IDC MarketScape

IDC MarketScape: Worldwide Mobile Threat Management Software 2020 Vendor Assessment

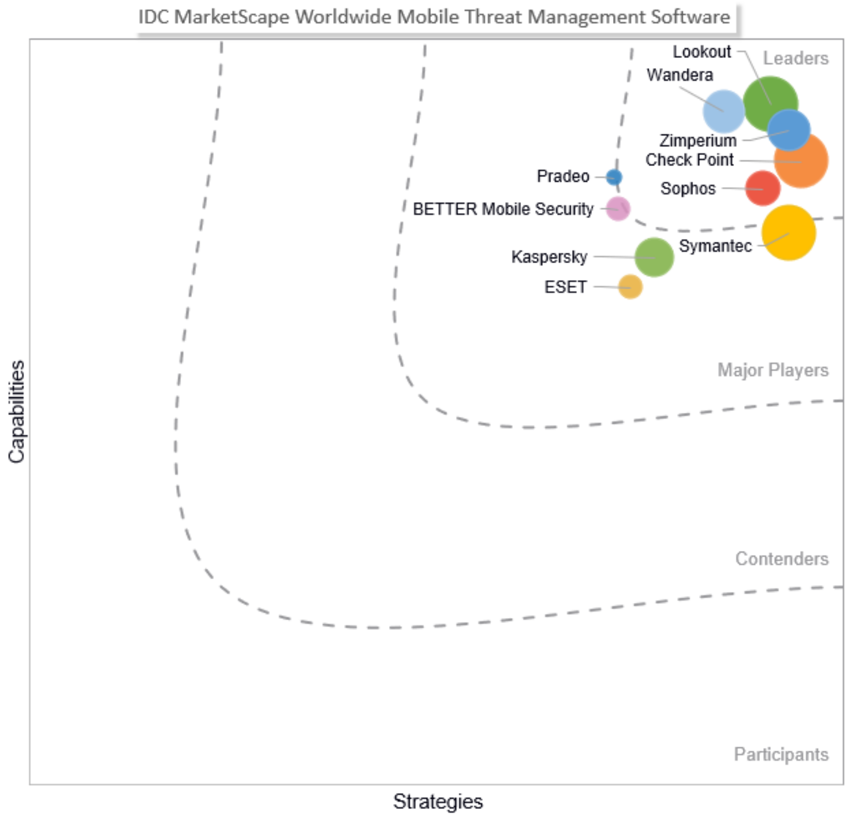
Phil Hochmuth

THIS IDC MARKETSCAPE EXCERPT FEATURES ZIMPERIUM

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Mobile Threat Management Software Vendor Assessment



Source: IDC, 2020

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

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Mobile Threat Management Software 2020 Vendor Assessment (Doc # US46092220). 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

Mobile threat management (MTM) technology is evolving from a corner case/niche product deployed mainly by government and high-security/regulated industries into a more mainstream, widely adopted security technology in the enterprise. While nowhere near as ubiquitous as endpoint security for enterprise PCs, MTM solutions are increasingly backing up enterprise mobility management (EMM) and unified endpoint management (UEM) deployments among enterprises. MTM is also proving to be a sound solution for adding security to unmanaged devices – particularly BYO iPhones and Android devices unmanaged by EMM/UEM but requiring some level of device posture checking and integration into larger security architectures based on technologies such as continuous authentication and software-defined perimeter/zero trust. These elements of mobile security are especially important in light of the current COVID-19 situation, which has more workers connecting from personal/noncorporate devices. At the same time, attackers are increasingly targeting work-from-home enterprise employees.

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 the purposes of this vendor assessment, is the protection, detection, analysis, and remediation of mobile device-based threats from a device, a network, and an app perspective.
- Software offerings must be standalone, or the primary focus must be mobile threat management. Offerings should have a client (mobile app) and a 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 2019 in MTM software.
- Offering must have at least two verifiable customers.

Vendors with MTM products on the market in 2020 but did not meet all inclusion criteria for this IDC MarketScape study include BlackBerry, CrowdStrike, Cybereason, DarkMatter, Kaymera, Microsoft, PSafe, and Proofpoint.

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:

- The MTM market is all about partnerships, integrations, and ecosystems, rather than best-of-breed threat prevention and remediation (although these core capabilities are certainly important). Look to vendors that have strong partnerships with key channels, such as mobile operators, as well as strong integrations with EMM/SIEM platforms.
- Vendors in the MTM market that also have broad portfolios of security products, or related IT/infrastructure technologies with strong integration of MTM into a larger security solution offering, should be evaluated closely — especially as the roles of security and management (for both PC and mobile) begin to converge at the organizational and functional level within IT teams (i.e., unified endpoint security).
- MTM buyers should analyze MTM vendors' capabilities and strategies from the context of securing and managing modern device operating systems (OSs) (e.g., iOS, Android, Chrome, some elements of Windows 10, and the direction of macOS with regard to kernel extension limitations). MTM technologies' strengths should focus more on anomaly detection, remediation of device access and privileges, identity-based controls, and corrective actions based on both EMM/UEM and nonmanaged device functionality. Reliance upon underlying access to device OS kernel and subsystem architectures for security visibility and remediation should be less of a focus in evaluating MTM technologies.

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.

Zimperium

Zimperium is positioned in the Leaders category of the 2020 IDC MarketScape for mobile threat management software.

Zimperium was founded in 2010 and has 160 employees in its Dallas, Texas, headquarters and other locations worldwide. It has received over $85 million in venturing funding, with investors including SoftBank, Sierra Ventures, and Samsung. The company's flagship offering, zIPS product, is an on-device MTM app with on-device machine learning, threat detection, and remediation capabilities. The zIPS product uses the company's z9 machine learning engine, which is the basis of its MTM offering. The technology can learn behavior and usage patterns of how employees interact with mobile devices and detect patterns and events that deviate from the norm and might be flagged as threats.

Zimperium's Advanced App Analysis (z3A) is another offering that scans the Apple and Google Play app installed on devices for malicious or potentially unwanted behaviors. For securely building apps, Zimperium offers its Mobile Application Protection Suite (MAPS), which can be used to build security into mobile apps through the development life-cycle process and through to deployment, including ongoing app protection and built-in app threat analysis. Zimperium also has a broad mobile device coverage with Apple iOS, Android, and Chrome OS support, which addresses the growing education vertical for mobile security, as well as emerging enterprise use cases, and remote work scenarios for Chromebooks.

As a business, Zimperium has two major partnerships, which have helped it gain visibility and broader adoption. With EMM/UEM vendor MobileIron, zIPS is the underlying technology behind the MobileIron Threat Defense — the vendor's integrated UEM/MTM security offering. Zimperium also has a white-label partnership for zIPS with McAfee, which uses the Zimperium technologies in its broader McAfee MVISION Mobile security portfolio.

Strengths

Machine learning and AI-based threat detection are key areas of strength for Zimperium. Especially relative is its on-device capabilities, which allow for threat detection of both known and unknown device, network, phishing, and malicious apps on device, even during network attacks or in a disconnected environment. zIPS does this with low system utilization (i.e., low processing/memory or battery tax on devices).

Zimperium has strong credentials for selling into federal government and regulated industries — areas where MTM adoption is the highest compared with other industries or the market overall. Zimperium has an Authority to Operate (ATO) status with the U.S. Federal Risk and a FedRAMP status.

Zimperium has broad EMM support, with over a dozen platforms supported. In addition, it has a deeper relationship with MobileIron, which OEMs the software provider's MTM solution as an integrated MTM product on top of the MobileIron EMM platform. This allows for tighter integration of zIPS detection and MobileIron-based EMM mitigation (such as conditional access controls, disconnects from VPN/SaaS apps, and device quarantine).

Zimperium's McAfee and MobileIron partnerships align well with industry trends toward unified endpoint management and security, as the markets for traditional (PC) endpoint security, device management (PC/mobile), and mobile threat management converge. These partnerships put Zimperium in a good position to integrate into broader integrated security initiatives while remaining an independent mobile security software vendor.

zIPS for Samsung Knox, a dedicated integration with Samsung business devices, allows for detailed forensics data to be pulled from devices. The integration also has local remediation, app uninstall capabilities, and advanced DLP capabilities, such as screenshot and clipboard protection.

Challenges

Zimperium does not have as extensive a carrier partnership lineup than expected given its presence in the market. However, Zimperium's go-to-market strategy of selling through security channels to security buyers (as opposed to telco/mobile teams) aligns well with the direction of the MTM market. In addition, Zimperium does partner with all major U.S. mobile carriers such as AT&T, T-Mobile, and Verizon, as well as with some major carriers in Europe and APAC (i.e., DT, Telefónica, and Telstra). The vendor's major investor, SoftBank, also has business in the mobile operator space and is a Zimperium partner.

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

- *2020 Enterprise Mobility Decision Maker Survey: Security Highlights* (IDC #US46766420, August 2020)
- *Worldwide Unified Endpoint Management Software Market Shares, 2019: Endpoint Management Convergence Drives Market Growth* (IDC #US45173520, June 2020)

- *IDC MaturityScape Benchmark: Unified Endpoint Management in United States, 2020* (IDC #US44577019, April 2020)
- *IDC MarketScape: Worldwide Mobile App Security Testing 2019 Vendor Assessment — InfoSec Emphasis* (IDC #US45459219, September 2019)

Synopsis

This IDC study assesses the market for mobile threat management software products for enterprise mobile devices. Organizations using this IDC MarketScape for worldwide mobile threat management can identify vendors with strong offerings and well-integrated business strategies aimed to keep the vendors viable and competitive over the long run.

"Many of the weak links and top threat vectors in enterprise mobile security are exacerbated by the current COVID-19 situation with massive remote workforces using personal devices," says Phil Hochmuth, program vice president, Enterprise Mobility at IDC. "Mobile threat management solutions can address some of these challenges, which include personal/BYO devices; remote, unmonitored mobile web access; unmanaged devices; questionable apps; and mobile phishing and SMS."

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