IDC MarketScape

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

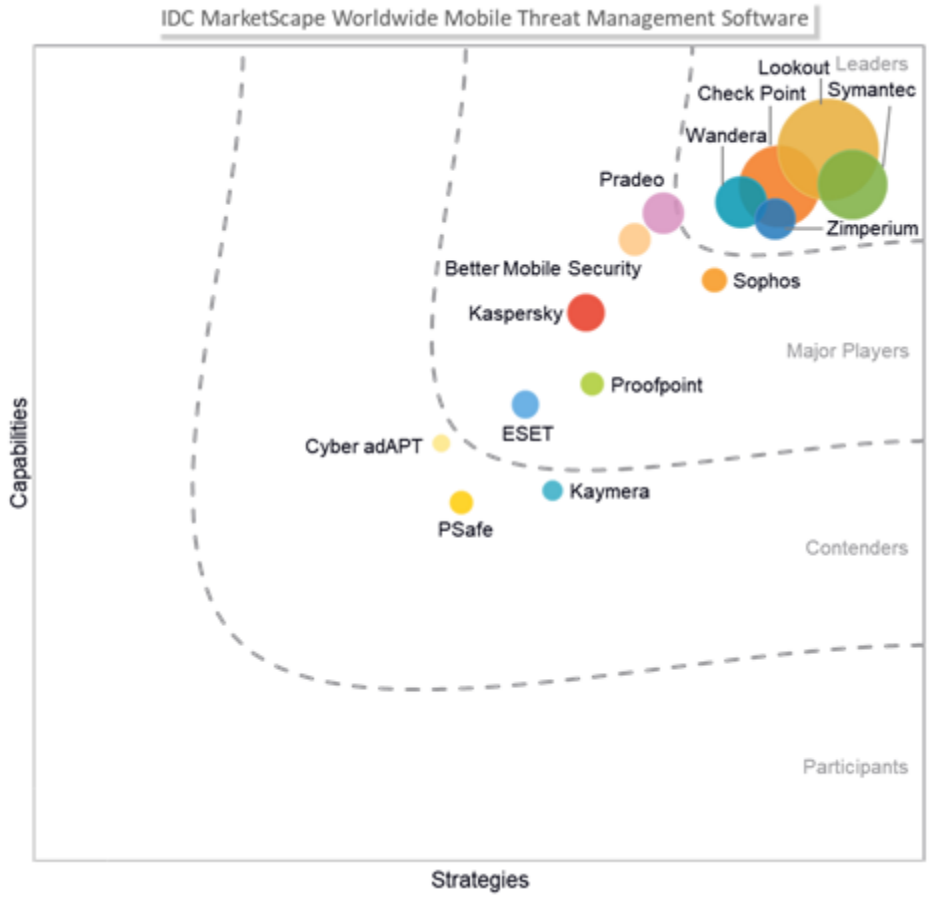
Phil Hochmuth

THIS IDC MARKETSCAPE EXCERPT FEATURES: CHECK POINT

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.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Mobile Threat Management Software 2018–2019 Vendor Assessment (Doc # US44521018e). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

As 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.

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.

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

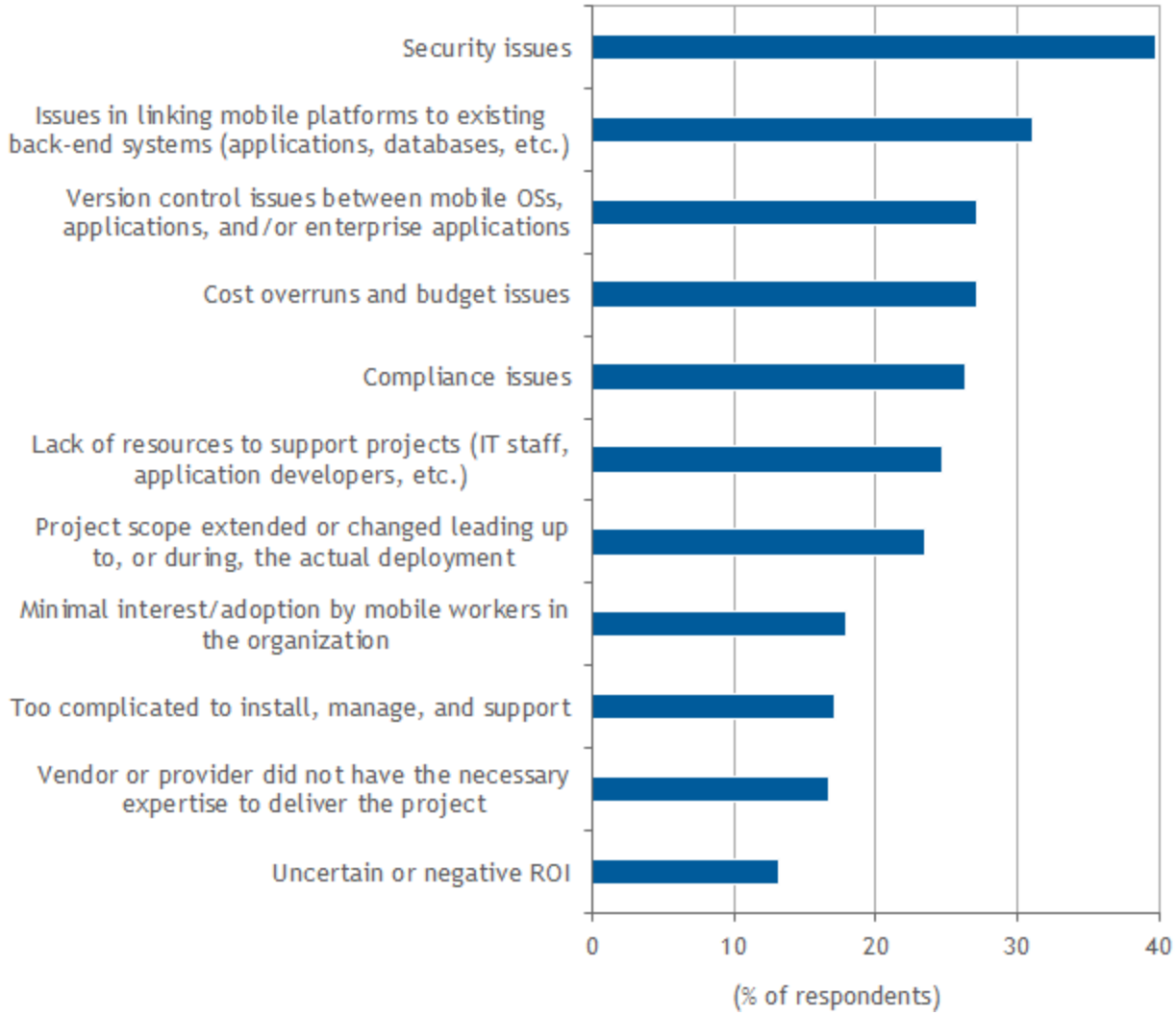
devices. The cloud-connected aspect of these products also allows the technology to communicate with EMM platforms or other security information collection or mitigation points, such as security information and event management platforms or firewall/VPN/IPS infrastructure. From a broader IDC taxonomy 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

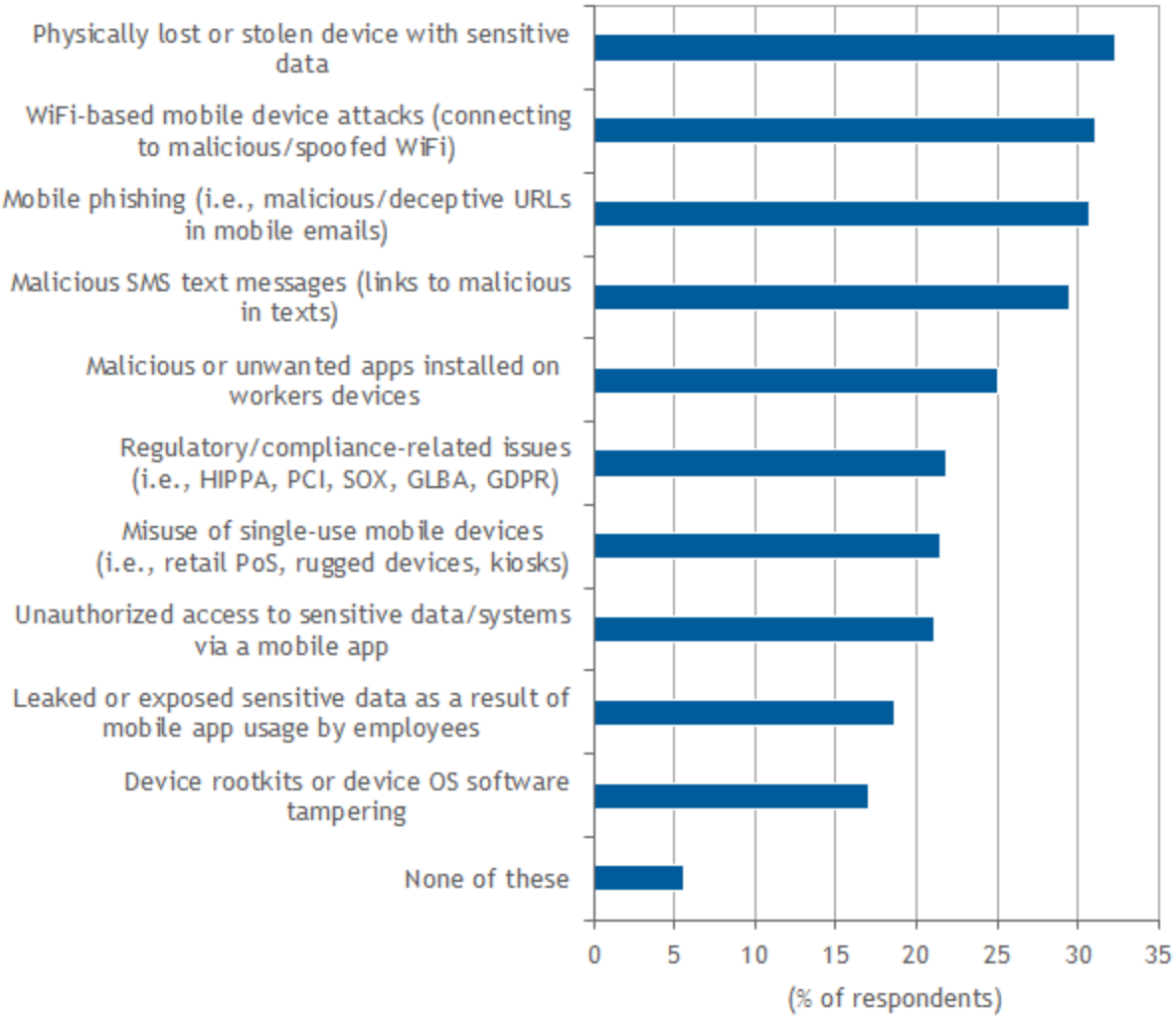


n = 250

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

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

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2018 IDC. Reproduction is forbidden unless authorized. All rights reserved.