IDC MarketScape

IDC MarketScape: Worldwide Mobile Threat Management Software 2018–2019 Vendor Assessment

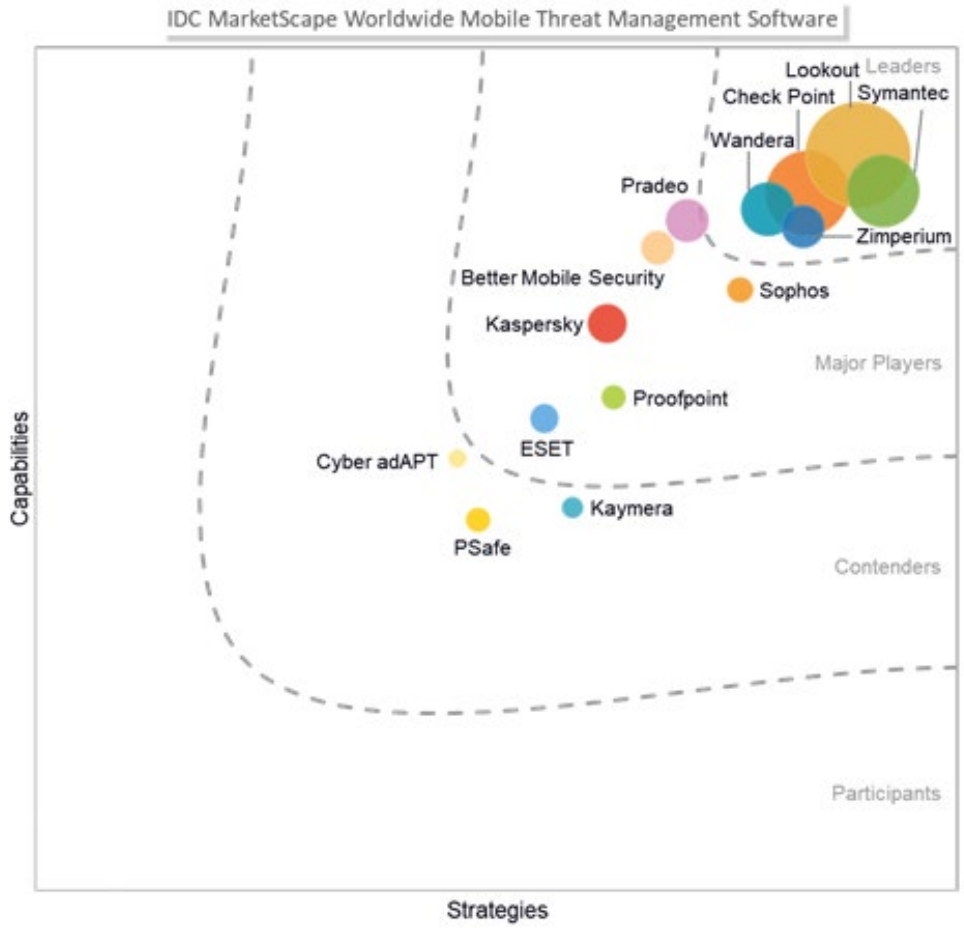
Phil Hochmuth

THIS IDC MARKETSCAPE EXCERPT FEATURES SYMANTEC

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Mobile Threat Management Software Vendor Assessment



Source: IDC, 2018

December 2018, IDC #US44521018e

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

IDC OPINION

As mobile security and governance frameworks mature, mobile threat management (MTM) software tools are filling a major security gap many enterprises are discovering across one of their most pervasive technology deployments: smartphones and tablets used by employees. Many organizations see enterprise mobility management (EMM; technology which manages, configures, and monitors mobiles) as the beginning and end of their mobile endpoint security strategy. While many EMM platforms support security functions (compliance checking, VPN connectivity, data security/encryption, and device certificate management, etc.), most EMMs do not actively scan for mobile-related threats on devices. This is where MTM technology comes in, with its ability to address actively misbehaving or malicious apps, as well as OS and network-based attacks on devices.

Driving many MTM early adoptions, and among more mature deployments, is the desire to deploy another layer of security to mobile end-user computing in addition to EMM. Among the more than two-dozen MTM customer interviews conducted for this document, 100% of these enterprises deployed their respective MTM products with an EMM platform; nearly all said that meeting existing or potential future compliance requirements was among the top 3 drivers behind their adoption of the technology. These requirements are driving much of the direction of the market from an MTM feature set and overall go-to-market strategy for MTM vendors. Key findings of this study include:

- Apple iOS and Android are the primary platforms covered by MTM solution providers, although some vendors are now supporting Windows 10, more from a tablet form factor standpoint than as a Windows PC endpoint software technology. Phishing and social engineering attacks on mobile users are an increasing focus of MTM vendors, as this is where customers are seeing the most activity and pain points. Protecting mobile email, SMS, and chat/messaging apps from malicious web links (a typical messaging attack approach) as well as embedded/sent malware is a major focus for most MTM vendors.
- Consolidation and partnering among software vendors is picking up in the MTM market, as smaller start-ups are either being acquired by larger vendors or start-ups reselling MTM software with larger vendors. Integration of intelligence integration, mitigation capabilities, and other functions of MTM with other security products and management technologies will be an imperative for vendors as MTM is integrated, or absorbed, into larger security frameworks.
- Carrier partnerships and EMM partnerships are still critical for MTM vendors in enterprise deployments; however, security integrators, distributors, and managed security providers are increasingly becoming important to MTM buyers, as customer buying centers consolidate (i.e., endpoint security teams and mobile security teams consolidating staff and budget).
- Beyond EMM, security information event management (SIEM) platforms are also now a key enterprise security platform for MTM vendors in terms of product integration and compatibility. Many MTMs now support multipole SIEMs to feed threat data and other telemetry and event data. Enterprises see this as critical for consolidating threat intelligence and events for having a more complete view of all threat vectors in the enterprise.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

A critical point in this research effort is to meet the following inclusion criteria:

- Mobile threat management, as defined for these purposes, is the protection, detection, analysis, and remediation of mobile device-based threats from a device, network, and app perspective.
- Software offerings must be standalone or primary focus must be mobile threat management. Offerings should have a client (mobile app) and network/cloud component that complement each other and provide real-time data for analysis and mitigation.
- Offering must, at a minimum, support Android- and/or iOS-based smartphones or tablets devices.
- Offering must have been available for at least one year.
- Vendors must have a minimum of $3 million in revenue for 2017 in MTM software.
- Offering must have at least two verifiable customers.

ADVICE FOR TECHNOLOGY BUYERS

This study analyzes and rates vendors across a broad range of capability- and strategy-focused criteria. As this market moves from an early stage to a more slightly more mature phase – with more acquisitions and partnerships forming among vendors and other players – enterprises need to consider criteria of MTM solutions in a broader context. Buyers must consider MTM vendors' key partnerships, adjacent technologies, and solutions integrated into larger vendor portfolios, should all:

- Look to MTM vendors that integrate well with key mobility management and enterprise security platforms, such as EMM/UEM platforms, SIEM, and threat intelligence services.
- MTM vendors with key partners in the mobile operator and carrier markets are critical in terms of deploying and supporting MTM software on devices procured through this channel. The more operator partnerships, the better. However, buyers should consider most their geographic and regional support needs from a carrier perspective.
- Consider MTM vendors with strong understanding of underlying mobile OS architectures (iOS and Android), as opposed to vendors only with strengths around antimalware and cyberthreats, as the mobile market – and interoperability of MTM software with mobile devices – is more intricate than other endpoint/device security solutions.

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 positioned as a Leader in this 2018 IDC MarketScape for MTM software. Symantec's MTM solutions are based primarily on its 2017 acquisition of Skycure, an MTM pioneer in terms of mobile app, device, and network protection. With the acquisition, Skycure was rebranded as Symantec Endpoint Protection (SEP) Mobile, a component of its larger SEP product suite for PC endpoint security. SEP Mobile provides protections across app security, device security, and network security –

an area Skycure was an early proponent and innovator, in terms of denying risky WiFi hotspots. Adding to Symantec's MTM portfolio was the October 2018 acquisition Appthority (a Major Player in the 2017 IDC MarketScape for MTM software). Appthority brings market's most advanced app inspection and reputation capabilities to Symantec's security portfolio. While Appthority had some overlapping features to Skycure/SEP Mobile in the market, Symantec has already began to integrate the stronger app reputation and app security monitoring features and incorporate these into the SEP Mobile product.

Part of Symantec's strength in analysis of mobile attacks is the wide visibility the company has with its cloud-based threat intelligence and dark web monitoring capabilities, combined with the on-device SEP Mobile enforcement. Symantec can use this to discover whether a back-end server or app platform is potentially malicious, or the reputation or risk of URLs communicating with the app. In addition, it can examine the behavior and code of installed apps and software on the device.

Symantec's integration aspirations around MTM and the company's larger product portfolio is ambitious. The company is going to market with a suite of endpoint security and security management products that extend to mobile as opposed to securing mobile as a unique or specific function. (Although SEP Mobile can be purchased as a separate product.) This is different from many vendors in the market that have MTM point products, as this integrates into broader security operations and unified/converged endpoint security and management roles in enterprises. Symantec has a threat intelligence gathering network of over 175 million endpoints — traditional and mobile — which provides enhanced security to all users.

Strengths

SEP Mobile provides advanced on-device protection and enforcement techniques with no dependency on EMM integration — critical for covering all customers' endpoints. This includes the ability to kill/block apps and processes predefined by the organization if a device falls out of compliance (i.e., if malicious apps, network connections, or device/OS-level tampering are detected). This also includes the ability to shut off email or other apps accessing corporate apps, or corporate WiFi networks.

A major strength is the ability to route devices to secure VPNs upon threat detection, as well as other device/app level and network kill switch and containment capabilities of the app. This potentially allows customers to secure mobile device activity on phones not necessarily owned and managed by the organization.

SEP Mobile integrates with a wide range of SIEM platforms, which allow for integration of security events and logging to back-end security event monitoring, orchestration, and response platforms. SEP Mobile also integrates with eight different EMM platforms, accounting for all of the most widely deployed EMM platforms.

Symantec has a very strong threat intelligence network and data gathering capability, based on its large installed base of products and other security information assets. Symantec has a threat intelligence gathering network of over 175 million endpoints — traditional and mobile to inform SEP Mobile products of threats as well as to inform other Symantec products in its ecosystem. Adding Appthority's library of app threat intelligence, which dates back to 2011, is also a competitive advantage, as competitors cannot analyze apps and versions that are no longer in the app stores.

Challenges

SEP Mobile's console has a strong feature set, especially for incident response and remediation and automatic response scenarios. However, some customers IDC spoke with said the platform requires more granularity for role-based access control at the admonitor level. Currently, administrators to the console have three levels of access: full access, read only, and "alert subscriber" alerting staff. More graduated levels of admin access, which limit visibility and capabilities for varying levels of control based on more granularly defined roles, will be necessary as SEP Mobile is deployed more in larger organizations with bigger IT and security operations staffs.

While Skycure had developed strong relationships with some carriers, Symantec currently has a formal relationship only with 1 of top 4 carriers in the United States, with fewer overall carrier partnerships than many of the leading MTM vendors. (Although Symantec does have strong overseas carrier relationships such as Vodafone Australia, Bouygues Telecom in France, and BT Mobile in the United Kingdom.

Consider Symantec When

Consider Symantec if your organization is looking to deploy MTM on mobile devices either with or without EMM management, as the SEP Mobile technology can handle both scenarios well. Also enterprises with a large Symantec endpoint, network, or content security installed base can also benefit from SEP Mobile at the portfolio level.

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 in an effort 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

- *Worldwide Enterprise Mobility Management Software Forecast, 2018-2022* (IDC #US43984018, September 2018)
- *Worldwide Mobile Enterprise Security Software Forecast, 2017-2021* (IDC #US43311217, December 2017)
- *IDC MarketScape: Worldwide Mobile Threat Management Security Software 2017 Vendor Assessment* (IDC #US42373417, September 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.

"While enterprise mobile technologies have not seen the same frequency, or severity of threats and malware as traditional PC endpoint computing, security and mobility management teams are starting to look for additional layers of security and the mobile device endpoint," says Phil Hochmuth, program director, Enterprise Mobility at IDC. "Many enterprises see mobile threat management software tools as a valuable frontline level of defense against mobile threats, as well as an emerging security technology requirement from a compliance standpoint."

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