IDC MarketScape

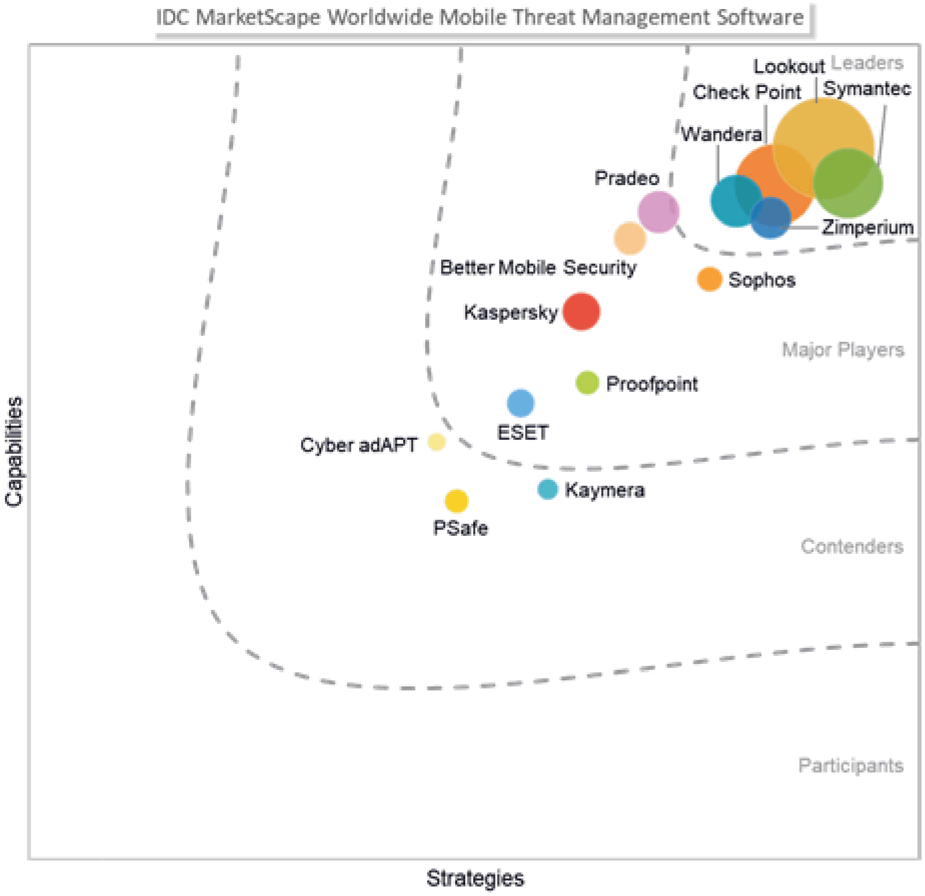
IDC MarketScape: Worldwide Mobile Threat Management Software 2018–2019 Vendor Assessment

Phil Hochmuth

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Mobile Threat Management Software Vendor Assessment



Source: IDC, 2018

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.

Better Mobile Security

Better Mobile Security is positioned as a Major Player in this IDC MarketScape for MTM software. The company was founded in 2011 and has had MTM product on the market since 2013. It supports iOS, Android, and Windows 10 devices. It's combination of cloud- and on-premise-based solutions support a mostly North American-based set of customers. The company has received approximately $4 million in venture funding.

Better's Mobile Threat Defense product consists of both an on-device app and a back-end management console that provide security administrators with a comprehensive view of devices and issues while integrating with existing EMM and SIEM products. The app protects against mobile malware as well as network- and OS/device-based attacks. Better's Mobile Threat Defense can remediate attacks directly on the device, as well as alert upstart platforms such as EMM and threat analysis and mitigation tools.

Another product in Better's lineup is App Analyzer, which looks at the operation and configuration of third-party and custom apps to identify vulnerabilities, malicious code, or unwanted behavior in software. It can alert administrators to block unsafe app downloads to end-user mobiles.

Better's mobile next-generation firewall (mNGFW) is an extension of Mobile Threat Defense, and it extends corporate firewall rules and DNS policies to mobile devices. It also can isolate apps that are detected as malicious, block apps based on country of origin, and provide for inline SSL inspections.

Strengths

mNGFW is a key differentiator for Better. It can run in as a cloud/SaaS or as an on-premise system (virtual appliance) and integrates with EMM and SIEM platforms. (Most major firewalls are supported by mNGFW: Check Point, Palo Alto, and Cisco.)

The in-app threat defense SDK is another strength. This allows for risk detection, device identification, and analysis for custom-built apps within the company. Windows 10 integration as well as Samsung Knox and Android for Work allow the solution to cover most devices.

Challenges

As a smaller start-up, Better does not have the mobile threat research staff or R&D team resources as even some of its more mature start-up competitors or larger enterprise security vendors with MTM offerings.

Better Mobile Security has fewer named carrier partners for distribution, support, and mobile services integration, which are key for the MTM market presence and expansion.

Consider Better Mobile Security When

Consider Better Mobile Security when your organization relies on network-based polices and firewall policies for broader endpoint computing security management.

Check Point

Check Point Software is positioned as a Leader in this 2018 IDC MarketScape for MTM software. Check Point, a leading network security vendor and firewall pioneer, acquired its MTM technology with the 2015 buyout of Lacoon — a forward-thinking buyout at the time when few enterprises were thinking about mobile security, even as clear threats to Android and iOS were emerging. SandBlast Mobile is now a widely used MTM platform deployed on hundreds of thousands of enterprise devices in industries such as finance, retail, manufacturing, and entertainment/hospitality. Many SandBlast Mobile customers look to the tool as a complement to existing EMM deployments or another layer of security, compliance, and assurance at the mobile endpoint.

Check Point goes to market in MTM mainly on the merits of its software standalone, although it does frequently package the product into larger endpoint, cloud, and network security-focused deals. Since

Check Point is not widely known as an endpoint security company, it often competes with other MTM solutions more like a pure-play or standalone solution. (Several customers IDC spoke with for this documents were SandBlast Mobile–only users, without other Check Point products installed; IDC did however speak with customers using mobile and network solutions.) The SandBlast Mobile solution provides strong protection across three fronts – device-level protection (anti-rooting, etc.) app scanning and mobile malware detection, and network-based attack protection (i.e., WiFi-based attacks, such as man-in-the-middle and spoofed AP/cellular network connections).

Strengths

Check Point has official selling partnerships or other go-to-market relationships with more than a dozen mobile operators and telcos. This is due to Lacoon's strong operator-focused approach when the company was a start-up, pre-acquisition. Check Point extended this approach with its own carrier relationships, and the company now has more carrier partnerships than any vendor in this document.

Check Point can integrate SandBlast Mobile into its larger administrative and threat monitoring console, allowing customers to touch and view multiple security products throughout a network, from smartphones and tablets to VPN, firewalls, IPS, and cloud security technologies such as CloudGuard SaaS (Check Point's cloud access security broker [CASB] solution).

A major integration point for SandBlast Mobile is Check Point's ThreatCloud security intelligence product, which feeds the MTM software with information on newly discovered threats, as gathered from across Check Point's entire installed base of active, opt-in ThreatCloud users (millions of devices and security gateways worldwide).

Check Point can do all inspection and mitigation functions on device without routing traffic through a proxy or cloud service. This includes antiphishing, antibot, URL filtering, safe browsing, conditional and access capabilities.

Challenges

SandBlast Mobile integrates with several leading SIEM platforms (IBM and Splunk), as well as Check Point's own product. However, support for SIEM platforms was not as broad as other leading MTM vendors.

Customers IDC spoke with said that their experience with Check Point sales/post-sales teams was inconsistent in terms of account representation – especially, if they were only customers of SandBlast Mobile and not a larger Check Point account (i.e., using firewalls and IPS from the company).

Consider Check Point When

Customers looking for threat prevention capabilities such as antiphishing, antibot, safe browsing, URL filtering, and conditional access, either with or without EMM integration should consider Check Point. Furthermore, customers looking for strong integration and support from mobile operators for advanced MTM (network, device, and app-level security) functionality should look to Check Point as a potential solution. Customers with larger deployments of Check Point security solutions should also consider the vendor for integration and bundling/pricing opportunities.

Cyber adAPT

Cyber adAPT is positioned as a Contender in this 2018 IDC MarketScape for MTM software. Cyber adAPT, founded in 2014, is focused on advanced persistent threats (APT; as the company name implies), with solutions that span network/cloud deployments, traditional PC endpoint, and mobile, under the company's skwiid solution brand. The skwiid platform is a network traffic analysis and anomaly detection platform that is deployed throughout an enterprise infrastructure via software-based agents. The technology creates a baseline of "normal/safe" behavior and then detects deviations from that based on live activity. It remediates potential attacks with this approach across network and endpoint enforcement. The skwiid mobile product taps into this function and extends to smartphones. The solution is based on an on-premise network appliance and an agentless mobile technology. This provides encrypted traffic tunnels to mobile connections, which can eliminate man-in-the-middle attacks and other network-based threats.

Strengths

The company has very strong network-based attack features for mobile devices, which protect against the top challenge most enterprises say they face in terms of mobile threats (according to IDC survey data).

The solution integrates well with the larger skwiid platform, allowing for bundled pricing, integrated policy creation/enforcement, and other monitoring and analytics features combining endpoint with network capabilities.

Challenges

The company has limited on-device security capabilities, such as app reputation or app behavior analysis, as most of its monitoring and mitigation functions are based on the company's network and packet inspection technology and its associated threat intelligence cloud service.

Consider Cyber adAPT When

Companies particularly concerned about mobile network traffic security (whether mobile internet or WiFi) should consider the Cyber adAPT skwiid platform, especially if deploying the solution at a larger scale across the enterprise (i.e., the network and traditional PC endpoint products).

ESET

ESET is positioned as a Major Player in this 2018 IDC MarketScape for MTM software. ESET, based in Prague, is a 30-year-old endpoint antimalware vendor with security solutions in advanced/targeted attack prevention, identity, messaging security, and security professional services arm serving enterprise and SMBs, as well as consumer. The company has over 1,600 employees worldwide and supports multipole security R&D centers focused on advanced malware research. The company offers its ESET Endpoint Security for Android as a mobile, a complement to its large PC endpoint security business, which serves millions of PCs. The mobile solution covers specific mobile threats, such as mobile ransomware/device takeover attacks, data loss prevention on business mobile devices, application control/security features, and remote management and configuration capabilities (similar to EMM functions but not a full-function EMM platform). The Endpoint Security for Android solution integrates with ESET's Management Server platform, allowing security administrators to create and deploy common security polices and monitor threats across smartphones and PCs running ESET software. The device compliance and management functions can restrict applications installed on devices, enforce encryption and pass codes, and control what WiFi networks' mobile devices can access. These management-focused functions can run on both Android and iOS solitons, whereas the mobile antimalware function is only covered on Android.

Strengths

The integration into ESET's larger product portfolio is a strength for customers standardized on ESET security products. The converged PC/mobile security and management functions are especially valuable if companies are managing large fleets of BYOD Android devices in the workplace.

ESET is a strong threat research and R&D organization as well as being among the first security companies to discover the emergence of Android-based ransomware. This work feeds into the larger threat intelligence cloud service and data feeds all ESET products, including the mobile solution, can access.

Challenges

As the product name implies, ESET Endpoint Security for Android does not support iOS, specifically for the mobile antimalware and app monitoring and behavior control functions of the software. Apple devices are supported from the device management and configuration functions of the ESET endpoint management solution for mobile (a plug-in that integrates with the larger ESET platform).

ESET has very few partnerships with key mobile channels, especially carriers, which are a primary source for mobile security software for a majority of enterprises.

Consider ESET When

Consider ESET if your organization already has, or is planning to migrate to, ESET as a standard endpoint and data security management platform. Organizations with a large fleet of Android, or Android-exclusive enterprises, should also consider the company for its strong support for this mobile OS from an MTM and management standpoint.

Kaspersky

Kaspersky Lab is positioned as a Major Player in this 2018 IDC MarketScape for MTM software. Kaspersky Lab, founded in 1997, is antimalware software pioneer and leading thereat research lab and has been active in mobile threat research and mitigation for over a decade, since the launch of modern smartphone operating systems with iOS and Android. Kaspersky has offered mobile threat management tools as sperate products in the past, and it previously had offered MTM capabilities as an add-on to its mobile device management (MDM) platform. The software vendor has settled on integrating MTM functions more closely with its Kaspersky Endpoint Security for Business.

Rather than requiring companies to adopt Kaspersky MDM/EMM, the company is partnering with leading EMM providers (BlackBerry, IBM, Microsoft, MobileIron, and VMware). By decoupling MTM from its own MDM platform, the company is opening its platform up to a much broader potential customer base. The move to couple MTM with its endpoint security platform also helps organizations standardize on Kaspersky endpoint security with MTM product selection and integration.

Strengths

Kaspersky's MTM functions are part of the company's Kaspersky Endpoint Security for Business – a full set of endpoint, servers, and network security solutions. This converged or unified endpoint security management approach can allow teams to analyze threats across every type of endpoint in an enterprise and provide more unified and coordinated polices and enforcement rules across multiple device types.

The focus of Kaspersky's MTM capabilities is on Android, and the company provides very strong functionality here, including cloud-based antimalware with cloud-assisted threat intelligence. Kaspersky also has strong Android content security capabilities, including antispam to block unwanted calls and SMS texts, as well as safe web filtering and antiphishing to block access to malicious and other unwanted websites.

Kaspersky has strong application control and setup or restrictions for apps on Android. It integrates with Google Firebase Cloud Messaging (Android) and Apple Push Notification Services (iOS) to enable near-immediate configuration controls and enforcement.

The integration of Kaspersky MTM with its overall endpoint security suite is a forward-thinking approach to endpoint security that reflects the converging nature of mobile and PC device management and security. While leaving the converged management up to EMM vendors, Kaspersky is one of only a few large, mainstream endpoint security vendors with a converged PC/mobile endpoint security solution.

Challenges

While Kaspersky has very strong Android MTM features and is among the preeminent threat researchers for Android-based malware, the company's iOS features and support doesn't match up. This is a challenge for enterprises with mixed iOS/Android environments (the majority of enterprises in the United States) as well as firms that have standardized on iOS (more than one-third of large businesses in the United States). Kaspersky says it focuses on Android because it believes the open nature of the OS exposes it to more threats. Also Android provides more access and visibility to third-party MTM solutions. This can be a greater benefit than supporting a more closed mobile OS with more limited MTM integrations, the company says.

Kaspersky has faced challenges in the market because of recent geopolitical issues between Russia and the United States — among them calls by U.S. Senators and government agencies for United States-based businesses to avoid the software, out of fear of foreign tampering and spying. Kaspersky maintains that it is an independent, private software company with no involvement with the Russian government.

To address concerns regarding unauthorized access to customer data, the company launched its Global Transparency Initiative in 2017, and Kaspersky Lab's first Transparency Center is located in Zurich (Switzerland). The Transparency Center allows customers and other trusted stakeholders to review the company's source code, software updates, and threat detection rules. The company will also install the new infrastructure necessary to collect, process, and store detection data from European customers in Zurich. Full relocation of data from European countries will be completed in 4Q19, with other countries to follow.

Consider Kaspersky When

Consider Kaspersky when your organization is largely deployed with Kaspersky endpoint security solutions. Kaspersky can provide a common deployment and security management platform, along with integration security analytics and policy creation/enforcement capabilities. Companies headquartered outside of the United States, or United States-based firms with subsidiaries or operations in EMEA, Central/Western Europe, and APAC may also be a good fit for a converged Kaspersky MTM/endpoint security solution.

Kaymera

Kaymera is positioned as a Contender in this 2018 IDC MarketScape for MTM software. Kaymera, an Israel-based mobile security vendor, was founded in 2015, and offers a range of mobile security products, from its MTM solution to a voice/texting security encryption suite as well a full secure mobile OS platform (based on Android modification and hardening). The company's CipherWatch MTM product provides network, app, and device-based security functions, including man-in-the-middle and rogue WLAN AP protection, traffic encryption, repackaged app detection, bad app behavior detection, as well as jailbreak, malicious device profile, and other deice hijacking and takeover techniques. The company claims it can enforce policy and mitigate threats across these threat areas with or without EMM integration, but does integrate with some EMM platforms, as well as some SIEM platform for security event integration.

In addition to CipherWatch, Kaymera also develops and markets a solution for security mobile communications – CipherBond product. This product claims to encrypt voice traffic between two devices running the software, as well as encrypting SMS/text messages between Kaymera-managed mobiles. Secure document/media sharing and group messaging are also features of the product. Last, the company's CipherFort product is a custom-modified version of the Android Open Source Project software stack, which adds additional security functions to the code, such as full-disk encryption/data extraction protection, as well as the CipherWatch and CipherFort MTM and secure communications features. Kaymera also offers a Command Center product that provides unified views on activities, threats, and incidents across the three products.

Strengths

Kaymera's MTM capabilities are strong, multiplatform (Android and iOS), and cover the three major MTM security areas of network, device, and application security. The company has a lightweight agent that can work on or offline.

The integrated suite of Cipher-branded mobile security products can cover a lot of mobile security use cases and could be a good choice for deploying and monitoring mobile security tools to a segment of high-risk/high-value end users or groups (e.g., corporate executives, government officials/workers).

Challenges

Kaymera is a small player with limited cloud-based threat intelligence and scale compared with larger security vendors with MTM products, or even some start-ups with larger installed bases and infrastructures.

The company only partners with two EMMs (VMware and MobileIron) and has limited interoperability with SIEM platforms. (It supports standard SIEM data interfaces but has no official integration or go-to-market partners.)

Consider Kaymera When

Kaymera should be considered if an organization is looking to deploy corporate-owned mobile devices with high security to a limited or controlled subset of users or teams. Companies adopting the Cipher suite of solutions, plus the monitoring/management platform, will get maximum benefit compared with just adopting one or two products.

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.

Pradeo

Pradeo is positioned as a Major Player in this 2018 IDC MarketScape for MTM software. Pradeo is a France-based MTM vendor, founded in 2010, with more than $10 million in investment and offices in San Francisco and Paris. Pradeo has artificial intelligence technology that is used to provide risk scoring across a range of mobile endpoint areas, such as app risk, device/OS-level risks, and other factors in smartphone technology security. The company also has a sophisticated app reputation and app behavior anomaly detection capability to go with its OS-level and network-level threat awareness. In addition to an MTM tool, Pradeo also has a strong mobile application security testing (MAST) technology used by application developers, ISVs, and enterprises to secure and lock down features and close threats on mobile applications delivered to end users and customers. This complementary tool does not overlap with MTM buyers in most enterprises. (MAST buyers are typically not MTM users.) However, the product offering leverages an area of expertise in Pradeo and opens the company to another potential buying center in enterprise accounts, as well as customers outside of the MTM space interested in secure mobile app development (i.e., app creation outsources, agencies).

Strengths

Pradeo's AI capabilities are a strong differentiation for the company with regard to its threat detection and analysis capabilities. The company's founders come from an AI background and leverage this expertise as the core of its SaaS-based threat analysis engine. The company uses multiple threat feeds, app store data, and other sources, as well as information from partners, as inputs to its AI threat modeling.

The company has mobile security strengths across three broader areas than MTM, including mobile application security testing and in-app (or SDK based) protection for third-party mobile apps. This gives highly mobile-centric enterprises and ISVs a strong set of tools across a range of scenarios and use cases.

Pradeo has a unique relationship with Samsung to expose Samsung Knox security enforcement features with Pradeo MTM detection functions. This makes Pradeo the only officially partnering MTM vendor with the largest enterprise Android smartphone brand in the industry. The relationship provides not only technical integrations that allow for event triggering and mitigation on device for Pradeo detection and Samsung Knox enforcement but also a go-to-market validation opportunity for Pradeo.

Pradeo leverages its detection capabilities to provide readability into personal data manipulation in light of GDPR.

Challenges

Pradeo has fewer carrier channel relationships than many of its larger competitors. While it has stronger carrier pacts in Europe (e.g., Orange, T-Systems), it lacks relationships with many of the large U.S. carriers. This puts the company at a disadvantage, although its Samsung device partnership can help the company piggyback into some accounts off of carrier partnerships the company has with the smartphone OEM. The company is also in talks to expand with U.S. carriers in 2019.

The EU is a target-rich environment for selling security and privacy tools (given the GDPR requirements and overall security/privacy focus of firms in the region), and Pradeo has had great success there with several Global 2000 accounts with large deployments of software. However, Pradeo's low presence and revenue share in North America and other regions is a challenge, as these are the biggest market opportunities for MTM software overall. Moves to integrate with Microsoft Intune and the Samsung partnership should help spread the technology beyond its home region to larger markets with more exposure.

Consider Pradeo When

Consider Pradeo if your organization has a large, or primarily, European-based footprint. Also companies that are heavy Samsung device users, or completely standardized on Samsung Android devices, should consider the integration capabilities between Pradeo and Samsung Knox. (The company also supports Apple iOS and Windows 10 devices as well.)

Proofpoint

Proofpoint is positioned as a Major Player in this 2018 IDC MarketScape for MTM software. Proofpoint is a publicly traded, widely known vendor in content and messaging security (partially email/antispam and phishing protection and message encryption). Proofpoint offers a separate Mobile Defense product, which it says addresses device, network, and app-based security threats for mobile devices (Android and iOS supported). On the network front, the solution can analyze WiFi network security to detect mobile threats, attacks, and bad network configurations (man-in-the-middle attacks being the primary threat). The on-device client also analyzed mobile OS/hardware behavior, such as spikes in OS and memory usage, unknown configuration profiles, and other signals of system tampering that could be due to an unknown attack or harmful application. Proofpoint combines its SaaS/cloud-based content security capabilities (messaging/antiphishing, advanced threat detection) with its Mobile Defense offering to augment the on-device mobile phishing and zero-day attack detection.

Strengths

Proofpoint Mobile Defense is a full-featured MTM (network, app, device protection) that draws from the company's strengths in antispam/phishing protection. The mobile product is strengthened by the larger security technology offerings from Proofpoint.

Challenges

Proofpoint has limited deployments of its Mobile Defense solution, mainly among its installed base. The company is not widely involved in large, competitive MTM deals or product RFPs.

The company has a limited number of official go-to-market and technical integration partnerships among top EMM and SIEM platform providers.

The mobile security solution is less effective if deployed without other Proofpoint products, limiting the products potential scope of addressable customers and use cases.

Consider Proofpoint When

Consider Proofpoint if your organization already standardizes on the vendor's content and cloud security solutions and is looking for a complementary and integrated MTM solution. Proofpoint customers can likely get bundled or reduced pricing on packaging the MTM product into larger Proofpoint deployment deals.

PSafe

PSafe is positioned as a Contender in this 2018 IDC MarketScape for MTM software. PSafe is a Brazil-based mobile security technology start-up founded in 2010. The company has raised more than $86 million in funding and has over 300 million installs, according to Apple/Google app store data. The company is more consumer focused but has large deployments among midsize and some enterprise firms, especially in Latin America. The company's "dfndr security" MTM app (iOS and Android) includes malicious app/mobile malware protection capabilities, some WiFi-based attack detection capabilities, and system monitoring functions for detection of device/OS-based attacks based on anomalous device behavior. The company also has a range of complementary mobile security and management apps for personal use: dfndr vault (secure content protection) and dfndr VPN (mobile VPN for traffic security and privacy). It also has a battery optimization and memory optimization tools.

Strengths

PSafe is a relatively low-cost, high-value MTM solution that covers more attack scenarios than most consumer-focused solutions and includes a range of additional tools and features that are particularly business oriented.

Challenges

The company is more of a consumer-focused vendor, with a free version of the product that is ad-supported and a paid version with limited additional features (besides eliminating ads).

The product has no central control or management platform for analytics device configuration. Also PSafe does not support EMM integration or SIEM platform integration.

Consider PSafe When

Organizations based in Latin America, or with large user bases with BYOD devices, might consider deploying or supporting user adoption of PSafe as a base layer of security for noncorporate devices.

Sophos

Sophos is positioned as a Major Player in this 2018 IDC MarketScape for MTM software. Sophos is a United Kingdom-based security software vendor spanning endpoint/antimalware, network, data protection, and content security solutions with a worldwide customer base of over 300,000 SMBs and enterprises. While the company offers individual security products across six IDC functional markets, Sophos' solutions are commonly deployed together for a holistic security architecture around threat detection and remediation. In the mobile market, the company's Sophos Mobile UEM solution is a competitive mobile and PC management, deployment, configuration, and security solution. Sophos Mobile Security is the company's MTM offering, launched in 2017. The product is an iteration of its earlier Sophos Mobile Control (introduced in 2013) and Central Mobile Security products.

Sophos Mobile Security provides all major mobile attack detection/prevention capabilities around device/OS, applications, and network-based attacks. This includes jailbreak detection, malicious app and app reputation checking, WiFi man-in-the-middle attacks, web filtering, and malicious SMS and call spam protection.

Strengths

Being in the market for over 30 years, Sophos has a strong mobile technology foundation. It has a large threat research and product R&D staff overall, and it has many specialists in mobile malware research and mobile OS/device threat modeling, with several patents in the area of mobile security technology.

Sophos has its own EMM/UEM platform, which integrates tightly with Sophos Mobile Security. The company also has a broad suite of security products; endpoint security, network, content, and data security tools; and Sophos Central administration platform. Customers deploying Sophos UEM solutions, as well as Sophos Endpoint and Mobile Security products, could have a single-vendor unified endpoint security/management solution — the only vendor across the mobile and endpoint security/management markets with such an offering.

Beyond its own EMM, Sophos Mobile Security integrates well with other EMM and SIEM platforms. It has a strong integration capability with Microsoft Intune, particularly around conditional access controls and the Sophos MTM agent: the agent can trigger Intune controls to block, or challenge, credentials and access to Office 365 and other Microsoft-protected resources if threats are discovered by Sophos Mobile Security on devices.

Challenges

Since Sophos sells its Mobile Security solution primarily as a suite product with larger Sophos deals and through its security reseller channels, the product and brand is not as widely known in the market as compared with leading vendors' solutions.

Carriers and EMMs are the key conduits to MTM software propagation in the market. However, Sophos has fewer integrations and go-to-market relationships among the top-tier carriers and EMM software vendors compared with leading vendors. The company does have strong tie-ups with some major European and U.S. operators (Telefonica and AT&T), but other MTM leaders had much broader distribution deals among mobile operators. And while Microsoft integration is important, as Intune will be a key platform in the EMM/UEM space over the next several years, Sophos had few other formal partnerships in the EMM space beyond Microsoft and its own product.

While Sophos has a strong feature set for iOS and Android devices, it does not have feature and functional support parity between the platforms. Several key capabilities, such as app reputation, malicious app detection, and side-loaded app detection, are not supported on iOS (but are supported on Android). While the Android use in the enterprise continues to grow, Apple devices are still the dominant corporate-liable smartphone technology (by shipments) in major markets, such as the United States. While Apple does not allow as deep access to its operating system, application permissions, and other capabilities as Android, many vendors in the market are able to address iOS security requirements.

Consider Sophos When

Companies with all-in deployments of Sophos security solutions, or even those using the EMM platform alone, should consider Sophos Mobile Security for a short list of MTM products. Microsoft Intune users should also look at the Sophos MTM offering for its strong conditional access features. Also organizations more concerned about Android threats should consider Sophos Mobile Security for an MTM deployment.

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.

Wandera

Wandera is positioned as a Leader in this 2018 IDC MarketScape for MTM software. Wandera is a cloud-centric MTM vendor founded by veterans from the secure web gateway market (ScanSafe, sold to Cisco, a decade ago). Wandera's MTM solution includes capabilities that span both the mobile endpoint and the mobile network; it is sold mainly through mobile operator channels as well as managed service providers and security solution resellers. The company is different from other vendors in the market in that it augments on-device MTM capabilities with an optional cloud-based inline mobile traffic inspection service, which can enforce policy on mobile data traffic from a security perspective, but also from a consumption and usage perceptive, in terms of data usage monitoring and even bandwidth throttling in cases where end users might be roaming and consuming expensive bits of module data.

Wandera can provide device-based, app-centric, and network-centric protections for iOS and Android devices, as well as Windows 10 devices, allowing it to span both PC/tablet and smartphone deployments. Wandera has deep technical integrations with over 10 EMM vendors (VMware, MobileIron, and IBM MaaS360 are among them), which offer streamlined device life-cycle management features, allowing for stronger policy enforcement options on managed mobile devices.

Strengths

Wandera provides mobile defense in depth and offers a variety of independent enforcement points that allow organizations to effectively manage risk across the security, legal, financial, and compliance use cases. The solution components can be deployed in different configurations to support a variety of management strategies, from BYOD to corporate managed.

The inline gateway capabilities of Wandera are a differentiation strength of the solution. The gateway can control access to unauthorized online mobile web and app activities, as well as monitoring usage of cloud storage services, which may not be allowed by some organizations. Wandera has the ability to block both apps and browser access to services that fall under various IT categories. Sitting in the data path allows Wandera to monitor access to third-party app stores, either preventing the stores from being accessed or scanning authorized app downloads before they are installed on devices. The gateway functionality also has use cases beyond security in terms of data usage monitoring, roaming data charge control, and overall analysis of mobile worker data usage patterns (valuable to finance and telecom planning teams at enterprises).

Wandera has a significant number of mobile operator partnerships, which provides the company with a strong go to market. In some cases, Wandera's services, data, and reporting are integrated with the carrier, allowing them to automate provisioning, deliver enhanced data, build their own interfaces, and extend managed services.

Wandera recently announced a go-to-market partnership with IBM to sell/support Wandera's MTM solution through IBM's MaaS360 sales channels and support organization. This provides a strong tie between the two platforms — both with similar carrier and MSP channel partners. It also allows for single-source purchasing (Wandera goes on IBM's price book) and first-line support for customers of the combined technologies.

Challenges

Being known primarily for its cloud-based service with inline inspection could be seen as a disadvantage to enterprises that prefer on-device threat monitoring, especially if devices have limited or sporadic connectivity or are largely offline or WiFi only devices. Even for connected devices, if the Wandera cloud becomes unavailable or limited, this could affect the ability to detect and protect against mobile threats. While Wandera does have noncloud/on-device detection and remediation capabilities, it is known in the market more for its cloud-based proxy and inline traffic enforcement.

Consider Wandera When

Companies looking for real-time, cloud gateway policy enforcement of mobile traffic should consider Wandera for its MTM deployment. Also, organizations interested in applying traffic monitoring, analysis, and bandwidth/cost management functions to business mobiles via a gateway platform should also consider Wandera.

Zimperium

Zimperium is positioned as a Leader in this 2018 IDC MarketScape for MTM software. Zimperium, a six-year-old MTM start-up, has 146 employees; is based in Dallas, Texas; and offers its zIPS MTM product on Android, iOS, and Windows 10-based tablets as well as zIAP, an SDK for embedded app security, and z3A for advanced app analysis. The company has raised more than $60 million in four rounds of venture funding, with backers including SoftBank, Samsung, Sierra Ventures, Telstra, and Warburg Pincus.

Zimperium provides on-device and cloud-assisted threat detection for app-based/mobile malware threats, OS/rooting-focused threats, as well as network attacks (WiFi and cellular based). The company also has antiphishing (mobile email and SMS protections) for mobile devices. The company has several large-scale deployments in Fortune/Global 1000/2000 accounts as well as government agencies. Recently, the company's zIPS technology was deployed at scale in the City of New York's public mobile security and public WiFi access/security initiative for New York citizens. In addition, beyond zIPS, the company also has a mobile application security tool in zIAP, which is used to build security features into other mobile apps via an SDK for third-party software developers. The zIAP product has been deployed in mobile apps, protecting over 25 million users.

Strengths

Zimperium's zIPS product has a strong machine learning (ML)-based core function, which creates a baseline of normal mobile device activity and behavior, then monitors, alerts, and mitigates threats based on deviations from the baseline. The zIPS product uses cloud-trained ML engines to create its security baselines, then uses device-level functions to detect, monitor, and react. The device-level capabilities can function without connectivity to Zimperium's cloud service, allowing the detection to take place under any circumstances. The product provides this protection with low system utilization (i.e., low processing/memory or battery tax on devices).

Zimperium has broad EMM support, with over a dozen platforms supported, offering a wide range of enterprise-class mitigations. In addition, it also has a resale relationship with MobileIron, where the EMM vendor sells Zimperium MTM software as MobileIron Threat Defense. This allows for tighter management and integration of MTM detection and MobileIron-based EMM mitigation (such as conditional access controls, disconnects from VPN/SaaS apps, device quarantine).

Zimperium recently became a key OEM partner with enterprise security software giant McAfee. Zimperium's products will be the basis for McAfee's MVISION Mobile solution. McAfee MVISION is an effort to consolidate visibility and threat/risk-state sharing across all McAfee security products (endpoint, network, content, datacenter, etc.). Without its own MTM solution, McAfee assessed all market players and chose Zimperium as a critical OEM partner to fill this gap in the mobile aspect of its MVISION architecture.

Challenges

While Zimperium has strong mobile operator partnerships with firms such as AT&T, Sprint, T-Mobile, Telstra, and SoftBank, its list of carrier partners is not as extensive as many of its peers. This could hinder the company in larger opportunities, especially with multinational enterprises looking for multicarrier support in multiple regions (e.g., North America and Western Europe, or LATAM)

Consider Zimperium When

Organizations looking for strong app/device/network protections with on-device functionality should consider Zimperium for MTM deployments. In addition, large McAfee customers looking to take advantage of its MVISION approach in mobile should also consider Zimperium technology as part of a larger enterprise endpoint security architecture.

Other Mobile Security Solutions

Many security vendors offer solutions that address several aspects of mobile security, such as BYOD security and control, mobile VPN provisioning, or mobile content security. While many of these offerings address some use cases of MTM, they are not actual MTM products; either the solution provides no on-device client, relying entirely on cloud or gateway-based traffic security controls or the offering falls short in other areas, such as app- or OS-level protections. Some vendors in this category are:

- **Cisco**: Cisco, the network industry giant, has a range of solutions to address mobile device BYOD security scenarios. From its strength in networking, the vendor's Identity Services Engine (ISE) can provide network-to-employee policy controls applying specifically to mobile devices attached to Cisco network infrastructure and beyond. The company's Umbrella cloud security service provides mobile traffic proxy and policy enforcement for mobile internet users, and the company's recent acquisition of cloud identity and BYOD security vendor Duo Security adds more capabilities. The company's Cisco Meraki Systems Manager, and EMM platform, also has mobile device security functions.

- **Palo Alto Networks**: Palo Alto is a provider of firewalls and other network security products and cloud services. The company positions GlobalProtect, its cloud-based firewall, as a mobile security solution, allowing mobile devices attached to the internet to have traffic inspected and filtered by the Palo Alto security SaaS technology.
- **Zscaler**: Zscaler offers a cloud-based secure web gateway product, used widely to control internet and web traffic for enterprise sites and individual users. The cloud-based web security product can provide mobile protection by acting as a cloud-based security proxy service for 4G/LTE-connected mobile devices; all mobile web traffic is run through the Zscaler cloud, where it can inspect traffic and enforce polices on web access, as well as detect network-based threats. The solution can also help monitor and throttle mobile bandwidth usage based on consumption thresholds.

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

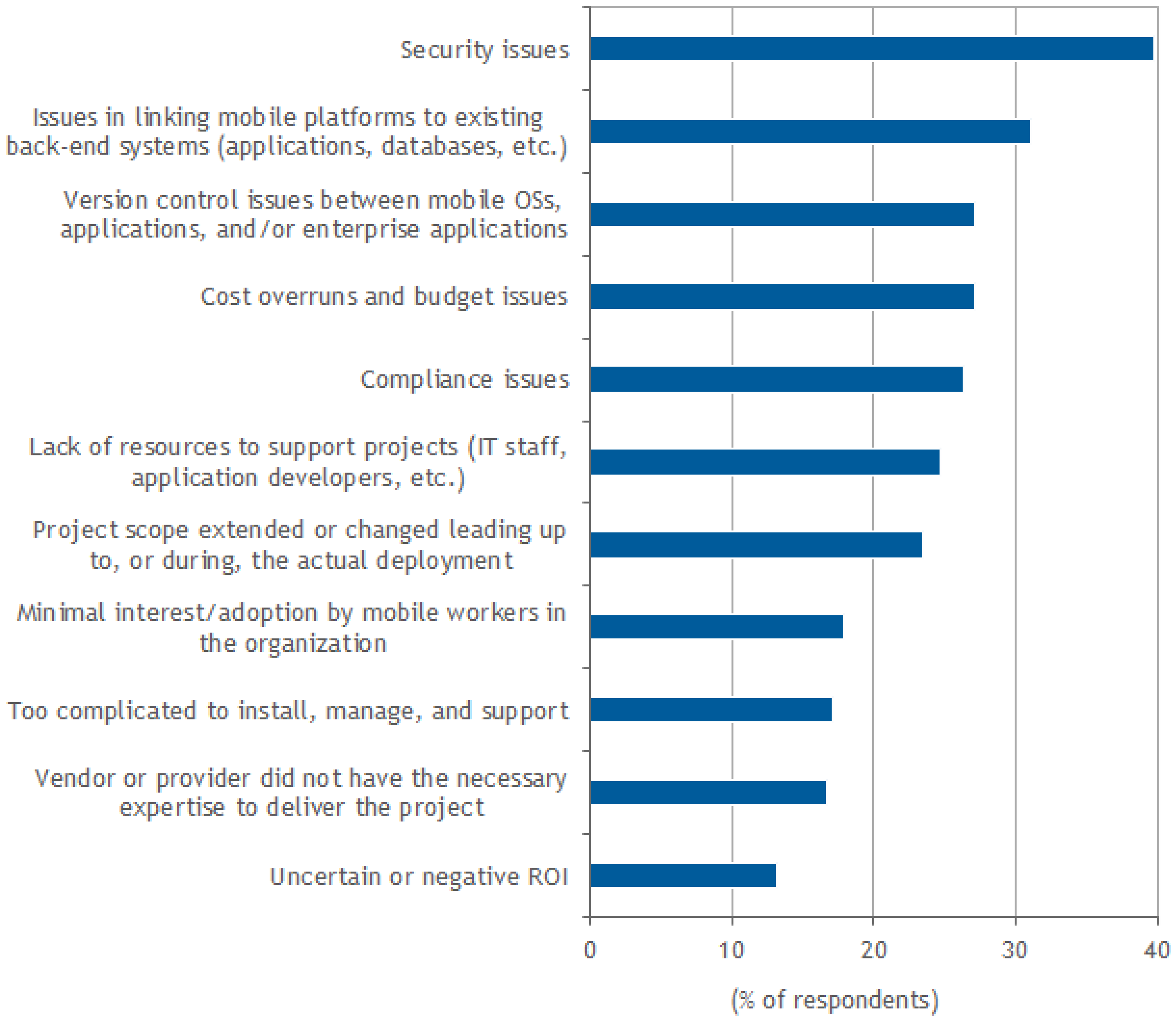
Mobile threat management solutions are products delivered as either pure SaaS or hybrid on-device/cloud technology that identify vulnerabilities and malicious code on mobile devices and active attacks and exploits and mitigate these attacks. Core functionalities of the products include detection of malicious 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.

IDC Mobile Security Survey Findings

In 2018, IDC surveyed 250 enterprise mobility decision makers about top mobility deployment challenges, buying decisions, and other factors involved in mobility management in security. Among the top challenges overall facing enterprises deploying enterprise mobile technology, security was the most frequently cited issue (see Figure 2). When asked about top security challenges facing enterprise IT mobility decisions makers, after lost/stolen devices, network-based attacks were the most frequently cited threat mentioned by respondents (over 30% said they'd experienced this issue in their environment). Mobile phishing/malicious SMS messages were the most common security incident, followed by malicious or unwanted apps on end-user devices (see Figure 3).

FIGURE 2

Top Challenges in Mobility Deployments

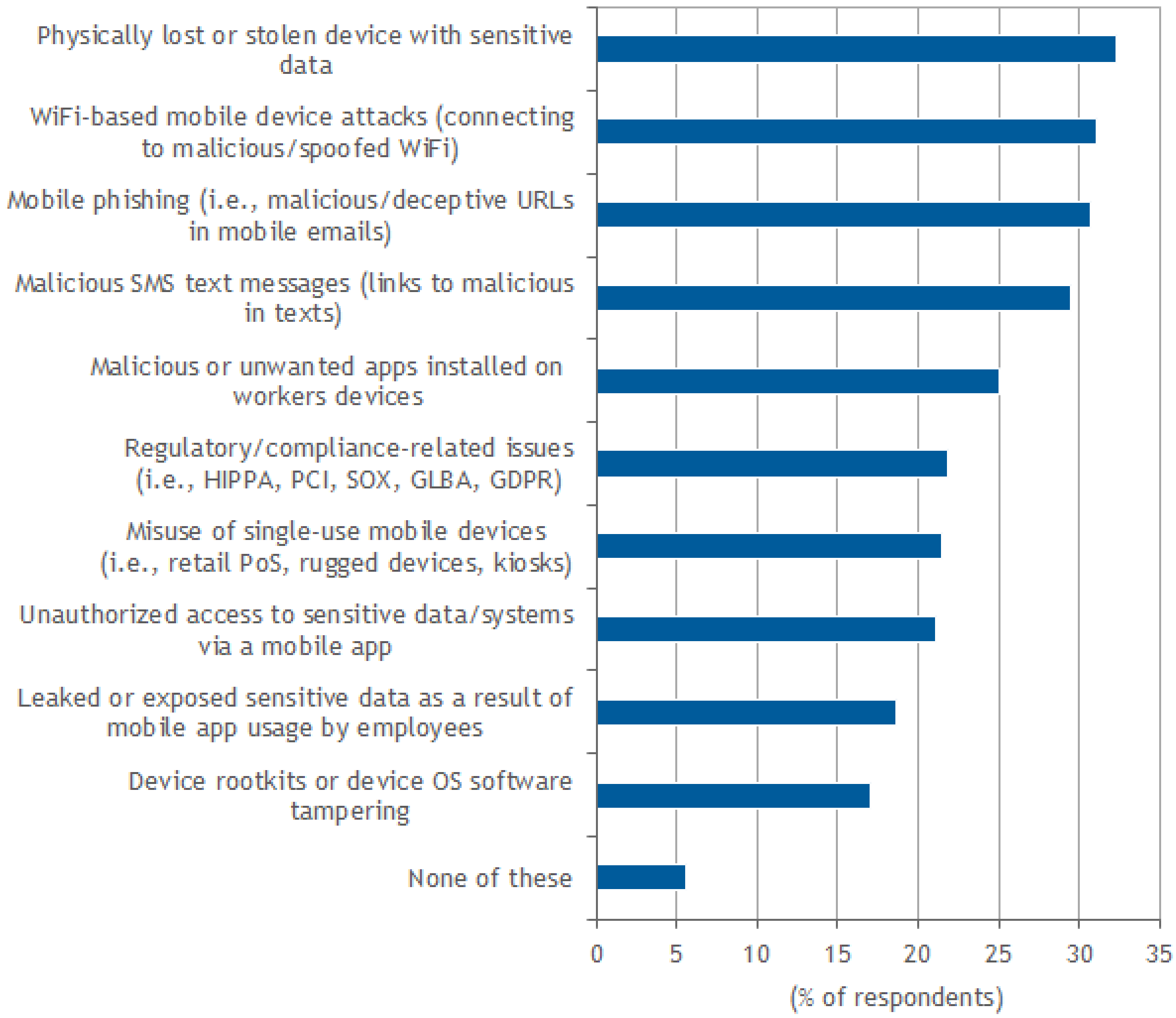


n = 250

Source: IDC's *Enterprise Mobility Decision Maker Survey: Software*, 2018

FIGURE 3

Top Mobile Security Issues



n = 250

Source: IDC's *Enterprise Mobility Decision Maker Survey: Software,* 2018

Strategies and Capabilities Criteria

Tables 1 and 2 provide key strategy and capability measures, respectively, for the success of mobile threat management software vendors.

TABLE 1

Key Strategy Measures for Success: Worldwide Mobile Threat Management Software

Strategy Criteria	Definition	Weight (%)
Functionality or offering strategy	There is a road map based on customer and partner input that cover part of cloud, data analysis, mobility solutions, and social integration, and also a demonstration of product growth and expansion to meet current and future market needs.	32.00
Delivery	It shows understanding of how security market is evolving to address mobile threat management architecture needs.	20.00
Growth	It has a large installed base of customers to grow/sell into.	18.00
Innovation	There is a strategic plan to make mobile threat management a key element of strategic security architecture, as well as innovation in R&D.	17.00
Growth	It has the ability to respond to competitive challenges and deliver new innovation.	8.00
Financial/funding	It shows sustainable revenue growth, internal/external funding sources, and profitability.	5.00
Total		100.00

Source: IDC, 2018

TABLE 2

Key Capability Measures for Success: Worldwide Mobile Threat Management Software

Capabilities Criteria	Definition	Weight (%)
Functionality or offering	Key capabilities match the market need for device/physical threats, network threats, malware, unknown threats, and vulnerabilities.	35.00
Portfolio benefits	Solution incorporates intellectual property that addresses key needs not currently available in the marketplace, and also evolving solution that has advanced product offering through strategic acquisitions.	30.00
Customer service delivery/satisfaction	Architecture supports multiple delivery mechanisms (on-premise, SaaS, etc.) and level of satisfaction with MTM provider.	23.00
Pricing model or structure of product/offering	Differentiated messaging and positioning are communicated through various direct, indirect, and social channels.	12.00
Total		100.00

Source: IDC, 2018

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

Copyright and Trademark Notice