IDC MarketScape

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

Phil Hochmuth

THIS IDC MARKETSCAPE EXCERPT FEATURES LOOKOUT

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.

Lookout

Lookout is positioned as a Leader in this 2018 IDC MarketScape for MTM software. Lookout was founded in 2007 and has raised more than $280 million from top-tier venture firms and strategic partners, including an investment from Microsoft in late 2015. From its market longevity and strong consumer deployment base, Lookout has visibility into over 170 million mobile devices and has inspected over 70 million applications. This telemetry feeds into the Lookout Security Cloud, which

enterprise MTM customers can leverage to get customized and actionable visibility into emerging mobile threats and compliance risks. Lookout built its consumer installed base and network from its partnerships with mobile carriers, such as AT&T, Verizon, T-Mobile, Sprint, Orange, EE, and DT. Lookout also uses artificial intelligence tools to analyze data in its cloud, allowing it to analyze and detect new and unknown threats such as malware/malicious app variants, phishing attacks, and other sophisticated network-based attacks. All of these techniques combine for a strong mix of on-device/cloud-enabled MTM functions that can cover most mobile threat scenarios around app, device, and network-level attacks.

Strengths

Lookout recently launched an initiative it calls Continuous Conditional Access. This is based on what it calls its Mobile Risk API – RESTful API, which can trigger actions from partner EMM platforms, identity access providers (i.e., Ping, Okta, or Microsoft Azure Active Directory), and other infrastructure such as Network Access Control (NAC) and secure web gateways (SWGs). These scenarios can involve detection of risks on devices that are beyond the reach of perimeter-based security tools like firewalls and web gateways. The approach applies varying degrees of network access restriction, or other controls, enacted based on endpoint risk.

Lookout has a strong console and administrative functionality, where it can display risky behavior of devices and apps across an entire network of devices. This allows IT to create and deploy controls for these scenarios, including granular levels of inspection and enforcement, such as app-level data handling that might violate polices or desired endpoint behaviors.

In addition to discovering over a thousand malicious apps on public app stores, and thousands per day from other sources, Lookout researches and AI have discovered vulnerabilities in watchOS, tvOS, Mac OS, Safari/Mobile Safari, WebKit, Google Glass, and Bluetooth stacks.

Lookout has very strong go-to-market partnerships with over 15 carriers in the United States, Europe, and Asia/Pacific. It also integrates with more than a dozen SIEM and EMM products, which are increasingly critical enterprise platforms for mobile security and management. Close adherence to standards, such as REST API model and the AppConfig standard for mobile management functions, contributes to this.

Challenges

Lookout has strong integration capabilities with third-party security vendors and EMM platforms, but enterprise customers are increasingly looking for deeper levels of integrated security functionality, as well as product bundling and consolidated support and licensing. Recent tie-ups between endpoint security and MTM vendors point to this, as well as the increased cautions in the market by large enterprise security vendors. There is always room in the market for a strong pure-play vendor. However, as endpoint security and security teams absorb more mobile security functions, and endpoint management and security converge at an organizational level, customers may turn to more unified end-to-end platforms, which Lookout does not provide.

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