THE RADICATI GROUP, INC.

Endpoint Security - Market Quadrant 2016


November 2016

Radicati Market QuadrantSM is copyrighted November 2016 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 ................................................................. 2
Market Segmentation – Endpoint Security ........................................................... 4
Evaluation Criteria ............................................................................................... 6
Market Quadrant – Endpoint Security ................................................................. 9
Key Market Quadrant Trends .............................................................................. 10
Endpoint Security - Vendor Analysis .................................................................... 10
   Top Players ....................................................................................................... 10
   Trail Blazers .................................................................................................... 29
   Specialists ........................................................................................................ 45
   Mature Players ................................................................................................. 50

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 a niche product.

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.
MARKET SEGMENTATION – ENDPOINT SECURITY

This edition of Radicati Market Quadrants℠ 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. Key players in this market, include: Bitdefender, Cisco, ESET, F-Secure, IBM, Intel Security, Kaspersky Lab, Microsoft, Sophos, Symantec, VIPRE, Trend Micro, and Webroot.

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

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

- The endpoint security market continues to see growth due to the constant need by organizations to protect against an ever increasing onslaught of malicious threats. The nature of endpoint protection is changing as it moves away from focusing on protecting each single endpoint and more towards integration with broad organization-wide efforts at threat detection, correlation and remediation. Traditional anti-malware techniques based on signatures, heuristics and context analysis are being augmented with sandboxing, and sophisticated threat intelligence.

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

- Cloud based endpoint security solutions are increasingly gaining popularity, as more organizations of all sizes are looking to move most of their IT infrastructure to the cloud. Most traditional endpoint security vendors, today, offer cloud-based options for endpoint security, while a newer generation of vendors offers exclusively cloud-based solutions. Cloud-based deployments are viewed as increasingly attractive not just in terms of cost but more importantly for the advantages they provide in terms of ensuring that updates are distributed.
quickly and effectively across the organization.

- The Endpoint Security market is expected to top $4.6 billion in 2016, and grow to over $5.8 billion by 2020. Figure 1, shows the projected revenue growth from 2016 to 2020.

![Endpoint Security - Revenue Forecast, 2016-2020](image-url)

*Figure 1: Endpoint Security Market Revenue Forecast, 2016-2020*
EVALUATION CRITERIA

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

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

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

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

• Deployment Options – availability of the solution in different form factors, such as on-premises, appliance and/or virtual appliance, cloud-based services, or hybrid.

• Malware detection – is usually based on signature files, reputation filtering (proactive blocking of malware based on its behavior, and a subsequent assigned reputation score), and proprietary heuristics. The typical set up usually includes multiple filters, one or more best-of-breed signature-based engines as well as the vendor’s own proprietary technology. Malware engines are typically updated multiple times a day. Malware can include spyware, viruses, worms, rootkits, and much more.

• Antivirus Removal Tools – serve to uninstall previously used security software on a user’s machine. Running multiple security solutions on one device can cause conflicts on the endpoints, which can result in downtime.

• Directory integration – can be obtained via Active Directory or a variety of other protocols, such as LDAP. By integrating with a corporate directory, organizations can more easily manage and enforce user policies.
• **Firewall** – functionality typically comes with most endpoint security solutions, and offers a more granular approach to network protection, such as blocking a unique IP address. Intrusion prevention systems are also commonly included as a feature in firewalls. Intrusion detection and prevention systems protect against incoming attacks on a network.

• **Patch Assessment** – is a common feature included in many endpoint security solutions. It serves to inventory software on protected endpoints to determine if any of the software on the endpoint is out-of-date. It is meant to alert administrators about important software updates that have not yet been deployed.

• **Reporting** – lets administrators view activity that happens on the network. Endpoint Security solutions should offer real-time interactive reports on user activity. Summary views to give an overall view of the state of the network should also be available. Most solutions allow organizations to run reports for events that occurred over the past 12 months, as well as to archive event logs for longer-term access.

• **Web and Email Security** – features enable organizations to block malware that originates from web browsing or emails with malicious intent. These features are compatible with applications for web and email, such as browsers, email clients, and others. These features also help block blended attacks that often arrive via email or web browsing.

• **Mobile device protection** – a growing number of endpoint security vendors are starting to integrate some form of mobile protection into their endpoint solutions. Some endpoint security vendors offer mobile protection through separate add-ons for Mobile Device Management (MDM) or Enterprise Mobility Management (EMM).

• **Data Loss Prevention (DLP)** – allows organizations to define policies to prevent loss of sensitive electronic information. There is a range of DLP capabilities that vendors offer in their solutions, ranging from simple keyword based detection to more sophisticated Content-Aware DLP functionality.

• **Administration** – should provide easy, single pane-of-glass management across all users and resources. Many vendors still offer separate management interfaces for their on-premises and cloud deployments. As more organizations choose a hybrid deployment model, an integrated management experience that functions across on-premises and cloud is a key differentiator.
In addition, for all vendors we consider the following aspects:

- **Pricing** – what is the pricing model for their solution, is it easy to understand and allows customers to budget properly for the solution, as well as is it in line with the level of functionality being offered, and does it represent a “good value”.

- **Customer Support** – is customer support adequate and in line with customer needs and response requirements.

- **Professional Services** – does the vendor provide the right level of professional services for planning, design and deployment, either through their own internal teams, or through partners.

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

![Radicati Market Quadrant](image)

**Figure 2: Endpoint Security Market Quadrant, 2016**

- Radicati Market Quadrant\textsuperscript{SM} is copyrighted November 2016 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants\textsuperscript{SM} should not be considered an endorsement, but rather a measure of The Radicati Group’s opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants\textsuperscript{SM} are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.
KEY MARKET QUADRANT TRENDS

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

- The Trail Blazers quadrant includes Sophos, Webroot, Bitdefender and VIPRE.

- The Specialists in this market are F-Secure, and Microsoft.

- The Mature Players in this market at this time are Trend Micro and IBM.

ENDPOINT SECURITY - VENDOR ANALYSIS

TOP PLAYERS

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

Symantec, founded in 1982, is one of the largest and best known security companies in the world. In October 2014, Symantec announced that it would split into two independent public traded companies, Symantec focused on security and Veritas focused on information management. In June 2016, it acquired Blue Coat Systems, a provider of network security and threat detection technology

SOLUTIONS

Symantec’s security solutions are powered by the Symantec Global Intelligence Network that offers real-time updates. Symantec Endpoint Protection 14, the latest version of its endpoint protection suite is compatible with the latest versions of Microsoft Windows, Apple Mac OS X, Linux, and VMware ESX, Citrix XenServer, and other virtual machines. It provides the following capabilities:
• **Malware protection** – is provided through multiple layers that include traditional signatures, and advanced detection technologies. Symantec’s next-gen capabilities include Advanced Machine Learning and Memory Exploit Mitigation, which combined with Proprietary components, Insight reputation analysis and Symantec Online Network for Advanced Response (SONAR) behavioral monitoring, offer defense against advanced threats and zero-day attacks.

• **Exploit Protection** – is provided through new Memory Exploit Mitigation technology to help prevent zero-day exploits of vulnerabilities in popular software (browsers, operating systems, enterprise software, and more).

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

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

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

• **Device control** – for USBs is included. Administrators can block files being written to these devices. Options are available to prohibit any software from an external device from running automatically. External storage devices can also be set to read-only. Symantec Endpoint Protection supports a long list of devices that can be blocked, such as disk drives, FireWire, and more. SEP 14 adds device control for managed Mac clients.

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

• **Recovery tools** – are included via the Symantec Endpoint Recovery Tool that can repair infected PCs by creating a rescue disk, or USB drive that can safely remove any malware.
• **Reporting** – for various levels of detail is available. Compliance, risk, application and device control, and others are among the different types of reports that can be generated. Frequency generation of reports can be scheduled.

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

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

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

Symantec also offers **Symantec Endpoint Protection Cloud**, which offers a simplified management console that is deployed as a cloud-based solution. While the core security technologies remain the same, some of the advanced functionality has been removed, such as device and application control, limited virtual machine support, and more.

Symantec endpoint protection enables Endpoint Detection and Response via **Symantec Advanced Threat Protection: Endpoint** with visibility into a file’s static file attributes (e.g. has keylogging functionality, has a UI window, and more) and its full behavioral process trace in order of their observation. Incident response workflows can use this information during investigations and correlate with similar actions on other systems in the environment using ATP:Network and ATP:Email. Symantec ATP supports searching for evidence of compromises (or IOC’s) on the endpoint devices.

**STRENGTHS**

• SEP offers multi-layered protection powered by artificial intelligence and advanced machine learning.
• Symantec Endpoint Protection has many features optimized for virtual environments and embedded machines, which reduce performance impact across both physical and virtual machines.

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

• The firewall functionality included can block unique IP addresses and leverages reputation analysis from Symantec’s Insight network. It can also do behavioral analysis and apply application controls.

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

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

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

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

**Weaknesses**

• Mobile device protection is not included in Symantec Endpoint Protection, but it can be purchased separately from Symantec.

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

• DLP capabilities require a separate add-on.

• Encryption capabilities also require a separate add-on.
Intel Security (McAfee)

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

Intel Security, a business unit of Intel Corporation, delivers security solutions and services for systems, networks, and mobile devices. The vendor offers a wide variety of security products for endpoints, Web, data, data centers, and databases.

Solutions

McAfee security solutions rely on the Global Threat Intelligence (GTI) network, which is powered by a worldwide network of threat sensors and backed by a global research team. GTI offers comprehensive threat intelligence across all threat vectors—file, web, message, and network. McAfee’s Security Connected framework brings together endpoint, network, and cloud security to provide full visibility into emerging threats and the threat landscape.

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

McAfee endpoint security solutions are compatible with Microsoft Windows workstations and servers, Mac, VMware ESX, Linux, Citrix XenDesktop and XenServer, and other virtual platforms. The solutions leverage the McAfee ePolicy Orchestrator (ePO) management console.

• McAfee Endpoint Threat Protection – consists of two new endpoint protection suites with two new optional Endpoint Threat Defense add-ons. Intel Security’s endpoint threat defense offers centralized management, advanced threat protection, detection and correction technologies. Intel Security endpoint threat defense solutions provide:

  o Comprehensive threat defense – collaborative and coordinated protection to help deal with emerging threats such as zero-day and ransomware efficiently.

  o Dynamic Application Containment – protection against patient zero, ransomware threats and helps isolate the network from infection by monitoring and intercepting post-
malicious process actions based on file reputation.

- **Machine Learning Based Protection** – machine learning based malware classification to detect zero-day malware in near real-time, tracing behavior when deemed suspicious and remediating without relying on traditional signatures.

- **Contextual defense** – to expose, hunt, and remediate advanced threats to reduce dwell time and costs.

- **Administration** – a single view for visibility, investigation, and action.

**McAfee Complete Endpoint Protection - Enterprise** – provides a security solution aimed at the advanced needs of large and security-conscious enterprises. It provides hardware-enhanced security against stealthy attacks, behavioral anti-malware, and dynamic whitelisting, in addition to the essential antivirus, antispam, web security, firewall, and intrusion prevention. It is managed through a single endpoint management console which covers all platforms including: smartphones, tablets, Macs, Windows, Linux, UNIX, virtual systems, and servers. The suite also includes McAfee® Endpoint Security 10 which is an intelligent, collaborative framework, enabling endpoint defenses to communicate, share intelligence, and take action against advanced threats. It features the following capabilities:

- **Collaborative anti-malware and antivirus protection** – guards against viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs. A collaborative endpoint defense framework allows multiple technologies to communicate in real time. The protection technologies analyze and collaborate against new and advanced threats blocking them before they impact systems or users.

- **McAfee Global Threat Intelligence** – is built-in to act as a file reputation system for suspicious files.

- **Proactive email and Web security** – scans both inbound and outbound messages for malware and spam and can intercept these before they reach inboxes. Filters can also be set up to block messages containing certain keywords. Built-in McAfee SiteAdvisor Enterprise Plus warns users about malicious websites before they click and allows administrators to block, provide warning, or disallow access to certain websites, ensuring compliance.
Host IPS & Endpoint Firewall – guards against unknown, zero-day threats and new vulnerabilities. It controls desktop applications that can access the network, and helps prevent network-borne attacks and downtime. It supports deployment and management of firewall policies based on location, such as for traveling users, to deliver protection and compliance with regulations.

Comprehensive device control – Monitors and restricts data copied to removable storage devices and media such as USB drives, iPods, Bluetooth devices or DVDs to keep them from leaving company control.

Dynamic application control – serves to block unauthorized applications and code on servers, corporate desktops, and fixed-function devices. It is a centrally managed whitelisting solution, which uses a dynamic trust model and other security features to thwart advanced persistent threats without requiring signature updates or labor-intensive list management.

Mobile Security – is provided through partnerships with AirWatch and MobileIron.

Endpoint Security 10 – offers a cloud-assisted endpoint security strategy by enhancing protection, detection, and correction against advanced threats. It provides a framework for IT to more easily view, respond to, and manage the threat defense lifecycle.

• McAfee Complete Endpoint Protection - Business – delivers security for businesses with up to 2,000 nodes, and includes the following features:

  Intelligent and collaborative anti-malware and antivirus protection – guards against the latest viruses, Trojans, worms, adware, spyware, and other potentially unwanted programs. In addition to malware definitions, McAfee Global Threat Intelligence is built-in to act as a file reputation system for suspicious files.

  Host IPS & Endpoint Firewall – protects against unknown, zero-day threats and new vulnerabilities. It controls desktop applications that can access the network, and helps prevent network-borne attacks and downtime. It supports deployment and management of firewall policies based on location, such as for traveling users, to deliver protection and compliance with regulations.
Web and messaging security – provide content filtering, reporting, and allow setting policies by user, or user group. URL categories can be blocked. Other methods of securing the Web, such as blocking access by time of day, are also available. It helps detect, clean, and block malware from Microsoft Exchange and IBM Domino servers.

Data protection – capabilities are provided to allow deployment of file, folder, and full disk encryption to secure confidential data across PCs, laptops, network servers, and removable media. Also prevents loss of sensitive data by restricting use of removable media. Native encryption for Windows BitLocker or Apple Fire Vault can also be managed by ePO.

McAfee Endpoint Protection for SMB – is designed for small and medium-size businesses. It offers an all-in-one solution that addresses anti-malware, anti-spyware, data, and web security needs. It is available both on-premises and through the cloud. Also included in this solution are mobile security and mobile device management capabilities. The solution can be managed through two management consoles – McAfee ePolicy Orchestrator (ePO), and McAfee ePO Cloud.

McAfee Active Response – is McAfee’s endpoint detection and response (EDR) solution, which offers continuous visibility into endpoints, so customers can identify breaches faster and gain more control over the threat defense lifecycle. Key features include:

- Collectors – help find and visualize data from systems.
- Triggers and persistent collectors – continuously monitor critical events or state change with one set of instructions.
- Reactions – offer pre-configured and customizable actions when triggered, to help more easily target and eliminate threats.
- Centralized management with McAfee ePolicy Orchestrator – leverages a single console for comprehensive security management and automation.

McAfee’s ePolicy Orchestrator (ePO) and ePO Cloud – offer 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. The web-

based single management console unifies control over security and compliance tools from McAfee, as well as third parties.

**STRENGTHS**

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

- McAfee Threat Intelligence Exchange delivers a cohesive framework where security products collectively pinpoint threats and act as a unified threat defense system.

- McAfee’s Endpoint Security 10 provides a framework for IT to more easily view, respond to, and manage the threat defense lifecycle.

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

- McAfee’s ePolicy Orchestrator is a powerful, single management console from which to implement policies, across all McAfee security solutions. It comes with a programming interface that lets administrators create complex policies. It also has a strong partner program, Security Innovation Alliance, where partners can integrate into ePO or their own framework.

- McAfee offers different levels of support packages that can include dedicated specialist support.

- McAfee solutions offer robust Web security controls that can also filter offensive content.

- The email security features offer filtering by keyword, which provides an element of DLP.

- McAfee integrates with Intel hardware features (such as Intel vPro Active Management Technology (AMT)) to enable remote endpoint management when PCs are powered on or off.
WEAKNESSES

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

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

• McAfee solutions, while very complete, can also be somewhat complex to deploy and manage for organizations with limited IT resources, which may therefore not fully leverage the full benefits of the solutions.

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

• In an effort to streamline its offerings, McAfee has retired its cloud-based McAfee SaaS Endpoint Protection Suite.

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

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

Kaspersky Lab is an international group, which provides a wide range of security products and solutions for consumers and enterprise business customers worldwide. The company’s security portfolio includes endpoint protection, as well as specialized security solutions and services to combat evolving digital threats. The company has a global presence with offices in 30 different countries.
Solutions

Kaspersky Endpoint Security for Business (KESB) is a platform, which delivers a broad array of tools and technologies to enable companies to see, control and protect all endpoint devices. It provides comprehensive security and systems manageability for all endpoints – including physical and virtual machines, mobile devices, and file servers.

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 Anti-Malware (for Windows, Mac and Linux), Device Control, Application Control, Web Control, Mobile Device Management (MDM), and Security Management.

- **Advanced** – provides Anti-Malware (for Windows, Mac and Linux), Device Control, Application Control, Web Control, Mobile Device Management (MDM), Data Protection (full disk and file-level Encryption), Systems Management (Patch Management), and Security Management.


Kaspersky Endpoint Security solutions offer support for a broad array of platforms, which include Windows, Linux, Mac, Android, iOS and Windows Phone.

All endpoint security products are managed by the Kaspersky Security Center, which delivers security management and control through a single administrative tool. Kaspersky’s management console allows organizations to identify all endpoint assets (physical, virtual, mobile), conduct fast vulnerability assessments, achieve a real-time hardware and software inventory, and offer actionable reporting.

Kaspersky Endpoint Security Cloud, released in September 2016, is Kaspersky Lab’s cloud-based endpoint security solution. Aimed at small and medium-sized businesses, as well as MSP partners, it offers a cloud-based management solution for securing endpoints, mobile devices and file servers.
In addition, **Kaspersky Security for Virtualization (KSV)** protects servers, desktops and data centers for VMware, Citrix, Microsoft Hyper-V and KVM virtual environments. KSV focuses on optimizing resource use and reducing infrastructure and equipment costs.

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

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

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

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

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


**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 at all times.

- Kaspersky solutions rely on its own multi-layered technologies with pre-execution prevention and proactive detection technologies to provide fast, up to date real-time protection.
• The Kaspersky Security Center management console provides a comprehensive management tool that allows organizations to identify all endpoint assets (physical, virtual, and mobile), as well as conduct fast vulnerability assessments, achieve a real-time hardware and software inventory, and provide clear actionable administrator reporting.

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

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

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

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

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

• Kaspersky lets administrators filter Web traffic by content, a feature that is rare in the Web security controls provided by other endpoint security platforms.

Weaknesses

• Kaspersky Lab has released Kaspersky Endpoint Security Cloud, which is its new cloud-based security solution aimed at small-medium businesses (with less than 1,000 users), and MSPs. However, this is probably a missed opportunity as cloud-based solutions are also increasingly attractive to larger enterprise customers.

• There is still some unevenness in supported feature set across Kaspersky Endpoint Security for Business solutions for Apple Mac OS X, Linux, and Windows platforms.
• Kaspersky’s product for Secure Mail Gateway has a separate management server, which is not integrated with the Kaspersky Security Center console.

**Cisco**

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

Cisco is a leading vendor of Internet communication and security technology. In 2014, Cisco acquired ThreatGRID, which offers a cloud-based malware analysis and on-premise sandboxing appliance. In 2015, Cisco acquired OpenDNS, which offers a cloud-delivered network security service that protects at the DNS layer, and in May 2016, it acquired CloudLock, a cloud access security broker (CASB) platform that extends security to SaaS applications. Cisco’s security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos) which is made up of more than 250 leading threat researchers.

**Solutions**

**Cisco Advanced Malware Protection (AMP) for Endpoints** is a cloud-managed endpoint security solution that can detect, contain, and remediate advanced threats if they get past front-line defenses. It offers coverage for PCs, Macs, Linux, mobile devices and virtual systems.

*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 the ability to automatically detect and block known and emerging threats in real time using both cloud- and system-based technologies that include: big data analytics, machine-learning, fuzzy fingerprinting, a built-in antivirus engine, rootkit scanning, and more. It analyzes unknown files using built-in sandboxing technology and closes attack pathways and minimizes vulnerabilities with proactive protection capabilities.

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

**Malware Response** – AMP for Endpoints provides a suite of response capabilities to contain and eliminate threats across all endpoints. Administrators can search across endpoints using a simple, web-browser based management console. Remediation capabilities come standard with AMP for Endpoints. If a threat is detected, AMP automatically contains and remediates across all of endpoints including PCs, Macs, Linux, and mobile devices.

**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 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 offers a broad security portfolio, which encompasses threat intelligence, heuristics, behavioral analysis and sandboxing to prevent threats from entering the endpoint. The solution also detects threats that may have entered the network and provides response capabilities to remediate across all protected endpoints.

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

- AMP for Endpoints offers protection across PCs, Macs, Linux, mobile devices, virtual environments, as well as an on-premises private cloud option.

- When integrated with Cisco AMP for Networks and other Cisco security solutions, AMP for Endpoints provides network edge to endpoint visibility.

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

Weaknesses

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

**ESET, SPOL. S.R.O.**

Einsteinova 24  
851 01 Bratislava  
Slovak Republic  
[www.eset.com](http://www.eset.com)

Headquartered in Bratislava, Slovakia, ESET has research, sales and distribution centers around the globe and a presence in more than 200 countries worldwide. The company has more than 25 years of experience in network security.

**Solutions**

ESET’s Endpoint protection products include the following components:

- **ESET Remote Administrator 6 (ERA 6)** – is a web-based management console that manages all ESET Business Security products. It provides an intuitive, easy to use web-based interface, and is available for Linux, Windows, as a Virtual Appliance and as a Virtual Machine in Microsoft Azure.
• **ESET Endpoint Antivirus 6 for Windows + ESET Endpoint Security 6 for Windows** – are ESET’s flagship endpoint security products for Windows. They offer a low footprint, support for virtual environments, and combine reputation-based antivirus with advanced detection techniques. ESET Endpoint Antivirus 6 for Windows comes with integrated Device Control and Anti-Phishing technology while ESET Endpoint Security 6 for Windows offers additional capabilities such as Firewall, Web Control, Botnet Protection and more.

• **ESET Endpoint Antivirus 6 for mac OS + ESET Endpoint Security 6 for mac OS** – are ESET’s security products for mac OS and OS X platforms. Similarly, to its Windows counterpart, they offer a low footprint, support for virtual environments, cross-platform protection, and combine reputation-based antivirus with advanced detection techniques. ESET Endpoint Antivirus 6 for mac OS comes with integrated Device Control and Anti-Phishing technology while ESET Endpoint Security 6 for mac OS offers additional capabilities such as Firewall, Web Control, and more.

• **ESET Endpoint Security 2 for Android** – offers reputation-based antivirus, Anti-Phishing, App Control, Anti-Theft, SMS/Call Filtering and Device Security.

• **ESET Mobile Device management for iOS** – integration of the Apple iOS MDM framework with ESET Remote Administrator allows configuration of security settings for iOS devices. Administrators can enroll iPhones and iPads, as well as setup security profiles adjusting device settings such as: Anti-Theft, settings for the Exchange, Wi-Fi, and VPN accounts, Passcode, iCloud and more.

• **ESET File Security 6 for Microsoft Windows Server** – is a lightweight server security product, which integrates with the ESET Live Grid reputation technology with advanced detection techniques previously included in ESET Endpoint solutions. It features support for virtualization (Shared Local Cache, optional snapshot independence, process exclusions, clustering support), Hyper-V and Network Attached Storage scanning and a Windows Management Instrumentation (WMI) connector. The product is also available as a VM Extension in Microsoft Azure.

• **ESET Mail Security 6 for Microsoft Exchange Server** – combines server malware protection, spam filtering and email scanning. It includes the malware protection technology previously included in ESET Endpoint solutions (ESET Live Grid reputation technology, Anti-Phishing, Exploit Blocker, and Advanced Memory Scanner), a new anti-spam engine,
and the ability of selective database on-demand scanning. It features native local quarantine management, process exclusions, support for virtualization (Shared Local Cache, optional snapshot independence) and a Windows Management Instrumentation (WMI) connector.

- **ESET Virtualization Security for VMware vShield** – is an agentless scanning solution for VMware environments. It streamlines the protection of all virtual machines on the same host by automatically connecting to the vShield appliance. It can be managed using ESET Remote Administrator, which allows complete endpoint security management.

**STRENGTHS**

- ESET Endpoint Security offers high performance and high detection rates.

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

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

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

- ESET Endpoint Security is well suited to offer protection for companies with heterogeneous environments, e.g. Windows, Mac, Windows Server, Exchange, SharePoint, Linux Server platforms, and iOS and Android mobile devices.

**WEAKNESSES**

- ESET products are deployed on-premises. ESET Remote Administrator is provided as a virtual machine in Windows Azure, and ESET provides virtual appliances, for deployment in Private and Public clouds. A cloud-based version of ESET Cloud Administrator is planned for early 2017.
• ESET does not provide its own DLP solution. However, it can offer DLP through the ESET Technology Alliance, its partner program of technology providers.

• ESET offers encryption through its DESlock acquisition, which delivers shared-key management technology in a hybrid-cloud architecture. DESlock administration is not currently integrated with ESET Remote Administrator, and is managed through its own remote management console. Full integration with ESET Remote Administrator is planned for late 2017.

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

TRAIL BLAZERS

SOPHOS, LTD.
3 Van de Graaff Drive
Burlington, MA 01803
www.sophos.com

Sophos provides IT security and data protection products for businesses on a worldwide basis. SophosLabs is the R&D division behind the vendor’s antivirus, anti-malware, anti-ransomware, and exploit mitigation research. Sophos offers security solutions such as endpoint and mobile security, enterprise mobility management, encryption, server protection, secure email and web gateways, next-generation firewall and unified threat management (UTM). In 2015, Sophos acquired Reflexion Networks, a provider of cloud based secure email services. The company plans to incorporate these capabilities into Sophos Central, its cloud-based security management platform, which includes endpoint protection, mobile management, server protection, network security and web gateway functionality.

SOLUTIONS

Sophos EndUser Protection offerings protect Microsoft Windows, Apple Mac OS X, Linux, Unix, virtual machines, network storage, Microsoft SharePoint, Microsoft Exchange Server, and mobile devices (iOS, Android and Windows Phone 8). The following capabilities are included:
• **Next Generation Endpoint Protection** – includes malicious traffic detection, exploit prevention, and application reputation to its Endpoint agent. Sophos has launched Intercept X designed to block ransomware, provide signature-less exploit prevention and Root-Cause Analysis. In addition, the company released Security Heartbeat, which delivers Synchronized Security by passing live security information between endpoint agents and the Sophos Next Generation Firewall / UTM.

• **Endpoint Antivirus** – Sophos’s agent includes anti-malware capabilities powered by SophosLabs and 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)** – along with other essential security features such as data control, web protection, encryption and patching, is integrated into the endpoint agent and console, allowing it to identify suspicious behaviors and patterns during execution of processes, thereby detecting and blocking previously unknown malware before damage occurs.

• **Server Lockdown/ whitelisting** – is a server protection product that integrates anti-malware capabilities with the ability to lock down the applications allowed to run and update themselves on a server based on a known whitelist.

• **Web security** – is integrated into the endpoint agent platform and provides live URL filtering, blocks access to malicious or infected websites, and blocks malicious code from downloading to the endpoint. 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. Administrators can set categories to Allow, Block, or Warn to give employees more control if necessary. 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. Administrators can authorize only certain applications to send or receive traffic on open ports. 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 Mac OS X 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. Some of the tools included allow for self-help solutions, such as automated password recovery, to limit help-desk tickets.

- **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 in a business.

- **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. Content transfers can be allowed or blocked on endpoints. Users can authorize a transfer if the feature is enabled, and the action will be recorded in the management console. Sophos DLP also has an enforcement point at the mail gateway, which will enforce the DLP policy by allowing, blocking, encrypting and/or logging content transfers via email.

- **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. The solution has a management window that lets administrators know which machines are missing what updates. Missing patches can be sorted based on a variety of criteria, such as name, vendor, or a Sophos-assigned security threat rating.

- **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.
• **Management** – is accessed via a single interface that can monitor the status of all machines on a network, regardless of platform. Granular detail can be viewed by drilling down on specific items, such as endpoints, in the management interface. Reports can be automatically generated according to a schedule, and emailed to selected recipients. Policy can be implemented on an individual machine or a group of machines. Sophos also provides options to manage endpoints via UTM or a Cloud-based management console.

• **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, which ensures high performance, avoids scan and update ‘storms’ and simplifies management.

• **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, including iOS, Android, Windows Phone 8, and others. Additionally, users can configure device policies and deploy them over-the-air, enforce built-in security features such as passcodes and device encryption, and leverage full loss and theft protection for lost or stolen devices.

• **Mobile Antivirus** – Sophos provides full functionality to protect Android devices without reducing performance or battery life. Using up-to-the-minute intelligence from SophosLabs, apps can be scanned on installation, on demand or on a schedule.

Sophos also offers **Sophos Antivirus for vShield**, which is available separately and provides a centralized, agentless scanning solution for optimal performance in VMware environments.

**Sophos Central** is the company’s new strategy of cloud-enabling its entire portfolio. Sophos Central is hosted by Sophos and currently offers complete endpoint, mobile, web and server protection.

**STRENGTHS**

• Sophos is adding “synchronized security”, through its Security Heartbeat technology, giving better protection and context reporting for customers who use both Sophos Cloud Endpoint and the Sophos XG firewall.
• Sophos solutions are easy to deploy and manage, and don’t require extensive training to take advantage of all features and functions.

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

• SophosLabs, which powers the company’s solutions, is fully integrated, analyzing and correlating data across PC malware, spam, mobile malware, and network threats.

• Sophos provides a choice of management platform; endpoint management is available on-premise, on the web via Sophos Cloud or as part of its unified threat management (UTM) platform.

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

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

• The Web security controls in Sophos EndUser Protection bundles can filter content in addition to malware. Most other vendors usually filter only malware.

• Sophos EndUser Protection includes MDM capabilities at no extra cost.

弱点

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

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

• Reporting features, while adequate, could be improved to support greater customization.
• Sophos EndUser Protection is best suited for small and medium sized businesses, looking for ease of use and administration.

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

Webroot offers a cloud based, real-time Internet threat prevention solution for businesses and consumers. Founded in 1997 and headquartered in Colorado, Webroot operates globally across North America, Europe and the Asia Pacific region.

**SOLUTIONS**

Webroot offers the **SecureAnywhere** suite of security products for endpoints and mobile devices. Webroot threat prevention is 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* – designed to counter unknown malware, it uses Webroot’s correlated threat intelligence to perform continuous file and process analysis, and provides malware detection and prevention, in combination with a lightweight, high performance endpoint agent. By moving intensive malware discovery processing to the cloud, it significantly increases system performance and minimizes local endpoint resource usage and impact on user productivity. Webroot requires zero signatures or definition updating of the endpoint as the Webroot Threat Intelligence Platform makes collective file and process security intelligence instantly available to all customers in real time.
- **Web Protection** – is provided through a number of different shields within the Webroot solution. The Web Threat Shield uses Webroot’s threat intelligence to block sites with poor reputations and known infected or malicious domains. Webroot’s Real-Time Anti-Phishing service is also integrated to stop phishing and spear-phishing. The Identity/Privacy Shield isolates the browser (and any other application needed) from the rest of the endpoint. This technology protects the user and device, so even if there is malicious code already present, sensitive information such as access credentials cannot be stolen.

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

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

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

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

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

- **Global Site Manager** – is an Enterprise and MSP management console specifically designed to meet the needs for multi-location and multi-site management. It is designed to simplify and reduce the operational management overhead associated with complex endpoint deployments. It is also now integrated with the Webroot Unity API, which allows MSPs to access real-time data to use within their own management, reporting, billing and workflow applications.
• **Dwell Time** – Webroot endpoint prevention reports and alerts on the dwell-time of infections, and gives administrators high visibility into infections and details about infection types.

• **Windows 10 Support** – Webroot supports Windows 10, and also covers the new Edge browser with web filtering and anti-Trojan protection (ID Shield).

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

• **Enhanced Web Filtering** – is a new web threat shield capability, where web sites are validated using Webroot’s web categorization and reputation threat intelligence data to ensure safer browsing for end users. Web sites are also checked using the BrightCloud Real Time Anti-Phishing service, which offers real-time site analysis. Search result annotations and safety ratings are also provided, and users will see their returned search results annotated to indicate the likelihood that a site is malicious. Information is also provided on why a site was blocked, and the actions that can be taken after a block has occurred.

• **New customer support system** – Webroot offers integrated support within the management console, which makes complex support and ticket number referencing easy. Tickets can be flagged as private per user account, and there is multilingual support with responses translated into the local language.

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

• **Advanced Reporting** – provides reporting capabilities from a new scheduled reporting engine that provides flexibility in generating reports based upon administrative preferences. The Standard console allows the ability to schedule the generation and emailing of reports without the need to log into the consoles.

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

**Webroot SecureAnywhere Business Mobile Protection** is a separate solution for mobile devices, which currently supports Android and iOS devices (both iPad and iPhone). It can be provisioned through the same web-based management console as the Webroot’s endpoint security solution.

**Strengths**

- The install footprint of Webroot SecureAnywhere Business Endpoint Protection is one of the smallest in the market, 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, while solutions from other vendors often work only with some Internet browsers.

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

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

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

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

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

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

- Webroot does not provide patch assessment and management.

Bitdefender

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

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

Solutions

Bitdefender’s GravityZone, is a business solution that can be installed on premise or cloud hosted by Bitdefender, and can provide security for physical, hybrid cloud and mobile enterprise networks.

The Bitdefender Business Portfolio includes 3 GravityZone security packages, as follows:

- **GravityZone Business Security** – allows small customers to protect physical and virtual desktop and servers, combining security with simple centralized management. The solution is available as an on premise installation, or as a cloud service.
• **GravityZone Advanced Business Security** – offers the same services as Business Security, but adds security services for protecting Microsoft Exchange servers and Mobile devices. It also includes a feature called Smart Central Scan, which allows Security administrators to offload antimalware processes to a centralized scanning server, thus lowering the resource consumption on protected systems. The solution is also available as an on premise installation, or as a cloud service.

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

**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/desktops) since the enforcement point, Bitdefender Enterprise Security Tools (BEST) is common to SVE and Endpoint Security; BEST can operate in full offload, partial offload or traditional local scanning.

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

Partnerships with diverse vertical MSP providers, like Connect Wise, LabTech and Kaseya, allow Bitdefender to serve multiple segments in the MSP community.

**STRENGTHS**

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

• Bitdefender relies on heuristics and machine learning models to keep up with the latest threats. Apart from signatures, it employs B-HAVE technology for heuristics in a virtual
sandbox, ATC (Advanced Threat Control) that permanently monitors running processes for signs of malicious behavior, and Machine Learning Algorithms.

• All Bitdefender antimalware technologies are developed in-house and are licensed to a significant number of OEM partners.

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

WEAKNESSES

• While Bitdefender has increasingly shifted its focus to the Enterprise market, it has at times lagged behind in terms of offering the right level of support for enterprise customers. The vendor is working to address this through the addition of professional services and premium support services.

• Bitdefender provides dedicated solutions for mobile device, data protection and management, supporting Android and iOS platforms. However, mobile device protection is available in GravityZone On-Premises versions only.

• 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.

• Patch Assessment is not currently provided but is on the roadmap for end of Q2 2017. Bitdefender also plans to add remediation capabilities alongside Patch Assessment.
VIPRE (ThreatTrack Security)
311 Park Place Blvd,
Suite #300
Clearwater, FL 33759
www.threattracksecurity.com

VIPRE is an endpoint security solution for small and medium businesses and consumers. VIPRE is a product of ThreatTrack Security, Inc.

Solutions

The VIPRE for Business product portfolio, offers the following three levels of solutions:

- VIPRE Endpoint Security 9.3
- VIPRE Business Premium
- VIPRE Antivirus Business 9.3

- VIPRE Endpoint Security 9.3 – introduced in April 2016, is compatible with Microsoft Windows, Apple Mac OS X, and virtual machines. It has all the capabilities of Business Premium (discussed below) but adds the following capabilities:
  
  o Advanced Active Protection – provides cloud-based security services and behavioral detection to help prevent evasive and prevalent threats, including ransomware, Zero-days and more.

  o Removable Device Control and Encryption – keeps data out of the wrong hands and protects networks from infected USB thumb, external hard drives and other devices.

  o Advanced Browser Protection – protects against exploits and browser-based downloads and provides instant URL lookup in the cloud to get the most up to date protection.

- VIPRE Business Premium – features the following capabilities:

  o VIPRE Roaming Agents – enable IT administrators to easily secure remote offices and off-network machines by installing roaming agents on their endpoints. These VIPRE agents call back to a cloud-based service, ensuring that organizations can manage all of
their endpoints from anywhere through the VIPRE management console without the need for secondary site servers or forcing users to connect to a corporate network via VPN. VIPRE 7.5 allows administrators to have complete visibility into the security status of all endpoints, and that all machines receive the latest virus definition packages.

- **Automated Policy Assignment** – makes endpoint security deployment faster and easier. VIPRE 7.5 automatically identifies the machine type - such as laptop, workstation or server - and operating system environment to apply the appropriate policy for each device. This ensures optimal protection profiles and scan settings, for robust malware defense without impacting user productivity and systems availability.

- **Rapid Scan & Enhanced Scan Customization** – offers a layer of protection for organizations that want to add additional system scans to their scheduled deep scans, or to quickly scan a suspect device for threats. Rapid Scan optimizes scan times by enabling VIPRE to focus on higher-risk files unique to each organization's environment. Enhanced scan customization offers greater flexibility allowing administrators to easily create and manage scans.

- **VIPRE for Hyper-V** – is an add-on service for VIPRE customers. It enables users to deploy VIPRE agents via the hypervisor to deliver optimized malware protection for Hyper-V virtual server environments. VIPRE offers fully integrated security management for Microsoft Windows Server Hyper-V.

- **Malware protection** – is provided via heuristics, traditional signatures, and behavior virtualization. VIPRE uses a combination of its own proprietary threat detection and removal technologies, alongside third-party anti-malware and security software, to offer customers maximum protection.

- **Patch Management** – is seamlessly managed from the VIPRE console. VIPRE customers can automate the deployment of patches across their network, including for the third-party applications most commonly targeted with malware exploits, such as Adobe Flash and Reader, Java, Firefox, Chrome and more. With integrated patch management, administrators do not need to manually update machines or rely on users to update vulnerable software applications every time a patch a released.
o **Mobile Device Management** – is integrated into the console, VIPRE MDM offers antivirus for Android devices and mobile security (such as locating lost devices, password management and remote wipe) for iPads, iPhones and Android devices.

o **Email security** – is included to scan emails for threats. Support is available for Microsoft Outlook, Outlook Express, and Windows Mail, as well as any POP3 or SMTP based email solution. Viruses, phishing attempts, and more are filtered out of messages.

o **Web security** – is offered with web filtering features that can block malicious URLs.

o **Firewall** – capabilities are included to offer inbound and outbound protection and monitoring. The firewall can be configured based on applications, ports, protocols and directions. The included firewall can also integrate with Windows Security Center, and VIPRE automatically reconfigures the Windows firewall upon deployment to enable uninterrupted communication between agents and the management console.

o **Antivirus removal** – tools are included to uninstall unwanted previous versions of antivirus or endpoint protection solutions.

o **Reporting** – can be accessed on-demand or scheduled. Common criteria are available, such as top infected machines, top threats found, and more.

o **Management** – can be conducted centrally from a desktop application. Distributed installations only require one management interface. The console features tabbed browsing that allows for easy navigation when setting and reviewing policies.

- **VIPRE Antivirus Business 9.3** – has all of the same features of Business Premium version, but does not offer patch management, firewall and Web security.

Other new developments include VIPRE Professional Services for dedicated, expert-assisted installation and deployments; full integration with LabTech managed services platform; and the addition of VIPRE Internet Security Pro Small Office to VIPRE’s small office product portfolio (non-centrally managed) to provide advanced protection to small and home-based businesses.
STRENGTHS

• The VIPRE product portfolio is well aimed at the needs of the SMB market with efficient, well designed solutions that are easy to manage and update.

• The VIPRE Endpoint Security 9.3 offers advanced defense against ransomware and provides efficient use and allocation of CPU and RAM usage, providing high-performance endpoint security without slowing down processing on the endpoint.

• Patch management and MDM offer additional layers of security managed from the same console that VIPRE administrators are already familiar with.

• VIPRE’s Security Response team can assist with malware removal on systems that are running VIPRE, all included in the purchase price.

• The Firewall controls included in the premium version offer very granular control.

• Discovery of unprotected computers to ensure that the environment is fully covered.

• Removable device control and encryption.

• VIPRE Endpoint Security helps defend against web-based exploits and with instant URL lookup in the cloud.

WEAKNESSES

• VIPRE security solutions are not available as purely cloud solutions.

• DLP features are not included.

• VIPRE offers basic Mobile Device protection through its Integrated console, however more MDM security features are on the roadmap for future releases.

• VIPRE does not currently offer support for VMWare virtualized environments.
• Directory integration could be improved for easier management and configuration through user-based policy management.

SPECIALISTS

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

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

SOLUTIONS

F-Secure endpoint protection products are available in two flavors: Protection Service for Business a cloud-hosted service, and Business Suite an on-premises product.

Key features of F-Secure Protection Service for Business (cloud service) include:

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

• Computer protection – security for Mac and Windows workstations, including advanced behavior and heuristic analysis, as well as fully integrated patch management.

• Mobile protection – next generation mobile security for iOS and Android devices. Personal VPN (WiFi Security), proactive App and Web protection and integrated mobile device management with anti-theft.
- **Server protection** – comprehensive server security for Windows, Linux and Citrix. Additional SharePoint and Exchange components, with fully integrated patch management.

Key features of F-Secure Business Suite (on-premises offering) include:

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

*Client Security* – multilayered 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 & 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 & third party applications.

**Strengths**

- F-Secure uses a multilayered 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.

• F-Secure offers both a hosted cloud-based solution, as well as an on-premises solution to fit different customer needs.

**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.

• Encryption is not included.

• While F-Secure’s cloud offering Business Suite is fully integrated with Active Directory, integration of Active Directory with F-Secure’s on-premises Protection Service for Business is still on the roadmap for future release.

• F-Secure’s Business Suite on-premises offering lags behind its cloud based offering in a number of key areas including: VPN support, iOS, Android, and Mac support. However, these capabilities are on the vendor’s near-term roadmap.

• Support for Microsoft Office 365 is not currently available but is on the roadmap for 2017.
• 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 future roadmap.

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

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

Solutions

Microsoft System Center Endpoint Protection (SCEP) is Microsoft’s solution for anti-malware and endpoint protection for traditional endpoint devices (laptops, desktops and servers). In addition, Microsoft Intune can be added for mobile device management of Windows, Windows Phone, iOS, and Android. Both can managed through a single administration console, Microsoft System Center Configuration Manager (ConfigMgr), which unifies policy management and device management. It includes the following features:

• Malware protection – to protect against viruses, rootkits, and more. Behavior heuristics and file reputation are used to protect endpoints from malware exposure.

• Rootkit Detection – SCEP offers rootkit detection and remediation.

• Firewall – tools are included to offer direct management of the built-in Windows Firewall and ensure that the firewall is updated and running appropriately to protect against threats in the network layer.

• Patch management – is included and can deploy missing software updates to at-risk endpoints.
• **Software removal** – features are included to remove unwanted older endpoint security software.

• **Management** – is provided through ConfigMgr, which distributes updates and removes software as needed.

• **Reporting** – is also available through ConfigMgr, to give insight into deployment statistics, out-of-date definitions, policy distribution status, and more.

**STRENGTHS**

• Automatic antivirus scanning policies can be created to limit CPU usage to a certain percentage to maintain worker productivity.

• Microsoft offers simple per user licensing for ConfigMgr and Intune. Microsoft Intune is also a component of Microsoft’s Enterprise Mobility Suite (EMS), which includes Microsoft Azure Active Directory Premium, and Microsoft Azure Information Protection.

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

**WEAKNESSES**

• Microsoft’s malware detection capabilities are often cited by customers are less accurate than competing security solutions. Most customers tend to deploy ConfigMgr for configuration and policy management but also deploy an additional security solution from a best-of-breed security vendor.

• Encryption capabilities are only offered via the Microsoft Desktop Optimization Pack.

• Microsoft ConfigMgr does not offer granular device control for removable media, CD/DVDs, and other common devices.
• Microsoft has focused most of its efforts into building security features into the Windows 10 platform. While this has advantages for Windows users it does little for non-Windows users and for organizations with heterogeneous platform environments.

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

**Mature Players**

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

Founded in 1988, Trend Micro provides multi-layered network and endpoint security solutions for businesses worldwide. Trend Micro offers email, web, and endpoint security platforms as software, appliances, and hosted solutions. Its solutions are powered by the cloud-based Trend Micro Smart Protection Network, which brings together threat reporting and analysis based on a worldwide threat assessment infrastructure.

**Solutions**

Trend Micro **Smart Protection for Endpoints** offers an integrated defense solution for desktops, laptops, servers and virtualized deployments, with a central management interface. The solution comprises several products, as follows:

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

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

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

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

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

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

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

**Worry-free Business Security Services** – is Trend Micro’s cloud based endpoint security suite aimed at small and mid-size organizations. The solution provides antivirus, anti-phishing, theft prevention and website controls for Windows and Mac workstations, servers, tablets and mobile devices, Point of Sale (POS) devices, and USB drives.

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

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

**Trend Micro Control Manager** – offers centralized, single pane of glass administration for endpoint, messaging, collaboration, web, and mobile security.
• **Trend Micro Mobile Security** – provides Mobile Device Management (MDM), Mobile Application Management, Application Reputation Services, and Device Antivirus for Android devices.

**STRENGTHS**

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

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

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

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

**WEAKNESSES**

• Device control only provides binary controls without an additional plug-in.

• Reporting only provides relatively basic information to the administrator.

• Encryption is only available as a separate add-on.

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

• MDM is a separate add-on.

• Some features, such as the IDF plug-in are not supported on Apple Mac OS X.

• Trend Micro has been somewhat slow to innovate, through the addition of sandboxing and ATP technologies. The vendor recently released its XGen Endpoint Security functionality which is meant to address complex threats, but this merely catches up with what other vendors have already been providing.
IBM Corporation
1 New Orchard Rd
Armonk, NY 10504
www.ibm.com

IBM is a global technology company that specializes in computers, IT consulting, messaging and collaboration software, and more. IBM’s Endpoint Management solution is built on technology acquired from BigFix (2010) and Trusteer Apex (2013). The malware technology used in IBM Endpoint Manager is licensed from Trend Micro.

Solutions

IBM BigFix (previously known as IBM Endpoint Manager) provides protection for a broad range of platforms including Microsoft Windows, Apple Mac OS X, Microsoft Virtual Server, VMware ESX, and other virtual platforms. It includes the following key features:

- **Malware protection** – is based on Trend Micro’s proprietary Smart Protection Network. Protection is also provided via a cloud-based database that analyzes the reputation of local machine files based on age, type, and more.

- **Web security** – features help block malicious URLs based on the reputation of websites.

- **Email security** – serves to scan incoming messages for malicious URLs and links.

- **Firewall** – tools are included for inbound and outbound network activity. Source or destination IP addresses can be blocked by administrator settings, and location-aware policies can be created.

- **Software removal tools** – are included to uninstall unwanted previously used security software.

- **Patch remediation** – lets administrators deploy patches to managed endpoints. This feature, however, is only available as an add-on to IBM BigFix.

- **Reporting** – offers real-time insight into security and deployment statistics. Additional, in-depth reporting on software usage can be obtained through deployment of an optional
 Endpoint Security - Market Quadrant 2016

module.

- **Mobile** – can be protected with the addition of IBM MaaS360, which supports all leading mobile devices.

- **Data Loss Prevention** – can be optionally added on to the IBM BigFix for Core Protection. Sensitive information can be monitored on email, USB drives, networked drives, and more. Data can be monitored to watch for patterns, administrator-created lists of keywords, or file attributes.

- **Device control** – is available through a DLP add-on. Device ports on endpoints can be disabled. Rules can be set for devices on endpoints based on their serial number, model, or manufacturer.

- **Management** – is performed through a central console. Add-ons to the IBM BigFix (e.g. Data Loss Prevention, or mobile device management) can also be accessed through the same management console.

**IBM Security Trusteer Apex Advanced Malware Protection**, is an augmentation of IBM BigFix designed to protect against unknown, zero-day threats and advanced malware. It combines multiple defense layers with dynamic global intelligence and offers the following features:

- **Credential Protection** – protects users from submitting their credentials to harmful phishing sites. It also allows enterprises to enforce password reuse policies.

- **Exploit Chain Disruption** – stops exploit code from using known or unknown (zero-day) vulnerabilities to write a file to the file system and execute it. Helps protect commonly exploited applications, including browsers, Adobe Acrobat, Adobe Flash, Java and Microsoft Office. It also serves to block the execution of files created from exploitation of vulnerabilities in these applications.

- **Malware Detection and Response** – helps detect and mitigate massively distributed APTs.

- **Lockdown for Java** – prevents high-risk actions by malicious Java applications.
• **Malicious Communication Blocking** – stops malware from communicating with the Internet and restricts untrusted files from executing sensitive operations that can enable external communication, as well as prevents malware from tampering with other application processes.

**STRENGTHS**

• A single IBM BigFix server and console can scale to manage over 250,000 devices across multiple platforms.

• IBM BigFix extends protections for corporate PCs by automating and enforcing the deployment of IBM Trusteer Apex endpoint protection against advanced threats and credentials theft.

• IBM Trusteer Apex utilizes threat research data collected from Trusteer and IBM XForce research teams.

• IBM BigFix provides broad support for virtual machines.

• IBM BigFix offers deep add-on capabilities for DLP, which include features such as pattern matching.

• IBM BigFix has a relatively low footprint on system usage (e.g. RAM usage).

**WEAKNESSES**

• Policy creation is not as simple in IBM BigFix as it is in many competing endpoint security platforms. This is especially true when add-ons are deployed, such as DLP or mobile device protection.

• IBM relies on Trend Micro for its malware protection, which leaves it vulnerable to direction changes by Trend Micro.

• IBM does not offer encryption as part of its solution.
• IBM needs to do more to integrate the management and administration of Core Protection and Trusteer Apex.

• IBM’s solutions require the integration of a number of different add-ons (e.g. mobile protection, DLP, etc.) to realize their full potential. This adds cost and complexity to its solution.
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
- Instant Messaging
- Unified Communications
- Identity Management
- 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, and is headquartered in Palo Alto, CA, with offices in London, UK.

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:

<table>
<thead>
<tr>
<th>Title</th>
<th>Released</th>
<th>Price*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SharePoint Market Analysis, 2016-2020</td>
<td>Jul. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Office 365, Exchange Server and Outlook Market Analysis, 2016-2020</td>
<td>Jul. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Email Market, 2016-2020</td>
<td>Jun. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Cloud Business Email Market, 2016-2020</td>
<td>Jun. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Advanced Threat Protection Market, 2016-2020</td>
<td>Mar. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Enterprise Mobility Management Market, 2016-2020</td>
<td>Mar. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Information Archiving Market, 2016-2020</td>
<td>Mar. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>US Email Statistics Report, 2016-2020</td>
<td>Mar. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Email Statistics Report, 2016-2020</td>
<td>Mar. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Instant Messaging Market, 2016-2020</td>
<td>Feb. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Instant Messaging Growth Forecast, 2016-2020</td>
<td>Feb. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Social Networking Growth Forecast, 2016-2020</td>
<td>Feb. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Mobile Growth Forecast, 2016-2020</td>
<td>Jan. 2016</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>eDiscovery Market, 2015-2020</td>
<td>Dec. 2015</td>
<td>$3,000.00</td>
</tr>
</tbody>
</table>

* Discounted by $500 if purchased by credit card.

Upcoming Publications:

<table>
<thead>
<tr>
<th>Title</th>
<th>To Be Released</th>
<th>Price*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Messaging Market, 2017-2021</td>
<td>Feb. 2017</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>Email Statistics Report, 2017-2021</td>
<td>Feb. 2017</td>
<td>$3,000.00</td>
</tr>
</tbody>
</table>

* Discounted by $500 if purchased by credit card.

All Radicati Group reports are available online at [http://www.radicati.com](http://www.radicati.com).