IDC MarketScape

IDC MarketScape: Worldwide Mobile Threat Management Security Software 2017 Vendor Assessment

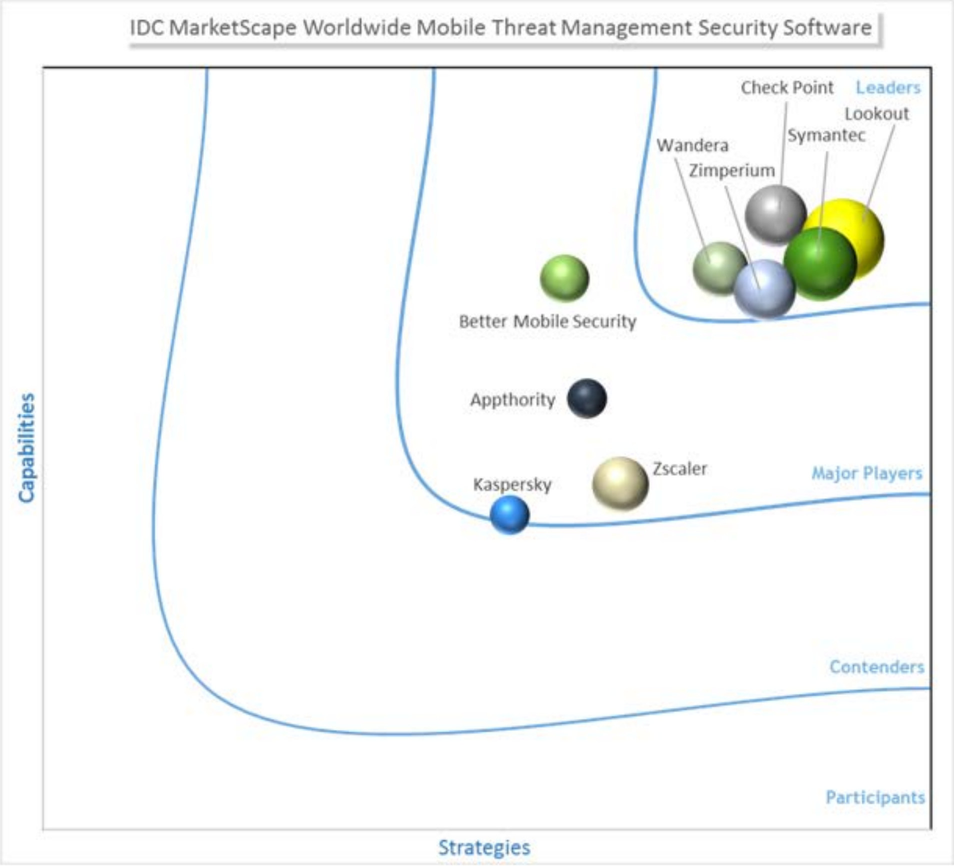
Michael Jennett Phil Hochmuth

THIS IDC MARKETSCAPE EXCERPT FEATURES: SYMANTEC

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Mobile Threat Management Security Software Vendor Assessment



Source: IDC, 2017

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

September 2017, IDC #US42373417e

IN THIS EXCERPT

The content for this excerpt was taken directly IDC MarketScape: Worldwide Mobile Threat Management Security Software 2017 Vendor Assessment (Doc # US42373417). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

As the mobility market continues to evolve, we are seeing changes to the way enterprises evaluate the security needs of their enterprise mobility solutions. This has brought about an expansion of mobile threat management (MTM) products that expand beyond the standard tracking and management of devices we have traditionally focused on with enterprise mobility management (EMM).

IDC sees the mobile threat management market gaining momentum as more enterprises decide that EMM/MDM and native sandboxing and segmentation on mobile operating systems (OSs) are not enough to meet overall mobile threat management needs. According to IDC's 2017 *U.S. Enterprise Mobility Decision Maker Survey,* half of U.S. enterprises and SMBs have deployed some form of mobile device security solution – mobile antimalware, mobile threat management, or mobile app scanning. An additional one-third of U.S. businesses not using MTM today plan to deploy this technology in the future.

Deploying EMM plus MTM is becoming the new defense-in-depth, or "belt + suspenders," approach to security. Every MTM customer reference IDC interviewed for this study deployed its MTM solution in concert with EMM technology. This follows the overall trend among U.S. enterprises; among the 50% of enterprises deploying MTM solutions, more than three-quarters also had deployed EMM, according to IDC's 2017 *U.S. Enterprise Mobility Decision Maker Survey.*

MTM interest is driven by the overall security challenges businesses face. According to the IDC mobility survey, mobile security/compliance, in general, was the most frequently cited challenge businesses said they face among all aspects of a mobility deployment — before cost, complexity, and vendor-related issues. Compliance requirements specifically drive a lot of MTM buying decisions, as businesses face market/industry-specific compliance requirements and mobile computing, as well as more broad-sweeping regulatory challenges, such as the General Data Protection Regulation in the European Union (EU), and for firms operating in that region.

Key findings of this study include:

- Vendors' MTM products are primarily focused on iOS and Android platforms with limited availability on the Windows 10 platform, with many believing the traditional Windows security products cover that area. This leaves a gap between pure-play mobile devices and enterprise tablet devices utilizing Windows 10 operating system.
- Capabilities found in most MTM products focus on protecting the device from phishing attacks, man-in-the-middle attacks, and device-specific security issues such as jailbreaking. Advanced MTM providers cover every aspect of interactions with the mobile device – from user downloaded apps through to network connections. Thwarting SMS-based attacks is also a focus for MTM providers, as texting is a frequently used business communications tool that falls outside the area of most traditional security solutions.

- Carrier partnerships are key go-to-market strategies for MTM providers as a way to get their software deployed on enterprise mobile devices provisioned through mobile operators and managed via mobile life-cycle management or managed EMM solutions.
- Similar to carrier partnerships, EMM partnerships are critical for MTM providers in business deployments, as most MTM solutions rely on these platforms for a range of remediation and device-level enforcement capabilities, as well as distribution of MTM agents to corporate-liable and BYO devices.
- Customers of MTM software are focused on device management beyond standard EMM and looking for the next level of security for their enterprise devices.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Vendors included in this research effort meet the following inclusion criteria:

- Mobile threat management, as defined for the purposes of this vendor assessment, provides protection, detection, analysis, and remediation of mobile device based on threats from both a device and a network perspective.
- Software offering must be standalone or, if not standalone, the products' primary focus must be mobile threat management. Offering should have both a client (mobile app) and a network component that complement each other and provide real-time data for analysis and mitigation.
- Offering must, at a minimum, support Android- and iOS-based devices.
- Offering must meet one of the following criteria: offering has been available for at least one year, or it must have five or more verifiable customers.

ADVICE FOR TECHNOLOGY BUYERS

This study analyzes and rates vendors across a broad range of capability- and strategy-focused criteria. As mobile threat management comprises a group of products in a nascent stage, it is important to evaluate them based on customer interactions with the available products as well as these products' view to the future of mobility. As threats evolve, so must the road maps of the products that will protect devices from these threats. Further as more IoT devices enter the market, it is important for the interaction between MTM products, enterprise mobile devices, and future devices to all work seamlessly together, which requires MTM products to go beyond traditional mobile device protections to take IoT into account. Some of the key areas that IT buyers should focus on when evaluating MTM products are discussed here.

Key Measures for Success

- **Current capabilities.** Key capabilities match the market need for protection from local physical attacks, [interactive] network attacks, mobile email attacks, SMS-based attacks, web-based attacks, app-based attacks, malware compromise, outdated operating systems, jailbreaking, and so forth. IDC believes that when reviewing mobile threat management products, customers should be aware that there are baseline capabilities that are necessary for these products to be functional for the enterprise market. These key capabilities ensure that the product goes beyond device management or simple virus scanning and is truly a threat management product that will provide IT organizations with a potent tool to fight mobile threats in fashion that is not cumbersome to the user.

- **Evolving product road map.** The product road map is based on customer and partner input that covers the aspects of cloud, data analysis, mobility solutions, and social integration. The product road map shows substantial investment in planning and timing based on inputs from customers and partners as well as an overall understanding of the industry. The road map extends past basic product functionality and looks to accommodate current mobile device offerings and is future looking in a fashion that positions the company and product to be a leader in the industry.

  Further, the road map shows understanding of how the security market is evolving to address mobile threat management architecture needs. With mobile security still in its nascent stage and mobile becoming more prevalent in the enterprise, it is imperative that the product road map can meet the evolving business needs that companies will be facing over the next few years. Having a product that is poised to handle today's security concerns and is looking to the future about mobile and IoT is imperative for success.
- **Planned service offerings (products to be introduced next year).** Demonstration of product growth and expansion meets current and future market needs. In conjunction with the overall strategic road map, the offerings planned over the next year are important to evaluating each of these enterprise MTM products. IDC looked at the offerings that are planned as well as what is currently in testing to determine the product will meet the needs of the enterprise today and will incorporate the changes in the industry; vendor is actively providing new features to meet those needs.
- **Customer assessment of vendor.** Customers rely on innovative opportunities with vendor for strategic needs. A key element IDC looks for when evaluating products is how the current customer base feels about that product in its implementation. No matter how many features a product has or how long it's been on the market, if it is does not meet the needs of the customer or if it is cumbersome for the customer to install, support, or use, it will not be adopted. Therefore, customer success is a key factor in the success of a product. Product is shown to be easy to implement and meets the current and future needs of the customer base in the enterprise market.

  Further, new security features can be cumbersome and difficult to implement on the enterprise level. The ability to deliver product that is easy to implement from the time the customer signs a contract to when the customer has the product up and running is one of the keys to a successful implementation. Based both on vendor information and customer impact, IDC evaluated the time required to roll out each new product both at the network level and at the device level.
- **Architectural innovation.** Strategic plan to make mobile threat management is a key element of strategic security architecture. Mobile threats are an ever-growing aspect of the enterprise, and with more mobile devices entering the enterprise arena, it is imperative that mobile threat management products focus on architectural development and innovation that are positioned not just for today's threats but also for tomorrow's threats. A mobile threat management product must be constantly evolving and able to look for the next threat on the horizon rather than simply focusing on the threats of today.
- **Implementation.** Mobile threat management is just one tool in the security toolbox for enterprise mobility today. For this reason, it is imperative that the MTM tool can easily integrate with existing security infrastructure and other security tools. The MTM solution must integrate out of the box with current EMM solutions and connect to existing security information and event management (SIEM) products used within the enterprise. The MTM product must also be easily installed on all mobile devices that are managed by the enterprise customer. Device installation should be simple and straightforward for the users and ensure that little memory and battery is required for usage.

- **Support.** Vendor offers various levels of support, providing customers with the ability to mitigate issues throughout the product life cycle. This can include carrier partnerships to deliver MTM software with business handsets as well as broader integration strategies with systems integrators and security solutions implementation partners with mobile-focused practices.

  As MTM is still a relatively new area for most enterprises, it is important that support is easily accessible to the IT organization. We evaluated products based on the level of support provided and the extent to which that support is available on a 24 x 7 basis. IDC looked at the support offerings of each product based on what was provided by the vendor, how the customers currently use support, and customer assessment of support.
- **Intellectual property.** To be a true leader in MTM, it is important for the product to go beyond just basic capabilities. This aspect of capabilities looks at things such as machine learning and AI capabilities within each product. IDC evaluated the unique features and offerings of each product.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Symantec

Symantec is listed as a Leader in this IDC MarketScape for the MTM security software market. Symantec Endpoint Protection Mobile (SEP Mobile), formerly Skycure Mobile Threat Defense, was announced in 2012 with its first general availability product release in 2014 and has had an exclusive enterprise reseller partnership with AT&T since October 2016. Skycure received substantial venture funding over the past five years and was recently acquired by Symantec. The acquisition will allow Symantec to integrate the Skycure product offering with Symantec's other consumer and enterprise security products. This acquisition has the potential to greatly expand the capabilities and reach of Skycure's products. SEP Mobile has more than 50 customers in various verticals, including several Fortune 500 companies. SEP Mobile has bidirectional technology and go-to-market partnerships with all major EMM vendors including BlackBerry, Citrix, IBM, Microsoft, MobileIron, and VMware.

The product consists of three main parts:

- **SEP Mobile app.** The app runs in the background of a smartphone, a tablet, or an IoT device (customer example – Western Union money transfer kiosks run SEP Mobile) to secure mobile devices 24 x 7. The app uses multiple patented technologies such as Active Honeypot, Repackaged App Detection, mobile network access control (mNAC) to analyze all apps, networks, and services used by the device to proactively identify known and emerging threats. In addition, it assesses the security state of the device itself, ensuring proper security configuration for complete protection. Once threats are identified, the app can alert the mobile user, alert the employee's IT department, and apply protection (both MDM policy enforcement and a plethora of standalone mobile active protection [MAP] measures via relevant security policies).
- **Cloud server.** The SEP Mobile cloud server leverages machine learning for connecting data from and to the mobile app, as well as providing the security console for the administrator. The server works to interpret information coming from connected devices and makes determinations about how threats are dealt with. This is done via continuous scanning of vulnerabilities as well as compliance issues and is augmented by crowdsourced intelligence embedded within the server. The server condenses millions of data points to calculate a risk score so that IT can quickly discern the state of the overall system and the risk to each device. Admins can see which users or groups are most at risk and adjust policy appropriately.
- **Mobile threat intelligence.** SEP Mobile uses a combination of sources to enhance its ability to identify all types of threats, including zero-days, through crowdsourced intelligence that comes from all public SEP Mobile apps (customers and non-customers) deployed globally. This helps enterprises differentiate between legitimate and malicious networks, apps, and configurations. SEP Mobile monitors devices all around the world and conducts tens of millions of security tests monthly by analyzing both the malicious and legitimate behavior of the services, apps, and networks touched by each device.

SEP Mobile's strategy starts with the proactive defense of the primary mobile operating systems, iOS and Android, and extends this by aggregating data and insights with the clients' existing EMM and SIEM solutions.

SEP Mobile offers multiple flexible pricing options ranging from per device per month to volume-based tiers. Most customers choose either the one-year or three-year subscription plans. The company also supports an unlimited ELA model.

Strengths

Symantec Endpoint Protection Mobile will gain from Symantec's cloud and threat intelligence offerings as well as the company's existing customer base and sales structure. Customers looking for a complete solution that will allow for integration into their existing systems will benefit from adding SEP Mobile's MTM product to their mix. Further, SEP Mobile has some unique capabilities that further extend the value to enterprise customers; these capabilities include its extensive crowdsourcing capabilities that inform administrators of risks on their systems and make them aware of probable risks on other systems that may not have impacted them yet.

Challenges

With the acquisition of Skycure by Symantec, there may be transition issues that could impact the current product strategy as well as deployment. As with any acquisition, there will be growing pains as the two companies merge their leadership and sales organizations and look to how the product will be developed moving forward.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Mobile threat management solutions are products delivered as either pure SaaS or hybrid on-device/cloud technology that identify vulnerabilities and malicious code on mobile devices and active attacks and exploits and mitigate these attacks. Core functionalities of the products include detection of malicious activities on mobile devices, such as apps, malware, or configuration settings. The technology can also include the ability to protect apps from attacks as well as to detect insecure or risky network connections. MTM solutions also have elements of big data analysis, as the products should collect data from deployed mobile devices and use analyzed data to improve device security – such as pushing the latest mobile OS attack profiles and behaviors or known malicious apps to devices. The cloud-connected aspect of these products also allows the technology to communicate with EMM platforms or other security information collection or mitigation points, such as security information and event management platforms or firewall/VPN/IPS infrastructure. From a broader IDC taxonomy perspective, MTM solutions by definition can also include antimalware (which includes antivirus and antispyware), antispam, intrusion prevention, and firewalls for mobile devices.

LEARN MORE

Related Research

- *IDC's 2017 U.S. Enterprise Mobility Decision Maker Survey: Key Trends for Devices, Platforms, and Wireless Providers* (IDC #US42995317, August 2017)
- *IDC MarketScape: Worldwide Enterprise Mobility Management Software 2017 Vendor Assessment* (IDC #US42890217, August 2017)
- *IDC PeerScape: Practices for Identity and Mobility Management Platform Integration* (IDC #US42775717, June 2017)
- *IDC PeerScape: Enterprise Mobility Practices for Mobile Deployment* (IDC #US42570617, May 2017)
- *Five Trends to Watch in Enterprise Mobility Management for 2017* (IDC #US42415517, March 2017)

Synopsis

This IDC study represents a vendor assessment of providers offering mobile threat management (MTM) software through the IDC MarketScape model. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for MTM software. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to its peers, and the framework highlights the key factors that are expected to be the most significant for achieving success in the MTM market over the short term and the long term.

"Mobile threat management is emerging as a must-have puzzle piece for successful enterprise mobility deployment and management," says Mike Jennett, research vice president, Enterprise Mobility Strategies, at IDC. "With the expansion of mobile usage for corporate work, the need for secure communications and the shoring up of device vulnerabilities is becoming essential, and the marketplace is responding with a robust offering of tools now available to the enterprise from MTM vendors that integrate with existing security and enterprise mobility management (EMM) tools. Integrating these tools into existing enterprise mobility deployments will expand enterprise security capabilities to handle both device and network risks associated with mobile deployments."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Trademark Notice