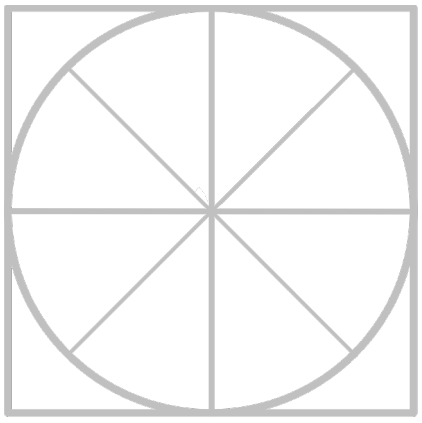
The Radicati Group, Inc.
Palo Alto, CA 94301
Phone: (650) 322-8059
www.radicati.com

THE RADICATI GROUP, INC.

Endpoint Security - Market Quadrant 2015



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

October 2015

TABLE OF CONTENTS

RADICATI MARKET QUADRANTS EXPLAINED 3

MARKET SEGMENTATION – ENDPOINT SECURITY 5

EVALUATION CRITERIA 7

MARKET QUADRANT – ENDPOINT SECURITY 10
- KEY MARKET QUADRANT TRENDS 11

ENDPOINT SECURITY - VENDOR ANALYSIS 13
- TOP PLAYERS 13
- TRAIL BLAZERS 32
- SPECIALISTS 45
- MATURE PLAYERS 55

==========

==========

RADICATI MARKET QUADRANTS EXPLAINED

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

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

    a. Emerging players that are still very new to the industry and have not yet built up much of an installed base. These companies are still developing their strategy and technology.

    b. Established vendors that offer a niche product.

2. ***Trail Blazers*** – These vendors offer cutting edge technology, but have not yet built up a large customer base. With effective marketing and better awareness, these companies hold the power to dethrone the current market leaders. "Trail blazers" often shape the future of technology with their innovations and new products designs.

3. ***Top Players*** – These are the current leaders of the market, with products that have built up large customer bases. 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 product innovation, or else they'll be replaced by the next generation of "trail blazers."

4. ***Mature Player*** – These vendors have large, mature installed bases of customers, but no longer set the pace for the rest of the industry. These vendors are no longer considered "movers and shakers" like 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, it may slow development on one product line and start another.

b. In other cases, a vendor may simply become complacent as a top vendor and be out-developed by hungrier "trail blazers" and other top players.

c. Companies in this stage either find new life and revive their R&D, moving back into the "top players" segment, or else they slowly fade away as legacy technology.

Figure 1, below, shows a sample Radicati Market Quadrant[SM]. As a vendor continues to develop its product, it will move horizontally along the "x" axis. As market share changes, vendors move vertically along the "y" axis. It is common for vendors to move between quadrants over the life of a product, as their products improve and market requirements evolve.

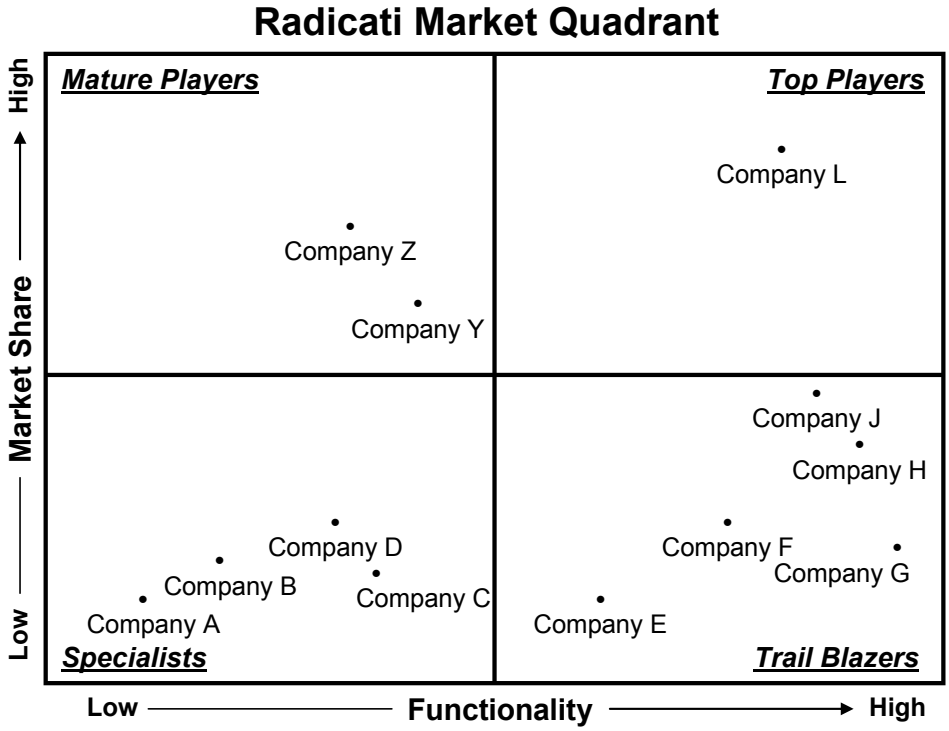


Figure 1: Sample Radicati Market Quadrant[SM]

- ***Functionality*** – is rated from 1 to 10, with 10 being the highest, and 1 – the lowest.

- ***Market Share*** – is assigned according to the company's ranking in our latest annual reports, based on its user Installed Base (e.g. the company with the largest installed base market share is number 1, the one with the second largest installed base market share is number 2, etc.).

MARKET SEGMENTATION – ENDPOINT SECURITY

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

- **Endpoint Security** – are appliances, software, cloud services, and hybrid solutions that help to secure and manage endpoints for business organizations of all sizes. The key features of endpoint security solutions are anti-virus and malware protection, web security, email security, firewall functionality, and much more. Key players in this market, include: *Cisco, ESET, F-Secure, IBM, Intel Security, iSheriff, Kaspersky Lab, Microsoft, Panda Security, Sophos, Symantec, ThreatTrack Security, Trend Micro, Webroot,* and others.

- 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 strong growth driven by the need by organizations of all sizes to protect against a growing range of malware threats. Malware penetration is a huge liability for organizations. Antivirus definitions, heuristic scanning, and other protection methods are included in endpoint security solutions to help guard against the risk of malware infections.

- Web and email security are typically included in endpoint security solutions. Web and email security are still seen as the prevalent vectors for malware penetration. While organizations rely on Endpoint Security solutions for this protection, many organizations also choose to deploy additional separate web and email protection solutions to augment their protection.

- Endpoint security solutions often provide the basis for a unified corporate security deployment that includes encryption, DLP, web security, email security, mobile device management (MDM), and more. Some vendors are able to offer all of this functionality in one deployment with a single management interface. Other vendors, however, still

offer these as additional components with a unified or partially unified management interface, or are missing one or more of these components. Encryption, DLP, and MDM are often still viewed as additional components.

- Cloud based endpoint security solutions are increasingly gaining ground, as more customers seek to move most of their IT infrastructure to the cloud. As a result, most security vendors today offer cloud-based options for endpoint security, while a newer generation of vendors have emerged that offer exclusively cloud-based solutions. In terms of endpoint protection, cloud-based deployments are viewed as increasingly attractive to help manage growing mobile workforces, which need quick, secure access without increased complexity.

- Revenue for the Endpoint Security market is forecast to reach over $4.4 billion in 2015, and grow to over $5.7 billion by 2019. Figure 1, shows the projected revenue growth in the Endpoint Security Market, from 2015 to 2019.

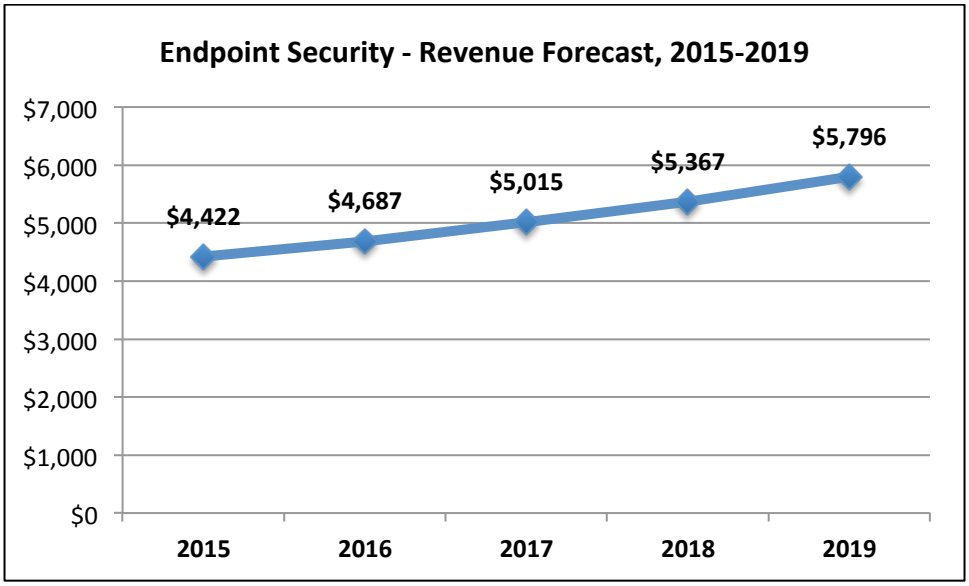


Figure 1: Endpoint Security Market Revenue Forecast, 2015-2019

EVALUATION CRITERIA

Vendors are positioned in the quadrant according to two criteria: Market Share and Functionality.

Market Share is based on the installed base published in our "Endpoint Security Market, 2015-2019" report. The vendor with the largest installed base has a market share of 1, the one with the second largest installed base has a market share of 2, etc. Vendors with larger market shares are positioned either in Top Player or Mature quadrants. Vendors with smaller market shares are positioned either in the Trail Blazer, or Specialist quadrants.

Functionality is assessed for each vendor's solution based on a number of key features that it offers out of the box. These capabilities 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.

In order for an Endpoint Security vendor to be placed in the right side of the quadrant (*Top Player* or *Trail Blazer*), their solution should possess some of the basic features summarized in Table 1 below.

Basic Features in an Endpoint Security Solution	
Malware Detection	Malware scans may be based on signature files, reputation filtering (proactive blocking of malware based on behavior characteristics, and an 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. Typical malware detection engines are updated multiple times a day. Malware can include spyware, viruses, worms, rootkits, and more.
Antivirus Removal Tools	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	Directory integration can be obtained via Active Directory or the LDAP protocol. Integration with corporate directories, allows organizations to more easily assign policies based on employee roles, and manage groups of users more effectively.

Firewall	Firewall functionality 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	Patch assessment is a common tool included in many endpoint security solutions. This feature periodically takes inventory of 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	Reporting lets administrators view activity that happens in the network. Endpoint security solutions may offer real time interactive reports of endpoint activity, or static information. Most solutions allow organizations to customize reports to best fit their monitoring needs.
Web and Email Security	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.

Table 1: Basic Features Included in Endpoint Security Solutions

The following capabilities are viewed as more advanced in an Endpoint Security solution and further add to a vendor's placement in the right side of the quadrant:

Advanced Features in an Endpoint Security Solution	
Data Loss Prevention	Data Loss Prevention (DLP) allows organizations to define policies to prevent the loss of sensitive electronic information. Some vendors claim they offer DLP functionality because they offer standard features that stop data from leaving the network, such as device control. Other vendors take a more vigorous approach and offer keyword blocking and deeper content inspection functionality.

Device Control	Device control allows administrators to control the usage of devices on endpoints, such as USB drives, CD/DVDS, and more. Basic binary policies are relatively common, but more granular controls, such as blocking a device by user, are considered an advanced feature.
Encryption	Various forms of encryption exist, such as full-disk encryption (FDE) or file-based encryption. FDE will lock an entire drive, whereas file-based encryption will only lock specific files. Encryption is usually unlocked with a password, but other forms of encryption also exist, such as only allowing a hard drive to be accessed by a unique endpoint.
Patch Remediation	In addition to patch assessment, some vendors also offer patch remediation in their endpoint security solution. This feature lets administrators actually deploy a missing software update discovered during the patch assessment phase. Software updates can be deployed directly from the management console.
URL Filtering	URL Filtering helps promote productivity by filtering out unwanted websites. It enables organizations to manage and control the websites their employees are allowed to visit. Organizations can block particular websites, or select from a category of websites (e.g. gambling), to keep employees from visiting these sites.
Mobile Protection	A growing number of endpoint security vendors are starting to integrate some form of mobile protection into their endpoint solutions. Other endpoint security vendors offer mobile protection through separate add-ons for Mobile Device Management (MDM) or Enterprise Mobility Management (EMM).

Table 2: Advanced Features Included in Endpoint Security Solutions

Note*: On occasion, we may put a vendor on the right side of the quadrant by giving them a higher than typical Functionality Score, even if they are missing one or two of the features mentioned above, if we feel that other aspects of their solution are particularly unique and innovative.*

MARKET QUADRANT – ENDPOINT SECURITY

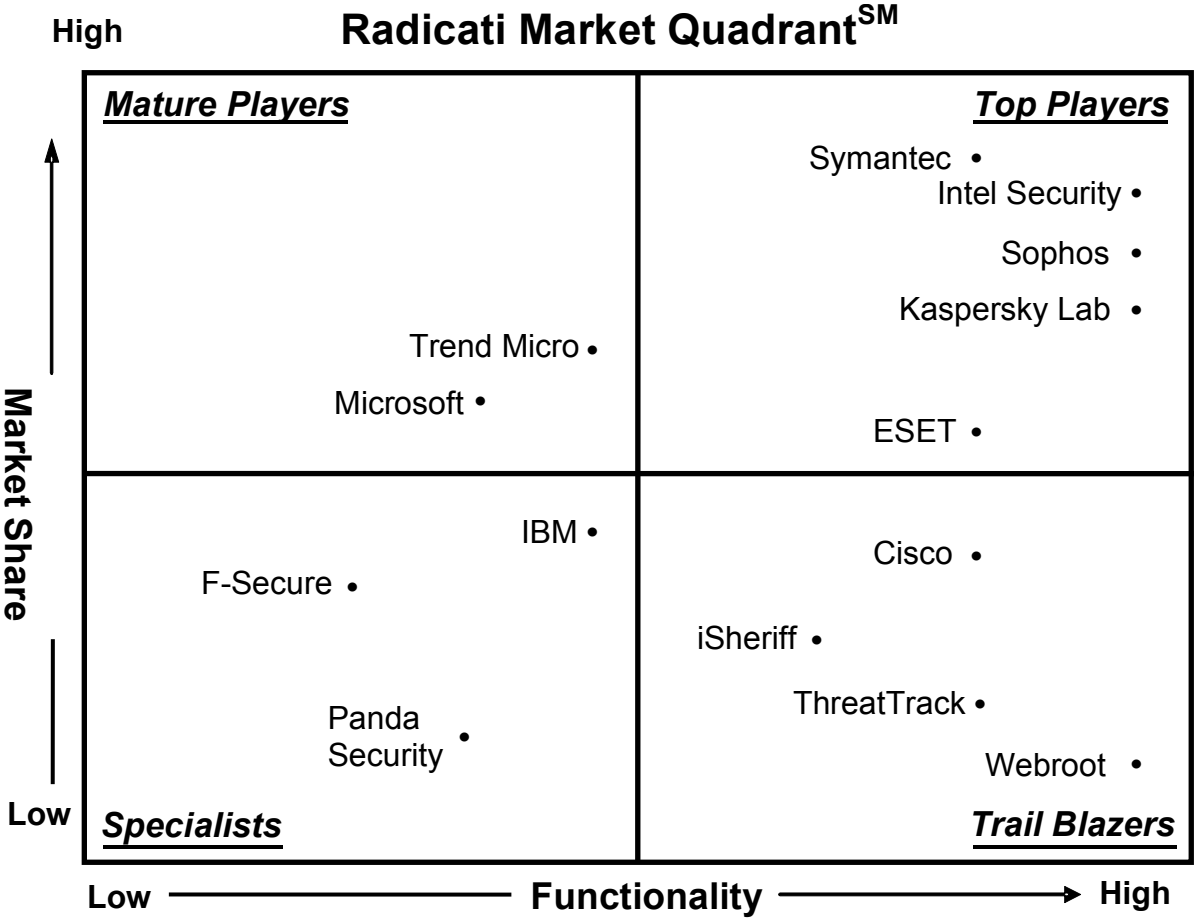


Figure 2: Endpoint Security Market Quadrant, 2015

· Radicati Market Quadrant℠ is copyrighted October 2015 by The Radicati Group, Inc. Reproduction in whole or in part is prohibited without expressed written permission of the Radicati Group. Vendors and products depicted in Radicati Market Quadrants℠ should not be considered an endorsement, but rather a measure of The Radicati Group's opinion, based on product reviews, primary research studies, vendor interviews, historical data, and other metrics. The Radicati Group intends its Market Quadrants to be one of many information sources that readers use to form opinions and make decisions. Radicati Market Quadrants℠ are time sensitive, designed to depict the landscape of a particular market at a given point in time. The Radicati Group disclaims all warranties as to the accuracy or completeness of such information. The Radicati Group shall have no liability for errors, omissions, or inadequacies in the information contained herein or for interpretations thereof.

KEY MARKET QUADRANT TRENDS

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

    - *Symantec* offers a broad range of endpoint protection solutions in different form factors aimed at the needs of enterprise customers of all sizes.

    - *Intel Security* continues to be a key innovator in the security space and offers solutions that are feature rich and meet the needs of customers of different sizes with varying security requirements.

    - *Sophos* solutions are easy to deploy and manage and are a good fit for mid-size and larger organizations that have a need for advanced features while retaining simplicity.

    - *Kaspersky Lab* is a leading innovator with very strong threat detection capabilities, its wide range of security solutions are aimed at a broad range of customers including large enterprises, and small and medium-sized businesses.

    - *ESET* is a well-respected player in the European market and offers solutions that deliver high performance with a low footprint.

- The **Trail Blazers** quadrant includes *Cisco, iSheriff, ThreatTrack,* and *Webroot.*

    - *Cisco* is a leading innovator and possesses a strong portfolio of security solutions aimed at meeting the full range of enterprise security needs.

    - *iSheriff* offers a well-rounded cloud-based endpoint protection solution aimed at the needs of SMBs and mid-size customers.

    - *ThreatTrack Security* offers a feature-rich solution aimed at the needs of small and midsize customers with advanced needs.

- *Webroot* offers highly innovative solutions well suited for small and medium organizations looking for solid, easy to manage protection.

- The **Specialists** in this market are *IBM, F-Secure,* and *Panda Security.*
  - *IBM* offers a broad portfolio of security capabilities, which when fully integrated offer endpoint protection across a range of computing platforms and devices.
  - *F-Secure* focuses mainly on the anti-malware and threat prevention aspects of its solution and continues to see good adoption mainly in the European region.
  - *Panda* offers a simple solution, which is easy to deploy and manage and is well aimed at the needs of SMB market.

- *Trend Micro* and *Microsoft* are **Mature Players** in this market.
  - *Trend Micro* offers a solid set of security solutions, however, it appears to have slowed down innovation in its endpoint solutions and seems more focused on other aspects of its security portfolio.
  - *Microsoft* offers strong security capabilities natively within its operating systems and delivers an endpoint protection solution, which is typically used as an initial building block for an enterprise security infrastructure.

ENDPOINT SECURITY - VENDOR ANALYSIS

TOP PLAYERS

SYMANTEC

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

Symantec was founded in 1982, and is based in Mountain View, CA. It has grown to be the largest security company through the variety of its offerings. 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.

Symantec's security solutions are powered by the Symantec Global Intelligence Network that offers real-time updates. **Symantec Endpoint Protection 12.1.6,** 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.

- *Malware protection* – is provided through multiple layers that include traditional signatures, and advanced detection technologies. Symantec's proprietary components Insight and Symantec Online Network for Advanced Response (SONAR) offer defense against advanced persistent threats and zero-day attacks through reputation and behavioral analysis.

- *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 also 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.

- *Antivirus removal tools* – are included that 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.

- *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 Small Business Edition,** which offers a simplified management console that can be deployed as a cloud-based solution or on-premise. 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 announced its roadmap for Advanced Threat Protection, which will complement its endpoint protection through two offerings: **Symantec Managed Security Services – Advanced Threat Protection** and **Symantec Advanced Threat Protection Solution**.

FUNCTIONALITY: 8
MARKET SHARE: 1

KEY STRENGTHS:

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

- 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.

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.

- The cloud-based version of Symantec Endpoint Protection lacks support for non-Microsoft Windows platforms.

- The recent split of the company into two companies (Veritas dedicated to information management and Symantec focused on security) has caused some transition pain and slowed down innovation. It remains to be seen how quickly the new, recently re-organized Symantec can regain focus on R&D and new technology development.

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, email, Web, data, data centers, and databases.

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. McAfee endpoint security offers both on-premises and cloud-based services.

On-Premises Solutions

McAfee on-premises endpoint security solutions are compatible with Microsoft Windows workstations and servers, Mac, VMware ESX, Linux, Citrix XenDesktop and XenServer, and other virtual platforms. Support is offered in a variety of packages, with Gold being the standard option and upgrades available to several different options that can include a dedicated technical representative to help with support queries. The solutions leverage the McAfee ePolicy Orchestrator (ePO) management console.

- **McAfee Complete Endpoint Protection — Enterprise** provides a scalable 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. It features the following capabilities:

    - *Collaborative and intelligent 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* — secures mobile devices from mobile malware threats with mobile antimalware protection and a secure container for Android devices.

- **McAfee Complete Endpoint Protection — Business** includes high-performance, 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 that steal confidential data and sabotage user productivity. 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 & 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.

Cloud-based SaaS Solutions

Intel Security also offers cloud-based security solutions. **McAfee SaaS Endpoint Protection Suites** offer endpoint, email, and web protection through a single, web-based console (SecurityCenter), and are available in three options:

- **McAfee SaaS Endpoint Protection –** is an entry-level suite which provides essential endpoint protection by blocking viruses, spyware, web threats, and hacker attacks.

- **McAfee SaaS Endpoint & Email Protection Suite –** offers comprehensive endpoint protection and enhanced email, web, and network defenses. It provides additional cloud-based email protection to ensure that inbound and outbound emails are filtered for spam, phishing attacks, and viruses before they reach the network.

- **McAfee Security for Business -** is an integrated suite that provides all-in-one SaaS protection across endpoint, email, and web.

On-Premises and Cloud-based SaaS solution (Combined)

McAfee Endpoint Protection for SMB – is designed for small and medium-size businesses. It offers an all-in-one solution that addresses antimalware, antispyware, data, web, and email 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 includes the two management consoles – McAfee ePolicy Orchestrator (ePO) and McAfee ePO Cloud.

Management Console

McAfee's ePolicy Orchestrator (ePO) and **ePO Cloud** — offers centralized management to provide instant visibility into the state of security defenses. Insight into security events allows administrators to understand and target updates, changes, and installations to systems. The web-based single management console unifies control over security and compliance tools from McAfee, as well as third parties.

FUNCTIONALITY: 9
MARKET SHARE: 2

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

- McAfee offers a choice of on-premises, cloud-based and hosted solutions.

- 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 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.

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 and malware 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 will incorporate these capabilities into Sophos Cloud, its cloud-based security management platform, which includes endpoint protection, mobile management, server protection, network security and web gateway functionality.

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 is working to launch what it calls, Security Heartbeat, which will deliver Synchronized Security by passing live security information between endpoint agents and the Sophos Next Generation Firewall / UTM.

- *Endpoint Antivirus* – Sophos's agent includes proven anti-malware capabilities powered by SophosLabs and detects viruses, suspicious files and behavior, adware, and other malware. Real-time anti-virus lookups help ensure the most up-to-date information available.

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

FUNCTIONALITY: 9
MARKET SHARE: 3

KEY 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.

WEAKNESSES:

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

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

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

KASPERSKY LAB

39A/3 Leningradskoe Shosse
Moscow 125212
Russian Federation
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 business solutions represent are aimed at a broad range of customers including large enterprises, small and medium-sized businesses.

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 & virtual machines, mobile devices and file servers. Kaspersky Endpoint Security for Business is available in four different tiers, each of which adds its own layer of protection against cyber-threats, as follows:

- *Core* – provides Anti-Malware (for Windows, Mac and Linux) and Security Management.

- *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 and Security Management.

- *Total* – 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, Security for Collaboration, Security for Mail, Security for Internet Gateway, and Security Management.

Kaspersky Endpoint Security solutions offer support for a broad array of platforms, which include Windows, Linux, Mac, VMware, Citrix, IBM Notes/Domino, Microsoft Exchange, Android, iOS and Windows Phone.

All endpoint security products are managed by **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, thorough vulnerability assessments, achieve a real-time hardware and software inventory and offers clear, actionable reporting.

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

Kaspersky offers a number of other security products that deliver similar features to those available in Kaspersky Endpoint Security for Business but are designed for other platforms. These solutions include:

- **Kaspersky Anti-Virus for Windows Servers Enterprise Edition,**
- **Kaspersky Anti-Virus for Linux File Server,**
- **Kaspersky Security for Microsoft SharePoint,**
- **Kaspersky Security for Linux Mail Server,**
- **Kaspersky Security for Microsoft Exchange Servers,**
- **Kaspersky Anti-Virus for Lotus Notes/Domino,**
- **Kaspersky Anti-Virus for Proxy Server,**
- **Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG.**

Kaspersky Security Solutions for Enterprise provides multi-layered protection. Kaspersky Lab offers an Enterprise Security Platform comprising the following solutions: Endpoint Security, Mobile Security, Security for Data Centers, Virtualization Security, Anti-APT, Industrial Security, Fraud Prevention, Private Security Network, Security Intelligence Services, DDoS Protection.

FUNCTIONALITY: 9
MARKET SHARE: 4

KEY STRENGTHS:

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

- 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 malware scanning engine and proactive detection technologies which combined with the Kaspersky Security Network provides 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.

- 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 solutions support for the broad range of systems found in enterprises, encompassing Windows, Linux, Mac, VMware, Citrix, IBM Notes/Domino, Microsoft Exchange, Android, iOS and Windows Phone.

WEAKNESSES:

- 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 security products for Microsoft Exchange and Forefront Threat Management Gateway have separate management servers, which are not integrated with the Kaspersky Security Center console.

ESET, SPOL. S.R.O.

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

Headquartered in Bratislava, Slovakia, ESET has research, sales and distribution centers around the globe and a presence in more than 180 countries worldwide. The company has more than 25 years of experience in network security.

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, and as a Virtual Appliance.

- **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, and combine reputation-based anti-virus 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, and more.

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

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

- **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, cluster support) 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 and will be available in late 2015. 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.

FUNCTIONALITY: 8
MARKET SHARE: 7

KEY 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 redesigned 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.

WEAKNESSES:

- ESET does not provide DLP. However, ESET has this on its future roadmap.

- ESET offers encryption as add-on option, however, management of this solution is not currently integrated with the ESET Remote Administrator. ESET is working to address this in future releases.

- ESET's patch assessment approach is somewhat limited and could be improved upon. The vendor is aware of this and is looking to address this in future releases.

- ESET Mobile device protection is limited and currently only available for Android platforms. However ESET is also working to add iOS support in the 2015 timeframe.

TRAIL BLAZERS

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

Cisco is a leading vendor of Internet communication and security technology. In October 2013, Cisco completed its acquisition of Sourcefire, and in June 2014, it completed the acquisition of ThreatGRID, which offers a cloud-based sandboxing service and on-premise sandboxing appliance. Cisco's security solutions are powered by the Cisco Talos Security Intelligence and Research Group (Talos), which is made up of leading threat researchers.

Cisco Advanced Malware Protection (AMP) for Endpoints can detect, analyze, block,

and track advanced malware outbreaks across endpoints, including PCs, Macs, Linux, mobile devices and virtual systems. AMP for Endpoints uses global threat intelligence from Talos Research and AMP Threat Grid to strengthen defenses to prevent breaches before they occur. It also uses a telemetry model to take advantage of big data, continuous analysis, and advanced analytics.

Malware protection – is provided through a combination of file reputation, cloud-based sandboxing, and intelligence driven detection. Cisco's Talos Security Intelligence provides the ability to identify and filter/block traffic from known malicious IP addresses and sites, including spam, phishing, Bot, open relay, open proxy, Tor Exit Node, Global Blacklist IPs and Malware sites in addition to domains and categorized, risk-ranked URLs.

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.

Firewall – AMP for Endpoints integrates with AMP for Networks. All detection information is sent to the FireSIGHT management platform and can be used to correlate against other network threat activity. FireSIGHT 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 FireSIGHT console for tighter management across all deployed Cisco

security solutions.

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. The latest version assists with the deployment of AMP for Endpoints and expands endpoint threat protection to VPN-enabled endpoints, as well as other Cisco AnyConnect services.

FUNCTIONALITY: 8
MARKET SHARE: 9

KEY STRENGTHS:

- Cisco offers a broad security portfolio, which encompasses threat intelligence, heuristics, behavioral analysis and sandboxing to predict and prevent threats from entering the endpoint.

- 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, mobile devices, virtual environments, as well as an on-premise private cloud option.

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

- Cisco is working to add more API's for integrations with existing infrastructure to make AMP even more compatible with Cisco security products.

WEAKNESSES:

- Cisco needs to improve on the management of its solutions through a more unified management console that can bring together its broad range of 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 customers that are vested into deploying Cisco's rich AnyConnect security suite, rather than customers that are just looking for an endpoint solution.

iSHERIFF

555 Twin Dolphin Plaza
Redwood City, CA 94065
United States
www.isheriff.com

iSheriff offers a cloud based, enterprise device security platform designed to protect all enterprise devices, including laptops, servers, tablets, point of sale devices, industrial equipment and emerging "Internet of Things" technologies. In 2012, the company was acquired by security vendor Total Defense, which re-named itself as iSheriff in 2014, following the divestiture of its consumer security business unit. iSheriff is privately held with headquarters in Redwood City, California and operations in New York, California, Europe, Ireland, Israel and Japan.

iSheriff Cloud Security is a cloud-based endpoint protection solution, which combines anti-malware, application controls, and protection against threats from removable media, such as USB drives. The solution includes the following:

- *Malware protection* – through traditional anti-malware technology and dynamic anomaly detection and behavior modeling systems to protect against viruses, botnets, spyware, trojans, and browser exploits across Windows, Mac and Linux devices.

- *Application Control* - is included to control the use of specific applications on endpoint devices, such as remote access applications, unwanted browsers, messaging applications, P2P sharing, or any other applications that administrators choose.

- *Device Control* - the iSheriff client can be deployed using Group Policy or other software distribution models. It also includes legacy end point uninstallation.

- *Management* - is cloud based, through an intuitive web interface, which allows organizations to configure, manage, control endpoint policies and view reports. iSheriff also works with Active Directory, and other directory services, to ease user account set up and maintenance.

iSheriff also offers **iSheriff Web Security** for web security, and **iSheriff Email Security**, for email security. All solutions are controlled through the same web-based cloud administration console, which allows organizations to view, report and control their entire endpoint, web, and email security deployment from a single console with a common set of policies.

FUNCTIONALITY: 7
MARKET SHARE: 11

KEY STRENGTHS:

- iSheriff offers a cloud based security platform that offers full control of endpoint, web, and email security from a single console.

- Easy deployment of its lightweight endpoint client via Group Policy, or other software distribution models.

- iSheriff offers integration with Active Directory and other directory services for ease of administration.

- iSheriff offers removable media controls (e.g. USB drives).

- iSheriff's easy to use cloud based management console, allows setting endpoint application controls, security policy creation and reporting.

WEAKNESSES:

- DLP is available only on the iSheriff Web and Email Solution. Customers that choose to deploy only endpoint security do not have access to DLP features.

- iSheriff does not offer encryption.

- iSheriff does not offer MDM capabilities for mobile devices, such as Android and Apple iOS.

- iSheriff Cloud Security does not offer patch assessment. While it reports on the version of the endpoint client and the anti-malware signatures that are on each device, it does not inventory other software that is on the system.

THREATTRACK SECURITY

311 Park Place Blvd,
Suite #300
Clearwater, FL 33759
www.threattracksecurity.com

ThreatTrack Security, spun off from GFI Software in 2013, develops advanced cyber defenses for government agencies and companies of all sizes.

ThreatTrack Security's **VIPRE Business Premium 7.5** is compatible with Microsoft Windows, Apple Mac OS X, and virtual machines. The solution features the following capabilities:

- *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. ThreatTrack Security writes its own antivirus signatures that are provided in VIPRE Business Premium 7.0. The solution’s file behavior replication scanning system, called MX-Virtualization, scans unknown files in a micro-footprint virtual environment to identify malicious behavior.

- *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.

- *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.

- *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.

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

- *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 and update server.

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

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

- *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.

ThreatTrack Security also offers a non-premium version of its solution called **VIPRE Antivirus Business 7.5,** which has all of the same features of the premium version, but does not offer patch management, firewall and Web security.

FUNCTIONALITY: 8
MARKET SHARE: 12

KEY STRENGTHS:

- The VIPRE Business Premium 7.5 solution offers 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 critical security managed from the same console that VIPRE administrators are already familiar with.

- ThreatTrack's Security Response team can assist with malware removal on systems that are running VIPRE, this is 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.

WEAKNESSES:

- DLP features are not included.

- Encryption is not offered.

- ThreatTrack does not currently offer support for VMWare virtualized environments.

- Device control is not offered aside from automatic scanning of USB drives for malware, and management of Android and iOS devices. However, removable device control is under development and is slated for inclusion in the next release, VIPRE 8.

- Directory integration could be improved for easier management and configuration through user-based policy management.

WEBROOT INC.

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

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

Webroot offers the **SecureAnywhere** suite of security products for endpoints and mobile devices. Webroot threat prevention is powered by the **BrightCloud 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 devices; Terminal Servers and Citrix; VMware; Virtual Desktops and Servers and Windows embedded Point of Sale (POS) systems. It features the following capabilities:

- *Real-Time Anti-malware* – designed to counter unknown malware uses Webroot's BrightCloud correlated threat intelligence to perform continuous file and process analysis, 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. Webroot requires zero signatures or definition updating of the endpoint as BrightCloud makes collective file and process security intelligence instantly available to customers in real time.

- *Web Protection* – is provided through a number of different shields within the Webroot solution. The Web Threat Shield uses BrightCloud Threat Intelligence to block sites with poor reputations and known infected or malicious domains. Webroot's BrightCloud Real-Time Anti-Phishing service is also integrated to stop phishing and

spear-phishing. The Identity Shield isolates the browser (and any other application needed) from the rest of the endpoint. This anti-Trojan technology protects the user and device, so even if there is malicious code already present, sensitive information such as banking access credentials cannot be stolen.

- *Outbound Firewall* – ensures that all outbound TCP/UDP requests and destinations are checked against BrightCloud 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 prove 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 is 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 overheads associated with complex endpoint deployments.

- *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 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 overrides.

- *Enhanced Web Filtering* – provides real-time Anti-phishing (RTAP) integration with BrightCloud Threat intelligence to help stop most spear-phishing attacks.

- *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.

- *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.

- *EP Forensics* – will be made available in late 2015 to support Log file visualization; unclassified file insights; event statistics and behavioral drilldowns.

- *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. Enterprise security platforms such as SIM/SIEM threat intelligence platforms are also supported.

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.

FUNCTIONALITY: 9
MARKET SHARE: 14

KEY 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 quickly remote rollback across all 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.

SPECIALISTS

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.

IBM Endpoint Manager for Core Protection, is a component of **IBM Endpoint Manager.** It 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 available as an add-on to IBM Endpoint Manager.

- *Reporting* - offers real-time insight into security and deployment statistics. Additional, in-depth reporting on software usage can be obtained through deployment of the optional IBM Endpoint Manager for Software Use Analysis.

- *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 Endpoint Manager 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 Endpoint Manager (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 Endpoint Manager.** It provides protection for Microsoft Windows XP, Windows 7, Windows 8, and Apple Mac OS X. Trusteer Apex is 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 to 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.

FUNCTIONALITY: 5
MARKET SHARE: 8

KEY STRENGTHS:

- A single IBM Endpoint Manager server and console can scale to manage 250,000+ devices across multiple platforms.

- IBM Endpoint Manager 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 Endpoint Manager for Core Protection provides broad support for virtual machines.

- IBM MaaS360 offers additional capabilities to protect and manage mobile devices.

- IBM Endpoint Manager for Core Protection offers deep add-on capabilities for DLP, which include features such as pattern matching.

- IBM Endpoint Manager for Core Protection has a relatively low footprint on system usage (e.g. RAM usage).

WEAKNESSES:

- Policy creation is not as simple in IBM Endpoint Manager for Core Protection 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.

F-SECURE

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

F-Secure, founded in 1988, offers security solutions for enterprise and consumer customers. F-Secure is based in Finland, and it is publicly traded in the country.

F-Secure offers **Business Suite,** which includes **Client Security** for endpoint protection. Client Security is compatible with Microsoft Windows 10, XP, Vista, Windows 7, and Windows 8. It is available only as an on-premises solution. The solution features the following capabilities:

- *Connection Control* – automatically sets up an extra layer of protection for business sensitive transactions, such as online banking. Connection Control activates automatically and protects against trojans and other malware.

- *Web Content Control* – allows the administrators to control web usage within the company network. Web site restrictions can be enforced via pre-defined categories from the Policy Manager. From the central management portal, IT administrators can create and enforce web access restrictions.

- *Automatic software updates* – a Software Updater is included in the clients and allows administrators to automatically manage software patches to protect against known vulnerabilities.

- *Advanced Protection* - Web Traffic Scanning Advanced Protection allows administrators to block certain content from unknown and suspicious sites, e.g. Flash, Silverlight, Executables, Java & ActiveX components. Administrators can also whitelist trusted sites.

- *Malware protection* - F-Secure offers multiple detection engines, including its own and third-party developed, which contain emulation and other heuristics-based technologies in addition to traditional signature-based approaches. F-Secure also offers its own behavioral anti-malware technology – DeepGuard, which offers proactive, instant protection against unknown threats. It monitors application behavior and stops potentially harmful activities in real-time. In addition, F-Secure offers BlackLight rootkit detection technology, which is able to find files, folders and processes that are hidden from users and programs.

- *Email security* - detects malicious content in email traffic (IMAP4, POP3 and SMTP protocols) to help protect against email malware.

- *Browsing Protection* - detects and blocks malicious content in web traffic (HTTP) to provide additional malware protection. Websites are also blocked if they contain an exploit aimed at the user's browser. Protection against unsafe web sites is also provided.

- *Internet Shield* - consists of Firewall, Application Control, and Intrusion Prevention (IPS). Firewall capabilities can be customized with administrator-created rules to block or allow certain IP addresses. Applications can be selected to block, prompt, or allow incoming and outbound connections. The firewall can enforce location-aware policies, and also contains an intrusion prevention system that alerts administrators when an incoming network attack attempt is detected.

- *Software removal tools* - are included that can uninstall previous deployments of unwanted security solutions.

- *Application control* – is centrally managed, administrators can decide which programs that access the network can be used in the workstations. This prevents the use of programs that violate company policy, and allows monitoring of programs in use.

- *Reporting* - is available to give insight into security and deployment statistics, such as number of applications blocked.

- *Management* - is centrally available through the Policy Manager, which allows administrators to track security status and configure polices.

F-Secure's Business Suite also comprises a separate product called **Linux Security**, which provides protection for Linux endpoints.

FUNCTIONALITY: 3
MARKET SHARE: 10

KEY STRENGTHS:

- Updates are transparent and delivered constantly throughout the day in a way that does not disrupt employee productivity.

- The footprint of F-Secure with regards to CPU and RAM usage is much smaller than that of other vendors in the space.

- F-Secure is priced lower than other competitors in the endpoint security market.

- Setting administrative policies is a straightforward, simple process.

- New, advanced features are included in the Premium version and can be managed through the central management portal.

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.

- MDM management is not included. Basic MDM capabilities are offered as a separate solution.

- Encryption is not included.

- Active Directory integration and the ability to manage and drive user policies through the directory service are lagging, however, F-Secure is working to address this in future releases.

PANDA SECURITY

Gran Via Don Diego Lopez de Haro, 4
48001 Bilbao Spain
www.pandasecurityusa.com

Panda Security, formerly Panda Software, was founded in 1990 in Bilbao, Spain. Panda solutions are sold to consumer and enterprise customers. The company is privately held by private equity firm Gala Capital, investment firm Investindustrial, and investment firm IPW.

Panda Endpoint Protection (**Plus)** was designed from the ground up as a completely cloud-based solution. It is compatible with Microsoft Windows workstations and servers, Linux systems, Mac OS X and Android. Panda Endpoint Protection provides the following features:

- *Malware protection* – is provided in part by Panda Security's proprietary Collective Intelligence technology that maintains a knowledge base of good and bad files, and which classifies files automatically in real time. Heuristics and behavior-based analysis of local files on machines are also available.

- *Firewall* – features can be managed centrally. Permissions can be created for any program and application. An intrusion detection system can be enabled to prevent unauthorized access to a PC on an organization's network. Remote users can be given access to the firewall settings if deemed appropriate.

- *Antivirus removal* – tools are included that can uninstall previous unwanted security software.

- *Remote access* – can be integrated into the management console. Administrators can control machines that have the appropriate software installed, such as LogmeIn, TeamViewer or any VNC-based solution.

- *Device control* – can be set up to block or allow the transfer of data on various storage devices, such as a USB storage device.

- *Reporting* – is available in three types of formats: executive, status, and detection. Each report type can be generated with varying levels of granularity. The reports can also be scheduled for creation or accessed on demand.

- *Management* – is controlled via a Web-based console with tabbed browsing. Administrators can create and edit policies, groups, licenses, and other features in the centralized console.

Panda Endpoint Protection (Plus) adds Web access control, which can be set to deny access to different categories of websites, or to restrict access only during certain hours of the day. This includes anti-malware and anti-spam protection as well as content filter for on-premise Microsoft Exchange Servers, all managed from the same SaaS console.

Panda Systems Management is a SaaS-based remote systems management solution, which can be accessed together with Panda Endpoint Protection through a Panda Cloud portal using Single Sign On. System Management offers the following functionality:

  - Hardware and Software inventory.
  - Patch Management.
  - Scripting and third party software distribution, with a library of pre-built components.
  - Monitoring and Alerting.
  - Remote control, remote command shell, remote task manager, reporting and ticketing.

- Basic MDM functionality for Android and iPhone devices.

Adaptive Defense and Adaptive Defense 360 - released in 2015, combines traditional antivirus with the latest EDR technology (Endpoint Detection and Response), ensuring proactive detection of strange behavior and advanced threats, from Cryptolocker to zero-day attacks, and providing automated response and remediation capabilities.

FUNCTIONALITY: 4
MARKET SHARE: 13

KEY STRENGTHS:

- Panda solutions were designed from the ground up as cloud-based solutions.
- Panda offers a multi-platform solution that allows customers to protect different system and devices from a unique centralized console, including Microsoft Exchange Servers.
- The endpoint protection client has a light footprint and achieves high detection rates.
- Panda Endpoint Protection solutions are designed to meet the ease of use and low management overhead needs of SMBs.
- Policy management can be controlled by resellers, which can be useful for organizations with no IT staff that would prefer to outsource the task of policy creation.
- The administration console allows remote management of machines via a virtual network connection, which gives administrators an easier way to troubleshoot any difficulties.

WEAKNESSES:

- Device control is somewhat limited in granularity. Management is largely binary, with block/allow policies.
- Encryption is not available in Panda Endpoint Protection.

- Panda does not provide patch assessment or remediation.

- Panda includes basic MDM capabilities with Endpoint Protection Plus, or through its separate Panda Cloud Systems Management solution.

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.

Trend Micro **Enterprise Security 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 anti-virus, 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 Anti-Virus for Android devices.

KEY 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 it they are 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.

- MDM is a separate add-on.

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

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.

Microsoft System Center 2012 Endpoint Protection (SCEP) is Microsoft's solution for antimalware 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 are managed through a single administration console, **Microsoft System Center 2012 R2 Configuration Manager**, 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 Microsoft System Center 2012 Configuration Manager, which distributes updates and removes software as needed.

- *Reporting* - is also available through Microsoft System Center 2012 Configuration Manager, to give insight into deployment statistics, out-of-date definitions, policy distribution status, and more.

FUNCTIONALITY: 4
MARKET SHARE: 6

KEY 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 System Center 2012 R2 Configuration Manager 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 Rights Management.

- Microsoft System Center 2012 R2 Configuration Manager 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 System Center 2012 R2 Configuration Manager for configuration and policy management but also deploy an additional security solution from a best-of-breed security vendor.

- DLP capabilities are not included.

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

- Microsoft System Center 2012 R2 Configuration Manager does not offer granular device control for removable media, CD/DVDs, and other common devices.

- Microsoft is focusing most of its efforts into building security features into the Windows 10 platform, for instance, MDM is built into the 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, these clients are not integrated with Configuration Manager.

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:

- Whitepapers
- Strategic Business Planning
- Product Advice
- TCO/ROI Analysis
- Investment Advice
- Multi-Client Studies

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

MARKET RESEARCH PUBLICATIONS

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

Currently Released:

Title	Released	Price*
Microsoft SharePoint Market Analysis, 2015-2019	Aug. 2015	$3,000.00
Email Market, 2015-2019	Jul. 2015	$3,000.00
Cloud Business Email Market, 2015-2019	Jul. 2015	$3,000.00
Corporate Web Security Market, 2015-2019	Jul. 2015	$3,000.00
Office 365, Exchange Server and Outlook Market Analysis, 2015-2019	Jun. 2015	$3,000.00
Advanced Threat Protection Market, 2015-2019	May 2015	$3,000.00
Enterprise Mobility Management Market, 2015-2019	May 2015	$3,000.00
Information Archiving Market, 2015-2019	May 2015	$3,000.00
Social Networks Statistics Report, 2015-2019	Mar. 2015	$3,000.00
Email Statistics Report, 2015-2019	Mar. 2015	$3,000.00
Instant Messaging Market, 2015-2019	Mar. 2015	$3,000.00
Mobile Statistics Report, 2015-2019	Feb. 2015	$3,000.00
Endpoint Security Market, 2014-2018	Dec. 2014	$3,000.00
eDiscovery Market, 2014-2019	Dec. 2014	$3,000.00

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

Upcoming Publications:

Title	To Be Released	Price*
Endpoint Security Market, 2015-2019	Oct. 2015	$3,000.00
eDiscovery Market, 2015-2019	Oct. 2015	$3,000.00

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

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

