the advanced threat protection capabilities through professional incident analysis. The EDR solution functions as a single-client and management infrastructure, with the cloud-based endpoint protection product.

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 vendor's roadmap.

- F-Secure's Business Suite on-premises offering lags somewhat behind its cloud-based offering in a number of areas, including: VPN support, iOS, and Android support.
- Support for Microsoft Office 365 is not currently available, but is on the 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 roadmap.

CYLANCE

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

Cylance, founded in 2012, uses artificial intelligence, algorithmic science and machine learning to provide technology and services that offer predictive and preventive protection against advanced threats. Cylance is privately held.

SOLUTIONS

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

- **CylancePROTECT** – is the prevention-focused component of the platform, which delivers malware prevention powered by artificial intelligence, combined with application and script control, memory protection, and device policy enforcement to prevent cyberattacks. The solution does not rely on signatures or stream data to the cloud. It delivers protection against malware, ransomware, file-less malware, malicious scripts, weaponized docs, and other attack vectors. CylancePROTECT supports Windows (32bit or 64bit), macOS, and Linux environments. It is available as a cloud deployment, on-premises (as a virtual appliance), and hybrid. It provides:
 - *Malware Execution Control* – rejects potentially unwanted programs, controls tools used in lateral movement, and more.

- *Device Control* – provides control over the use of USB devices, and prevents exfiltration of data through removable media.
- *Applications Control* – offers device binary lockdown, prevents bad binaries, prevents modification of good binaries, and more.
- *Script Control* – stops unauthorized PowerShell and Active Scripts, stops risky VBA macro methods, weaponized documents, and file-less attacks.
- *Memory Protection* – stops memory misuse and exploitation, halts process injection and more.
- **CylanceOPTICS** – is the endpoint detection and response (EDR) component of the Cylance Security Platform that enables easy root cause analysis, threat hunting and automated threat detection and response. It augments CylancePROTECT prevention without requiring organizations to make significant investments in on-premises infrastructure, stream data to the cloud continuously, or employ highly skilled security resources. It helps organizations automate threat detection and response tasks using existing resources, reducing the workload on security analysts. It also supports Remote Forensic Data Collection, to retrieve advanced sets of forensic data from endpoints, as well as execute scripts, or applications to capture critical information related to suspicious events or security incidents.

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

STRENGTHS

- Cylance is a cloud based security provider, however, all client data is stored locally removing the need for an always-on cloud connection. The vendor also supports on-premises and hybrid deployment options.
- CylancePROTECT has a small footprint compared to other security products.
- CylanceOPTICS (i.e. EDR) is highly intuitive and does not require additional hardware or continuous streaming of data to the cloud, making it one of the more lightweight EDR solutions on the market. It is designed to detect threats as well take responsive action,

without human intervention.

- All Cylance products are managed through a single dashboard.

WEAKNESSES

- Capabilities such as firewall, DLP and Mobile Device Management are only available through partners.
- CylanceOPTICS can do patch assessment, however, it is not an automated process.
- Customers we spoke with as part of this research, indicated a high degree of false positives.
- Cylance could improve market awareness of its security partnerships, as well as make it easier for customers to integrate its products with third party solutions.
- Cylance has lost some visibility and mindshare over the past year, as nearly all traditional endpoint protection vendors have added advanced AI, EDR, and ATP capabilities.

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's endpoint protection solutions consist primarily of Windows Defender, also known as Microsoft System Center Endpoint Protection (SCEP), and Microsoft Intune. SCEP and Intune are available for Windows 8, 9, and 10 platforms. Separate security solutions, available through Microsoft partners, are required for macOS and Linux platforms.

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

SCEP and Intune can both be managed through a single administration console, **Microsoft System Center Configuration Manager (System Center)**, which unifies policy management and device management.

Starting with Windows 10 and Windows Server 2016 computers, Microsoft has folded much of its endpoint protection directly into the operating system, and re-branding the solutions under the **Windows Defender** umbrella name, as follows:

- **Windows Defender Antivirus (AV)** – is loaded into the system directly at configuration time, to provide basic endpoint anti-malware protection.
- **Windows Defender Security Center** – is a local security dashboard.
- **Windows Defender SmartScreen** – provides phishing and malware filtering for Microsoft Edge browsers and Internet Explorer 11 in Windows 10.
- **Windows Defender Application Guard** – helps isolate and sandbox Internet Explorer and Edge browsers.
- **Windows Defender Application Control** – is an application whitelisting solution that can also limit the capabilities of unsigned scripts, as well as enforce established use policies. It overlaps somewhat in functionality with Microsoft App Locker, another application whitelisting technology, which was originally available with Windows 7 but has also been

upgrade for use in Windows 10.

- **Secure Boot** – helps ensure that a device boots using only trusted software.
- **Windows Defender Device Guard** – allows Windows desktops to be locked down to run only trusted apps (similarly to mobile phones).
- **Windows Defender Exploit Guard** – provides exploit mitigation, blocks risky activity, can be used to restrict HTTP and HTTPS connections to malicious hosts, and can be used to restrict access to designated folders.
- **Windows Defender Credential Guard** – prevents unauthorized access to OS credential information.
- **Windows Defender Systems Guard** – protects key OS components starting at boot-time.
- **Windows Defender Advanced Threat Protection ATP** – is a cloud-based EDR analytics protection and response service designed to help detect, block and remediate zero-day threats. It provides protection against phishing, malware and spam attacks. It can offer near real-time protection against high-volume spam campaigns, with DKIM and DMARC support. It also adds protection against “zero-day” attachments and harmful URL link, through real-time behavioral analysis and sandboxing.

Microsoft continues to invest heavily in security and identity protection, with new security features and technologies aimed primarily on Windows 10 customers.

STRENGTHS

- Microsoft offers a strong set of security features for Windows 10 platforms, making it easier for users and administrators to adopt a strong security posture.
- SCEP is included at no additional cost as part of the Microsoft Enterprise Client Access License and Core CAL programs. Microsoft Intune is available as a component of Microsoft’s Enterprise Mobility Suite (EMS), which includes Microsoft Azure Active Directory Premium, and Microsoft Azure Information Protection. This makes SCEP and Intune some of the least expensive endpoint security solutions on the market, as many

customers are able to get the solutions at no additional cost as part of their existing licensing agreements.

- Microsoft offers customers a complete vision which goes well beyond simply endpoint malware protection to encompass Advanced Threat Protection (ATP), as well as information security, data loss prevention and identity management.
- Microsoft continues to invest heavily in security, delivering an impressive ecosystem of solutions that encompass the OS, applications, and services.

WEAKNESSES

- Despite Microsoft's strong investments in security, customers still cite Microsoft's malware detection capabilities as being less accurate than competing security solutions. Most customers tend to deploy Microsoft technologies as a baseline, but also deploy additional security solutions from other vendors.
- In order to benefit from the more advanced security features, customers have to upgrade to Windows 10.
- In order to obtain Microsoft's full range of security solutions, including the EDR component, Windows Defender Advanced Threat Protection (ATP), customers must upgrade to the high-end Windows Enterprise E5 license.
- Microsoft offers a highly complex ecosystem of security solutions involving the operating system and many additional components. However, integrating all these components correctly and maintaining them fully integrated throughout Microsoft's continuous upgrade cycle can be daunting for many organizations.
- Encryption capabilities are only offered via the Microsoft Desktop Optimization Pack.
- Microsoft System Center does not offer granular device control for removable media, CD/DVDs, and other common devices.

- Microsoft offers endpoint protection for Mac and Linux, as separate add-ons through partnerships with third-party vendors, 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 email security solutions for organizations, service providers, and consumers. In the enterprise space, 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 Suite** offers an integrated defense solution for desktops, laptops, servers and virtualized deployments, with a central management interface. The vendor's XGen Endpoint Security functionality, which combines machine learning and other techniques, in order to protect against ransomware and advanced attacks. Smart Protection for Endpoints Suite also integrates with additional solutions, such as Endpoint Detection and Remediation (EDR), and Deep Discovery network sandboxing.

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 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 (VDI) Module* – the OfficeScan client can recognize if an agent is running on a virtual or physical endpoint to improve protection methods.
- *Vulnerability Protection Option* – provides intelligent virtual patching, blocks exploits and zero-day threats on physical and virtual endpoints based on host-based intrusion prevention system (HIPS) technology.
- *Security for Mac Module* – provides malware protection, including pattern-based anti-malware and web reputation protection specifically for Apple macOS.
- *Endpoint Encryption* – ensures data privacy by encrypting data stored on endpoints, including PCs, Macs, DVDs, and USB drives. It provides full-disk encryption, folder and file encryption, as well as removable media encryption.
- *Endpoint Application Control Option* – prevents malicious software or unknown applications from executing on endpoints. Uses correlated threat data to maintain a database of validated, good applications and can be used to lock down systems to run only applications that the organization wants in use.
- *Trend Micro Endpoint Sensor Option* – provides context-aware EDR capabilities, including detailed recording of system-level activities, multi-level search across endpoints using search criteria such as OpenIOC, Yara and others. Detects and analyzes advanced file-less attacks and allows to rapidly respond to avoid compromise.
- **Trend Micro Control Manager** – offers centralized, single pane of glass administration across on-premises, cloud and hybrid deployment models for endpoint, messaging, collaboration, web, and mobile security.
- **Trend Micro Mobile Security** – available for iOS, Android and Windows Phone offers capabilities such as provisioning, remote lock and wipe, password and encryption

enforcement. It includes mobile device threat protection, mobile app management, mobile device management (MDM), and data protection.

- **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.

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, Mobile Security, and EDR.

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.
- Trend Micro was relatively late to market with its EDR capability, which is only available as a separate add-on.
- Encryption is only available as a separate add-on.

- DLP is only available as a separate add-on.
- Mobile Security 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, 2018-2022	Jun. 2018	\$3,000.00
Corporate Web Security Market, 2018-2022	Jun. 2018	\$3,000.00
Email Market, 2018-2022	Jun. 2018	\$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2018-2022	Jun. 2018	\$3,000.00
Cloud Business Email Market, 2018-2022	Jun. 2018	\$3,000.00
Information Archiving Market, 2018-2022	Mar. 2018	\$3,000.00
Unified Endpoint Management Market, 2018-2022	Mar. 2018	\$3,000.00
Advanced Threat Protection Market, 2018-2022	Mar. 2018	\$3,000.00
Email Statistics Report, 2018-2022	Mar. 2018	\$3,000.00
Social Networking Statistics Report, 2018-2022	Feb. 2018	\$3,000.00
Instant Messaging Statistics Report, 2018-2022	Feb. 2018	\$3,000.00
Mobile Statistics Report, 2018-2022	Jan. 2018	\$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Endpoint Security Market, 2018-2022	Nov. 2018	\$3,000.00
Secure Email Gateway Market, 2018-2022	Nov. 2018	\$3,000.00
Enterprise Data Loss Prevention Market, 2018-2022	Nov. 2018	\$3,000.00
Cloud Access Security Broker Market, 2018-2022	Nov. 2018	\$3,000.00

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

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