G00290746

Critical Capabilities for High-Security Mobility Management

Published: 25 August 2016

Analyst(s): John Girard, Dionisio Zumerle, Rob Smith

High-security mobility management is a subset of the enterprise mobility management market that serves organizations with the most stringent requirements. If security is the highest priority, IT planners should pursue best-of-breed solutions for each platform they intend to support.

Key Findings

- High-security managed mobility solutions do not correspond to a single or specific mobile technology market.
- The solutions that provide the highest security also require that users accept reductions in scope and flexibility, which will affect users' experiences. This may involve expensive, specialized hardware and software, as well as reduced choices in devices and features.

Recommendations

- If security is a high priority, IT planners should look at best-of-breed solutions for each of the platforms they intend to support.
- Solutions with high-security qualifications may not meet usability expectations; buyers need to ensure that their choices will support business processes without undue disruptions or interference.
- High-security organizations should plan for tiers of access that support the use of less-secure configurations for less-sensitive tasks.

Strategic Planning Assumption

Through 2019, users that require the highest levels of security will prefer platforms that rely on dedicated security hardware that leverages trusted environments.

What You Need to Know

The decision to pursue the highest levels of security and privacy on small mobile devices that do not run workstation-class operating systems is an absolute necessity for the protection of confidential, secret, sensitive and competitive, official and unofficial information, as well as intellectual property (IP). This research provides tactical guidance to help with the selection of software and hardware vendors that offer solutions that may satisfy the requirement for robust defenses.

The vendors reviewed in this research include some providers covered in the "Magic Quadrant for Enterprise Mobility Management Suites," as well as others that would not normally qualify based on market share, revenue or platform breadth, but which qualify to manage high-security use cases. These vendors do not represent an exhaustive list.

There are various methods for creating secure environments in software, by a combination of containers, hardened apps, rights methodologies and other means. However, buyers who seek the highest levels of protection may prefer a combined hardware and software solution, and their choices are dwindling. Vendors that own and control their own secure hardware platforms tend to be specialized, expensive and sell in small quantities, compared with the larger mobility scene. Some companies make use of security features in more accessible and popular hardware platforms, mainly Apple iOS and Samsung Android devices with Enterprise Knox.

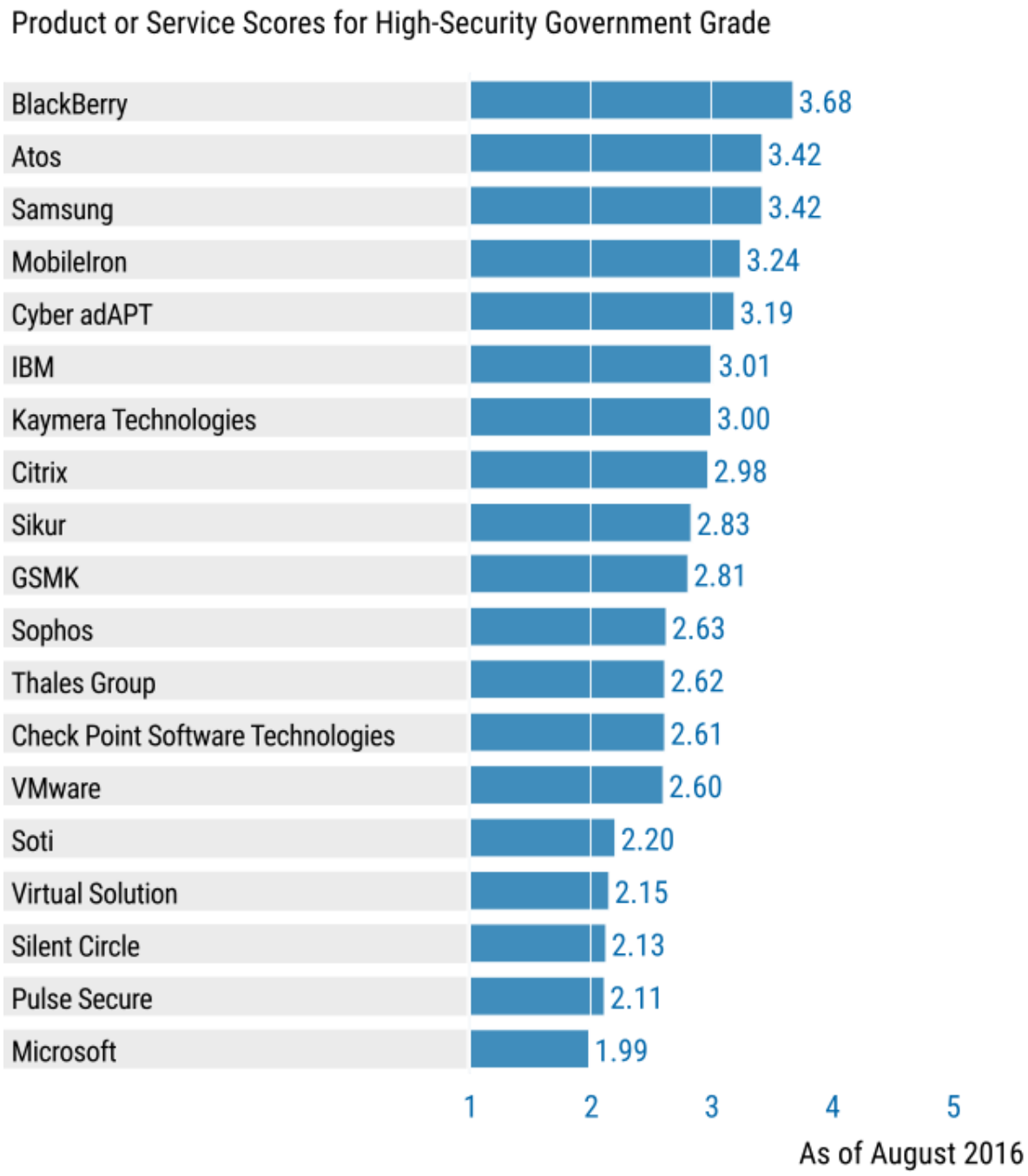
This research assesses the following six use cases that are described in a later section:

- High-Security Government Grade
- High-Security Commercial
- Shared Data
- Shared Devices
- Nonemployee
- Bring Your Own (BYO)

Analysis

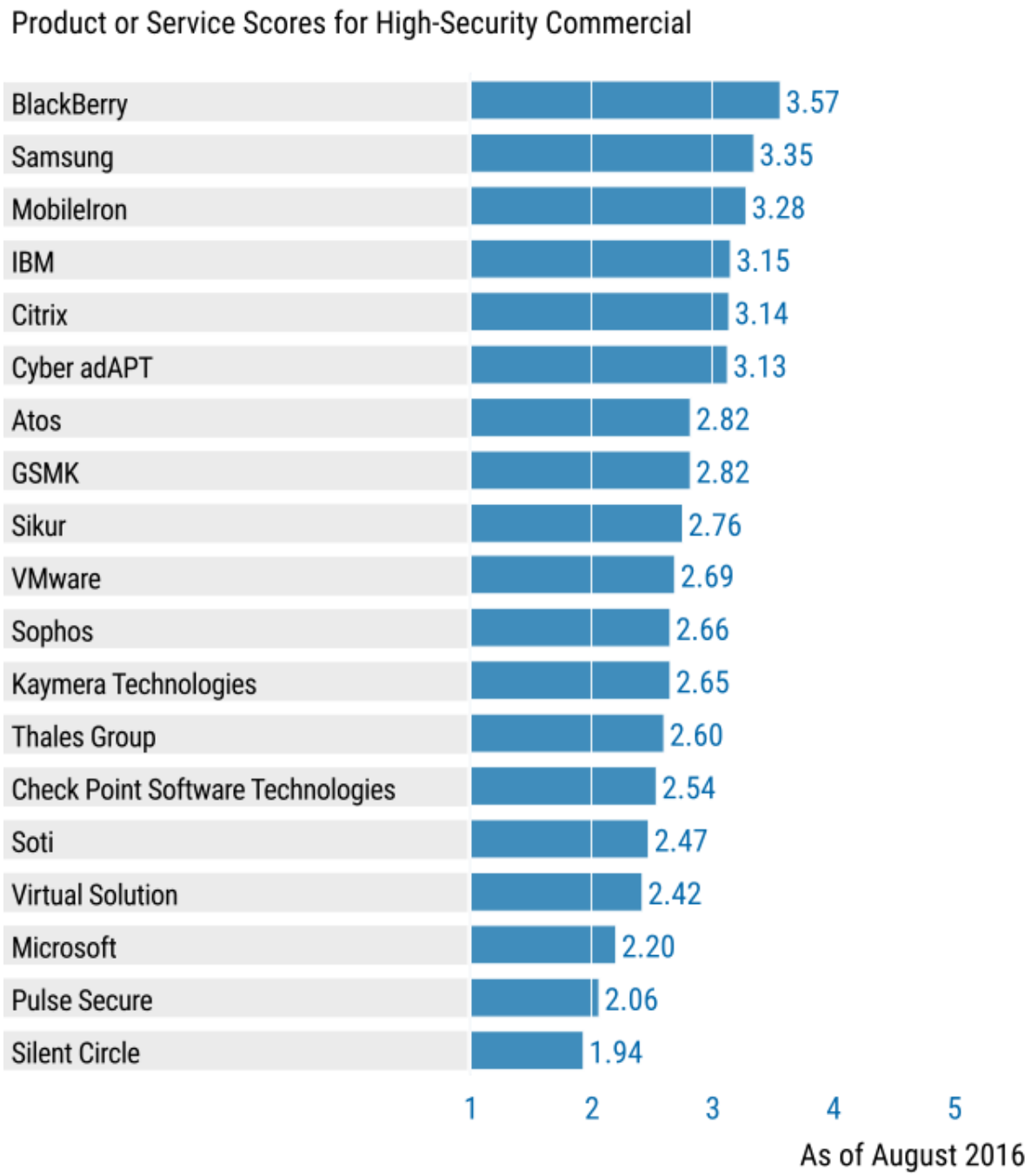
Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for High-Security Government Grade Use Case



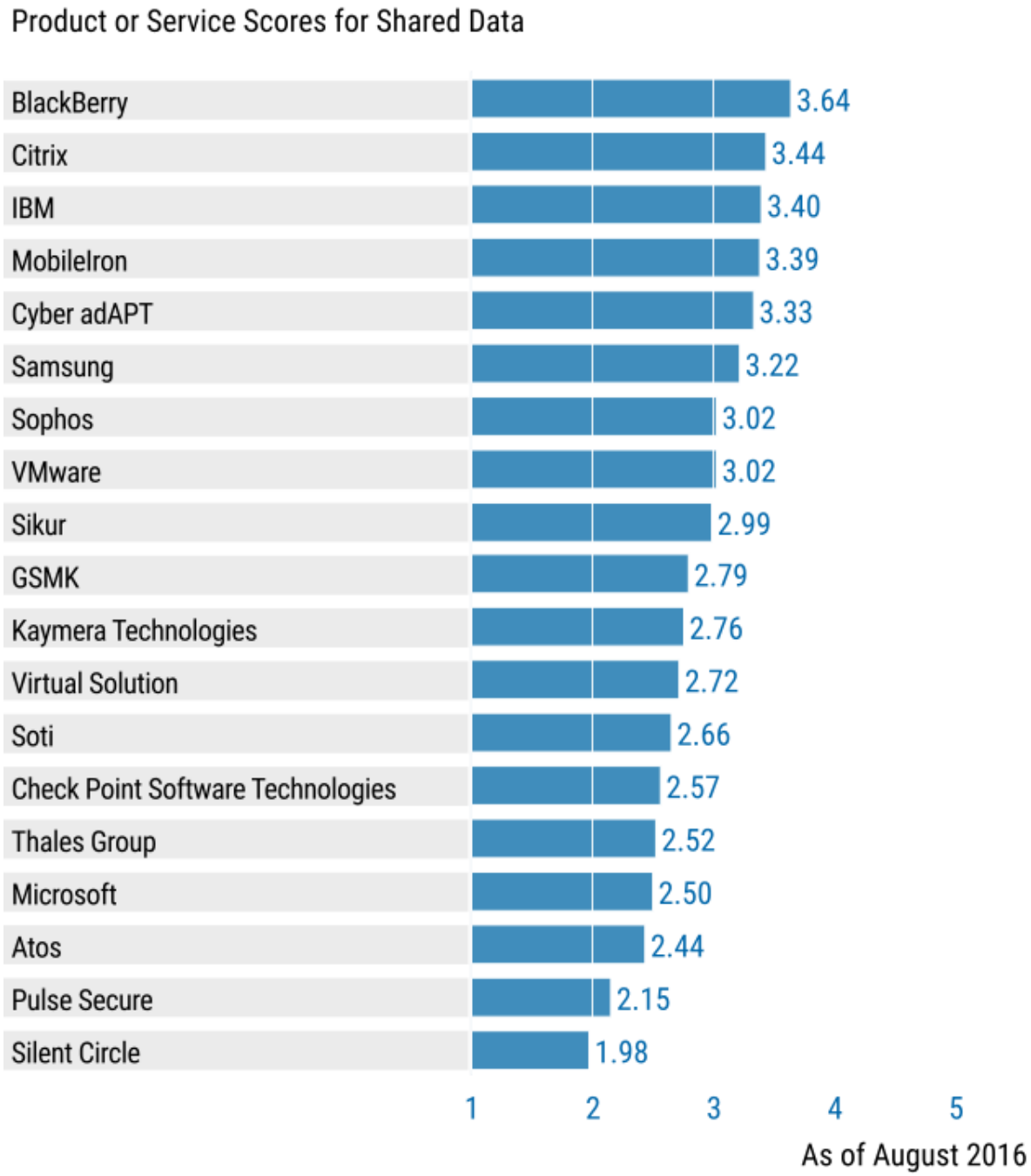
Source: Gartner (August 2016)

Figure 2. Vendors' Product Scores for High-Security Commercial Use Case



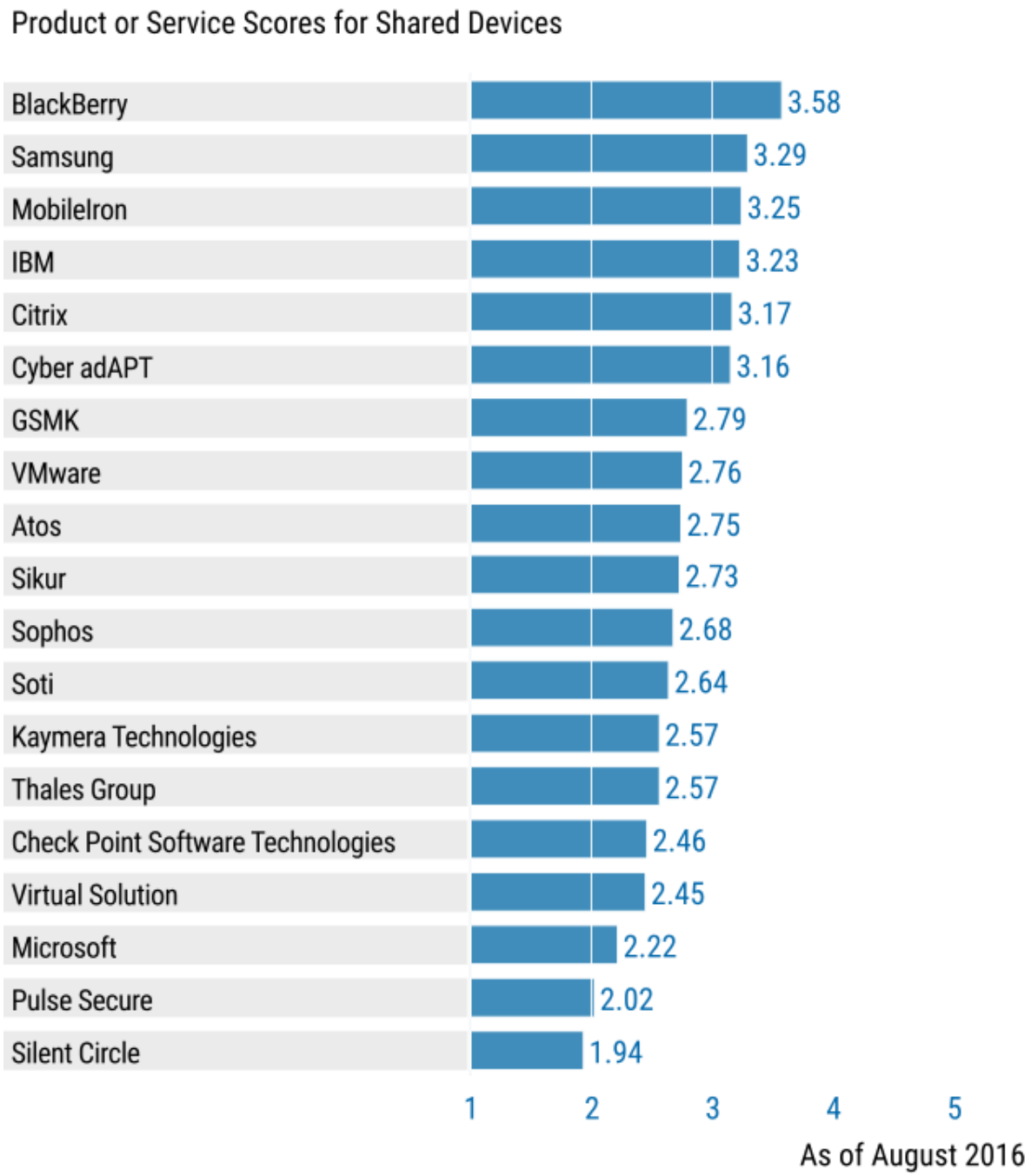
Source: Gartner (August 2016)

Figure 3. Vendors' Product Scores for Shared Data Use Case



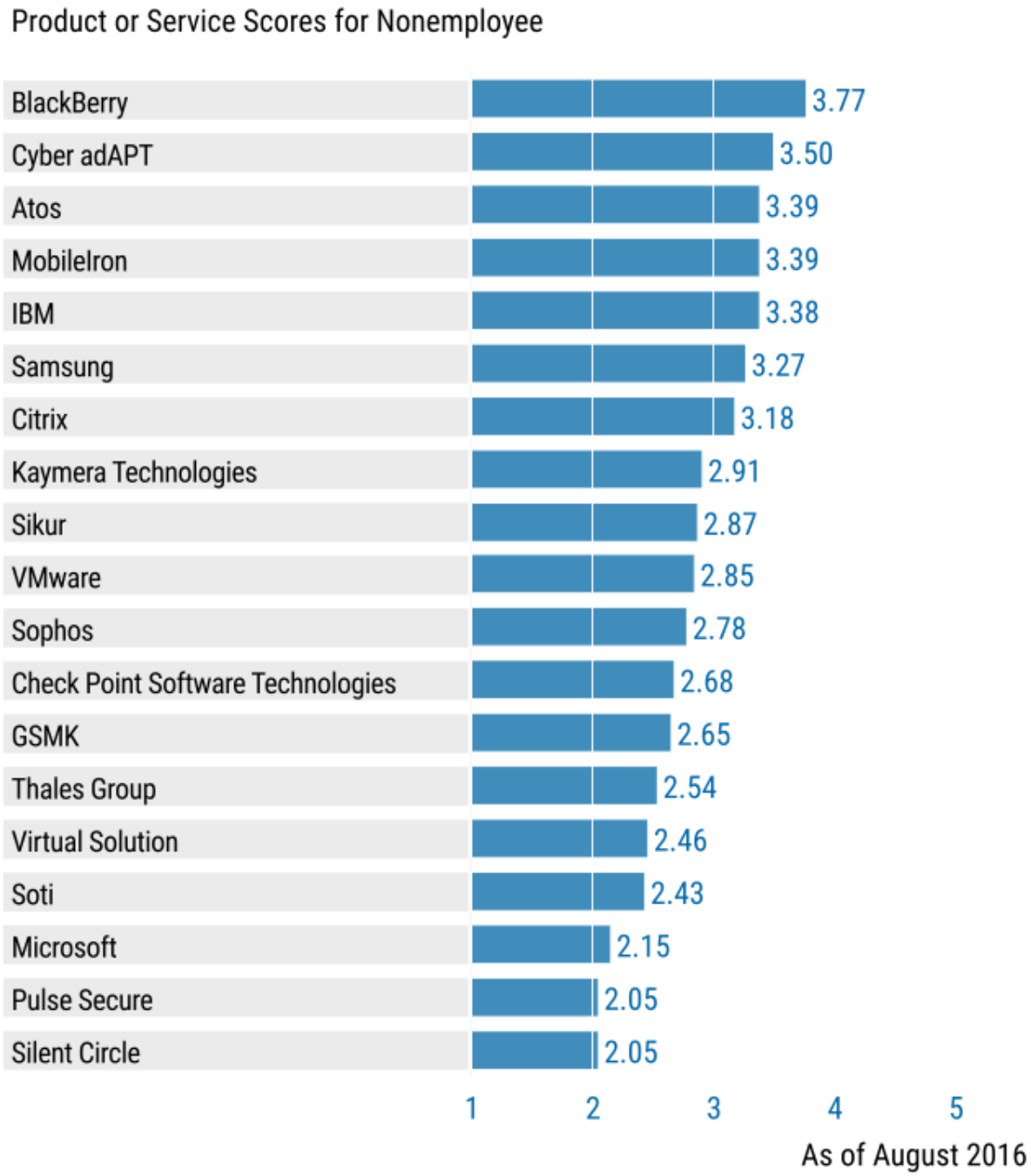
Source: Gartner (August 2016)

Figure 4. Vendors' Product Scores for Shared Devices Use Case



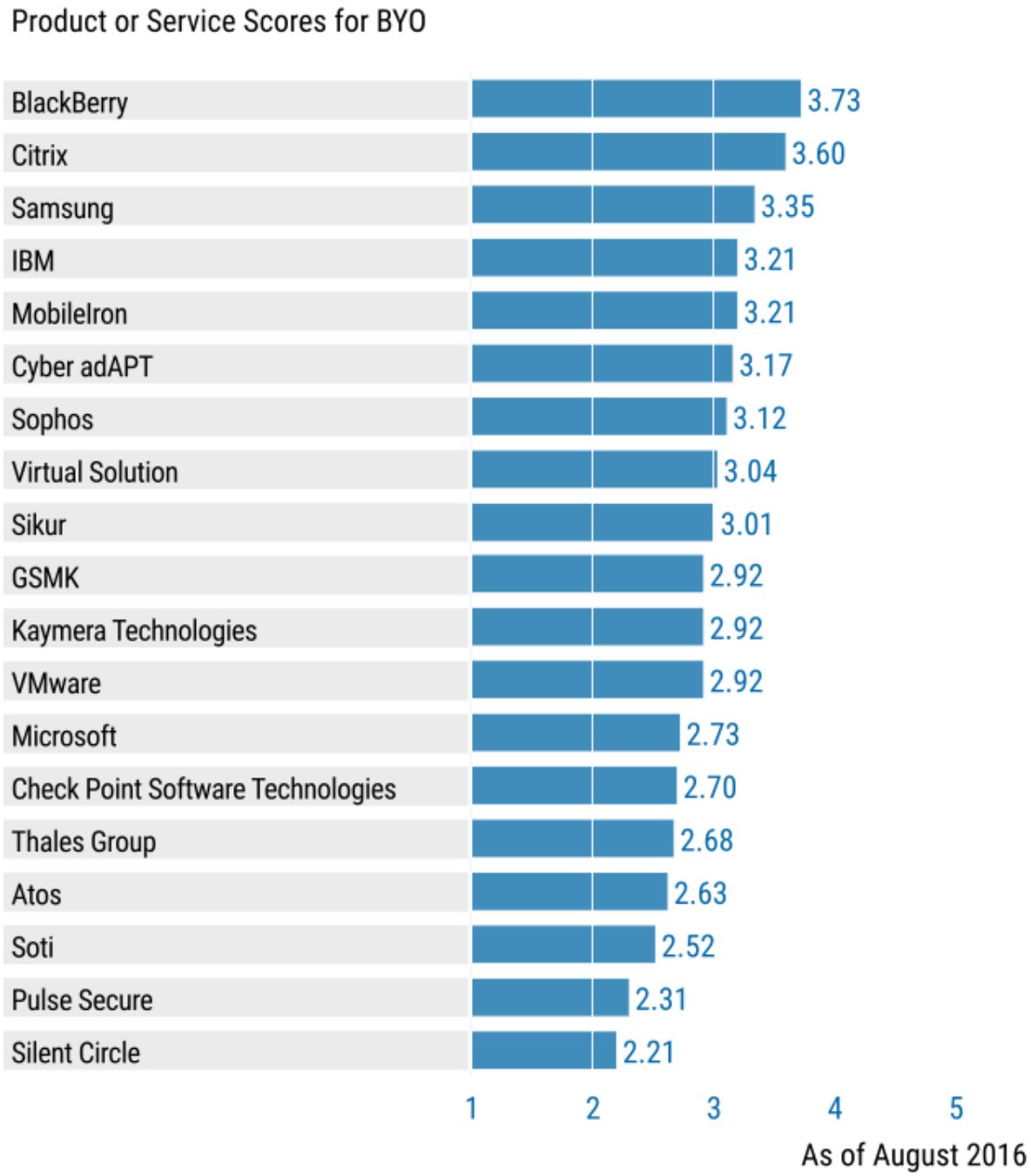
Source: Gartner (August 2016)

Figure 5. Vendors' Product Scores for Nonemployee Use Case



Source: Gartner (August 2016)

Figure 6. Vendors' Product Scores for BYO Use Case



Source: Gartner (August 2016)

Vendors

Atos

Atos provides, through its acquisition of Bull, two secured smartphones: Hoox m2 and the newer Hoox m3. The devices are a dedicated hardware/software platform targeted to high-security enterprise contexts and it is intended for business use only. Atos does not appear in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Hoox m2 and Hoox m3

Certifications and Awards

The Atos Hoox products exceed certification requirements set forth by FIPS 140-2. It is certified EAL5+ for the secure element and EAL4+ for the encryption applet. The device is approved for France Restricted, EU Restricted and NATO Restricted communications levels. The solution has also obtained the French Cybersecurity label.

Secure Life Cycle Management

Hoox comes with its own MDM tool, but is also interoperable with AirWatch and MobileIron. Interfaces such as USB can be enabled or disabled via MDM for data transfer. The life cycle management also foresees a remote wipe and kill functionality, where the device is fully wiped and rendered inoperable.

Hardened Platform

Atos provides its own fully locked down platform. Google services are disabled on Hoox devices and third-party apps cannot be installed.

App Security

Hoox offers a suite of inbuilt apps for business use, intended to minimize reliance on third parties, as well as a wrapping function for adding third-party apps. The wrapping offers confidentiality and integrity on an application level. Hoox also offers an app auditing service, licensed by Pradeo, built into the device.

Data Security

Hoox does not offer information rights management or content-based DLP functionality. File transfer leverages the same encryption mechanism as the voice encryption feature. The system is meant to be self-contained; thus, data security involving the larger challenges of sharing and sync does not apply.

Authentication and Access Protocols

Hoox provides a secure element in the form of an embedded smart card to store user credentials. Two-factor authentication is natively present and nonremovable. Authentication is based on a combination of an RSA challenge and a passcode or a fingerprint scan. Hoox uses its own certificate authority or the existing one, if there is one. Certificate revocation is handled by the MDM tool. CAC is not natively supported since it is not an EU or NATO standard.

Attack Prevention and Mitigation

Since the device aims to offer a reduced attack surface, therefore attention to detail focuses on disabling many functionalities such as Near Field Communication (NFC), Google services and AT commands. The device performs an OS authentication and integrity test at boot time, as well as for every app before use.

Hardened VPN

The solution offers a proprietary encrypted tunnel from the mobile device to the gateway, hosted on-premises. To establish the tunnel, the solution uses a proprietary Hoox protocol that offers AES-256 encryption. All IP connectivity will be send through this encrypted tunnel.

Multiuser Device and Kiosk Mode

Kiosk and multiuser modes are not offered. The device is meant to be used by a single user.

Geo/Time Tracking and Fencing

Geofencing is not currently supported.

Forensics

Hoox provides basic functionality for reporting and auditing but does not offer or partner with computer forensics.

Scalability and Portability

Atos offers an extremely hardened solution that is a good choice for very high-security use cases. Hoox is not designed as a dual persona solution and cannot tolerate personal usage of the device. Pricing is significantly higher than mainstream commercial solutions. The typical deployment will foresee a restricted pocket of population with very high-security needs.

BlackBerry

Following the acquisition of Good Technology, BlackBerry, headquartered in Waterloo, Canada, has created and released a new platform, Good Secure EMM Suites. The suites merge features of BlackBerry Enterprise Server (BES12), Good Collaboration Apps, Good Dynamics and WatchDox

Enterprise. BlackBerry's evaluation in this report reflects the capabilities of the new configuration. BlackBerry appears in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Good Secure EMM Suites

Certifications and Awards

Good Secure EMM Suites combine products with high levels of certification, but details vary both as a result of acquisitions and lack of a single government certification program across EMM. Good Dynamics is certified to Common Criteria EAL4+. All cryptography within BES12 and Good components are certified to FIPS 140-2 Level 1. BES12 supports a large range of keys and key sizes to meet government needs, and is undergoing NIAP certification. The Good Technology components use a combination of owned code and OpenSSL. Good components are FIPS recertified after any change to the crypto module. Other certifications for the Good components include U.S. FISMA purchase approval with HSPD-12, CIO Council, DoD Directive 8100.2, Australian and New Zealand Signals Directorate (ASD) EPL 4, ISO 19790, and U.K. CESG Configuration Guidance. The Good components have also been assigned a DISA STIG.

Secure Life Cycle Management

BES12 provides a variety of baseline secure EMM functions for Android, iOS, OS X, Windows 10 and BB10 OS. Guidelines are offered for default high-security EMM configurations. The Good Dynamics component is completely manageable as a container, with the same policies on multiple platforms and on unmanaged devices. The Good product design detects unauthorized attempts to move certificates and keys and provides granular controls over most platform services, such as the use of the camera within contained apps. Additionally, the Good Dynamics component can detect exploit attempts, jail breaking/rooting, and locking or wiping exploited, lost or unauthorized containers.

Hardened Platform

BlackBerry offers a hardened version of Android for their PRIV, DTEK50 and future BlackBerry Android devices, and BES supports Samsung Knox and Android for Work. On Android, all startup processes are subjected to integrity tests based on code signatures and protected key stores. Similar tests are not available for iOS. Feedback from highly regulated clients indicates that the PRIV is not considered as a substitute for the protection levels of the BB10 platform. BES12 and Good Dynamics can run within the Knox Workspace and Android for Work, and device health attestation is supported for verifying device integrity. The Good component supports the Trusted Execution Environment (TEE) for secure key storage.

App Security

BES12 securely manages apps by using Good Dynamics and native OS capabilities such as Samsung Knox and Android for Work. Good Dynamics provides a defended app container that limits sharing among apps and movement out of the device on all supported platforms to

destinations, including popular sync and share apps. The PIM and Dynamics-developed apps are self-hardened and isolate themselves from the underlying OS. In the event of a profile violation caused by the user, malware or some other reason, access keys are withdrawn. The container is not recoverable by local action, and can be selectively or fully wiped. An SDK is available to make it easy for companies to import their own apps with a Good Dynamics container. Trusted root certificates can be associated with individual apps, as well as the container, and additional app passwords can be required. Security could be compromised, for example, if a decision is made to allow public access to the container, but this must be a conscious administrative policy decision.

Data Security

The WatchDox component provides a secure Enterprise File Share & Sync solution and incorporates a rich set of Digital Rights Management tools that run on mobile platforms, as well as PCs (Windows and Mac) and web browsers to provide functional controls (e.g., no print, no copy/paste, etc.) on Microsoft Office and Adobe PDF files. In addition, files that are shared or accessed via WatchDox will maintain protection of the files at rest, in transit and when desired, in use. The WatchDox mobile apps can be managed by BES12, or operate stand-alone or integrated with the Good Dynamics framework. Several popular third-party EFSSs offer clients preconfigured for use with the Good solution and are offered through public app stores. Data movement into and out of the container can be fully monitored and controlled.

Authentication and Access Protocols

Good Dynamics containers register to back-end servers via a symmetric key. Multiple containers on the same device or between devices can communicate and authorize intercontainer transactions by means of certificates that are signed by the back-end Good control server. Individual apps and containers can be bound to additional local authentication, including CAC, multifactor authentication, TrustZone and various biometrics. Partnerships with NAC vendors defend container access to internal networks.

Attack Prevention and Mitigation

BlackBerry has no anti-malware or app reputation support integrated with the enterprise app store feature for Android or iOS. Good interoperates with several secure web gateway (SWG) and app reputation vendors so that users can perform additional tests. Third-party apps approved for the Good container are tested and signed with Veracode, and guaranteed to be certified when downloaded from commercial app stores. Good Dynamics integration with Zimperium is available from BlackBerry for advanced mobile threat detection. Trusted app side loading can be managed on Samsung Knox. If problems are detected with apps or with the device, such as jailbreaks, three wipe/lock options are available: specific container, multiple containers and whole device.

Hardened VPN

BlackBerry uses platform VPN APIs and has some supported relationships with mainstream vendors. BlackBerry Secure Connectivity is available for iOS native (configurable as a per-app VPN), as well as for Samsung Knox Workspace and Android for Work, and supports proxies for third-party

secure web gateways (SWGs) on Android and iOS. Good Dynamics can work with device-embedded VPN clients; however, the preferred communications method associates a fully contained micro-VPN with each managed app. The containerized VPN does not rely on local APIs, keys or certificates, defending against local and network-borne MITM attacks, and its operation is transparent to the user. Split or closed tunnel mode is configurable on an individual app basis, as is proxy forwarding to third-party SWGs. Good provides its own enterprise VPN gateway that embodies the authentication tests described elsewhere. Third-party VPN clients and VPN gateways can be used as an additional layer of protection when Good Dynamics is configured for Direct Connect, although this extra layer of security may be superfluous.

Multiuser Device and Kiosk Mode

A basic multiuser mode can be implemented for Android and iOS by changing BES12 EMM policies dynamically, depending on the logged-in user. However, managing shared (e.g., a device's Wi-Fi profile) versus individual users is not available for iOS. Kiosk mode is available on Android and iOS. Android kiosk support requires Samsung Knox. Samsung Knox kiosk mode will survive a device reboot. Kiosk mode operation is supported for Android and iOS using built-in OS capabilities, and has mainly been applied to guest sign-in rather than to high-security scenarios. Knox Workspace can be deployed in "Workspace Only Mode," removing the personal space for a high-security configuration.

Geo/Time Tracking and Fencing

Geolocation tracking is available via BES on Android, iOS and Windows. Good Dynamics supports location and time-based tracking and policy controls via third parties. There is a plan to directly integrate these capabilities into the platform beyond the close of this evaluation. An export control type of data blocking is not available; however, container access can be changed, depending on time and location, and containers can be locally locked/wiped if they do not check in with the BlackBerry server within a predetermined interval. The company also owns AtHoc, a mainstream emergency notification solution, but it is not presently integrated with the Good Secure EMM Suites.

Forensics

Forensic capabilities are available through a mobile-focused computer forensics provider.

Scalability and Portability

Good Secure EMM Suites are priced competitively in the EMM market and are feasible and affordable for large-scale implementations. BlackBerry can certify the Good Dynamics container against hundreds of Android platform variants and publishes an official list on which it can run safely. It also provides above-average functional parity and user experience across Android and iOS. The list of fully contained apps and services is typically comprehensive for business purposes. Containerized services will meet most enterprise needs, and many popular third-party business apps are containerized.

Check Point Software Technologies

Check Point Software Technologies, headquartered in Tel Aviv, Israel, is a leading global firewall and VPN vendor. Their mobile security solution consists of a software container called Capsule (Workspace, Docs and Cloud) for both iOS and Android, Mobile Threat Prevention, and Capsule Connect/VPN. The Capsule Workspace is a traditional PIM client and Capsule Docs offering basic MCM functionality. Check Point Mobile Threat Prevention offers real-time detection of malware while the Check Point Capsule Connect/VPN offers secure remote access for mobile devices. Check Point does not appear in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Products: Check Point Capsule, Check Point Mobile Threat Prevention, Check Point Capsule Connect, Check Point Capsule VPN, Check Point Capsule Workspace

Certifications and Awards

The products have both FIPS 140-2 Level 1 and Common Criteria EAL4+ certifications. It is also the only product covered in this research to have the Russian GOST certification.

Secure Life Cycle Management

Check Point Capsule Workspace does not offer any device management functionality but the product can be configured and managed over a central management server.

Hardened Platform

Check Point does not supply hardened device platforms or hardened OS versions. Capsule is able to run Knox-protected apps via APIs within the Capsule container, without invoking the full Knox environment, using a trusted app key assigned to the Capsule container agent. Check Point also has a partnership with Cellrox to operate on top of its Thinvisor secure mobile virtualization platform.

App Security

The Capsule Workspace component includes a secure email client, calendar, contacts, notes, messaging, SharePoint access, a file repository and a secure web browser within a single application. It also offers app-wrapping technology to incorporate in-house-developed applications into the capsule workspace. The solution also includes partial wipe capabilities to wipe only the data stored within the container.

Data Security

Check Point Capsule Workspace can protect both data in motion and data at rest through encrypted communications and an encrypted container. However, the container does not run in a separate memory space, exposing it to potential attacks. The container also includes copy/paste protection to prevent document leakage into unauthorized applications.

Authentication and Access Protocols

Check Point Mobile Threat Prevention offers two-factor authentication for access to its container. However, it does not support high-security solutions such as common access cards (CACs). There is no third-party IAM support nor is an IDaaS provided.

Attack Prevention and Mitigation

Mobile Threat Prevention offers software-based, real-time malware detection for both iOS and Android. Although it cannot directly remediate if an event occurs, it can interface with leading EMM vendors to issue a wipe of corporate data. At the time of this writing, there was no direct remediation capabilities between the Mobile Threat Prevention detection module and Check Point gateways, although a plan for this capability has been planned since last year.

Hardened VPN

Capsule Connect and Capsule VPN offer both IPsec and TLS VPN connections to Check Point gateways. The VPN is IP or domain activated but does not offer per-app VPN. It is also important to note that the user can disable this VPN at any time, which is a serious caution for high-security environments.

Multiuser Device and Kiosk Mode

The solution does not support multiple users or kiosk mode.

Geo/Time Tracking and Fencing

The solution does not offer geofencing or time-based rules. It does offer the ability to auto-wipe a device if it does not check-in during a set interval.

Forensics

The solution offers basic OS tampering detection but does not offer any additional forensics, nor does it offer export of log data to other systems.

Scalability and Portability

Although the Check Point mobile solutions have had limited market exposure, Check Point firewalls and VPN solutions are deployed globally on a very large scale, which could improve buyer accessibility to direct and channel support. Buyers need to consider the complexity added by integrating several product lines to build a managed mobile platform.

Citrix

Citrix XenMobile Enterprise is a comprehensive mobile management solution that also integrates with the company's server-based computing, virtual desktop and VPN products. Android, iOS, Mac

OSX and Windows 10 platforms are targeted for full management. Limited capability exists for Windows Mobile legacy platforms. Citrix appears in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: XenMobile Enterprise

Certifications and Awards

XenMobile provides FIPS 140-2 Level 1 cryptography in software for Android and iOS, based on OpenSSL FIPS Object Module. Apple's built-in, FIPS-certified cryptography is also used on iOS platforms. Citrix is an active sponsor of the OpenSSL project and recertifies their cryptographic capabilities on a regular basis. The iOS version has received purchase approval designation from the Australian government security agency, ASD. NetScaler supports a NIST-certified hardware module.

Secure Life Cycle Management

Citrix provides actionable settings advice for high-security policies involving all standard device settings on Android, iOS, Windows Mobile Legacy, Windows 10 and OS X. A trusted bridge is provided so that Citrix's Public Key Infrastructure (PKI) can integrate with a customer's choice of key infrastructure and certificate authorities. Device enrollment can be strongly validated using multiple factors including Active Directory (AD), one-time password (OTP) and one-time URLs that prevent cloning images to unknown devices

Hardened Platform

Citrix does not supply hardened device platforms nor hardened OS versions. However, it allows for the leveraging of policies and capabilities in Samsung Knox and Android for Work.

App Security

In addition to an included set of apps such as secure email, browser and others, the XenMobile MDX wrapper works across all supported platforms, including legacy Windows Mobile, providing execution control of business apps that is tied to the embedded PKI and Citrix Secret Vault certificate repository. The wrapper is fully owned by Citrix. Wrapped apps are digitally signed and tracked by XenMobile, and the Citrix PKI is applied to all I/O events.

Data Security

XenMobile encrypts any data created on the mobile device, forming a default defense against data leakage. Citrix ShareFile, interoperable with XenMobile, further extends protection for data sharing. ShareFile is popular with users and supported by third-party DLP and CASB vendors, making it easier to direct business processes away from vulnerable sync and share platforms.

Authentication and Access Protocols

XenMobile's PKI, certificate vault and various authentication tests constitute a robust suite of authentication capabilities. Device certificate-based authentication and certificate pinning are supported. Wrapped apps can be configured to require additional password and PIN challenges. XenMobile is also compatible with several third-party IAM and NAC vendors. CAC is supported via partnerships with Intercede and Entrust.

Attack Prevention and Mitigation

Citrix does not license or offer anti-malware and app reputation products, relying instead on strong signature and certificate controls. Commercial apps that have been wrapped for MDX are trusted and signed in the Citrix Worx Home Store.

Hardened VPN

Citrix NetScaler, an application delivery controller that has been optimized for Xen Desktop and XenMobile users, provides VPN and secure web gateway functionality and other capabilities. Client connection modes for all supported platforms include continuous, domain activated and per-app. FIPS-certified cryptography is standard for XenMobile but optional in the gateway, therefore buyers must be sure to specify their requirements.

XenMobile establishes platform authentication prior to first use of VPN, meaning that certificate data is both pinned and never exposed, thus reducing the possibility of network layer MITM attacks against remote access logins.

Multiuser Device and Kiosk Mode

XenMobile offers a comprehensive set of features for configuring and managing multiuser mobile platforms and user accounts, but only for Android and iOS platforms. In addition to login controls based on AD credentials, XenMobile has many options for group and organizational settings, pushing use-specific configurations, and selective data deletion after logout. As a leading provider of server-based computing by means of XenApp, Citrix can solve the multiuser problem in other ways, by use of remote viewing techniques.

Geo/Time Tracking and Fencing

Device behavior, time limit since last check-in, application access, network services and other functions can be controlled according to time of day and location for Android and iOS only. On all supported platforms, Citrix can apply location decisions to restrict access to data both in terms of direct access and programmatic access through WorxMail. XenMobile can request data inventory reports. It can also initiate autonomous selective wipe based on time since last check-in.

Forensics

Forensic capabilities are provided through a partnership with Gotham Digital Science.

Scalability/Portability

XenMobile is competitively priced, offers many security benefits, and has better than average user references for authentication, VPN and file sharing. Full benefits are mainly offered on Android and iOS platforms, which of course represent the majority of demand.

Cyber adAPT

Cyber adAPT's EMM platform supports Android and iOS with solutions suitable to all types of enterprises, with a particular appeal to higher security environments. Cyber adAPT provides an IPsec VPN for iOS, Android, Windows and OS X. Cyber adAPT's Secure Device Management (SDM) Server gateway applies security policies and provides identity management and authentication, while Cyber adAPT's SDM client provides on-device tamper-resilient connectivity to the SDM Server for behavior-based threat detection. Cyber adAPT does not appear in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Cyber adAPT SDM

Certifications and Awards

Cyber adAPT's SDM Server uses OpenSSL FIPS Object Module, which is validated to FIPS 140-2 Level 1.

Secure Life Cycle Management

SDM supports granular EMM policies for both iOS and Android, including complex passcodes, partial and full device wipe, as well as blocking external media and cloud storage. In addition, SDM can interoperate with other EMM suites.

Hardened Platform

Cyber adAPT SDM Server is built on a hardened Debian Linux platform with an integrated stateful firewall. On the device, the SDM agent enforces low-risk profiles and provides tamper-resistant controls to reduce attack surfaces. Profiles can only be removed or modified during a live connection and require passcodes for any changes. For Samsung Knox devices, SDM can prevent removal of the VPN.

App Security

Cyber adAPT provides a good range of app-wrapping capabilities and policy enforcement on an application level, as well as a secure PIM client, provided by Virtual Solution's SecurePIM. SDM provides application whitelisting as well as secure web gateway functionality.

Data Security

Cyber adAPT does not provide content-based DLP capabilities or IRM for enterprise data, but Cyber adAPT's VPN can be rerouted to a DLP solution to provide those capabilities. Also, Cyber

adAPT can integrate with a number of enterprise file sync and share solutions, including Salesforce, Box and Dropbox. The built-in firewall can allow/deny access to network storage resources.

Authentication and Access Protocols

The Cyber adAPT SDM Server gateway uses a built-in PKI for identity management and authentication, providing its own certification authority, as well as offering integration with certain third-party certification authorities. Cyber adAPT partners with WidePoint to offer two-factor authentication.

Attack Prevention and Mitigation

Cyber adAPT's solution includes an embedded firewall and a licensed anti-malware solution. Because SDM enforces a VPN, all traffic is analyzed in real time for data and process behavior aspects that are indicative of attacks. This is also helpful for preventing MITM attacks, for example, at public hot spots.

Hardened VPN

The fundamental design of SDM focuses on providing a tamper-proof IPsec VPN for iOS and Android. The SDM Server gateway applies granular security policies such as content filtering and traffic inspection.

Multiuser Device and Kiosk Mode

Cyber adAPT's offering provides good multiuser functionality, as well as the kiosk mode provided natively by the OS.

Geo/Time Tracking and Fencing

Cyber adAPT provides granular geofencing functionality, including filtering based on the specific country or location. In addition, Cyber adAPT provides best practices and guidance for traveling in high-concern locations.

Forensics

Cyber adAPT has its own forensic module. Cyber adAPT Plus delivers intelligent, postcompromise forensics by integrating research support with Cyber adAPT's best-in-class, real-time detection solution. SDM Server is tightly integrated with Cyber adAPT Plus.

Scalability and Portability

SDM can be delivered on-premises or as a cloud solution and can integrate with an existing EMM suite or provide its own device management. SDM will appeal in high-security environments

requiring strict device and traffic controls. The lightweight design makes for a quick setup and is suited to situations where a typical EMM footprint and agent cannot be installed.

GSMK

GSMK, headquartered in Berlin, Germany, offers CryptoPhone, a solution that combines custom hardware and software. The software is based on GSMK's hardened versions of Android and Windows Mobile. The solution offers a secure container for execution of high-security software. CryptoPhone is not intended for BYO use cases, although it scored well on capabilities considered in this research. GSMK produces a software-based security system; however, it is only sold by other vendors under license and is not associated with the GSMK brand.

Product: CryptoPhone

Certifications and Awards

CryptoPhone's kernel module is certified for FIPS 140-2 Level 1 and runs with a default asymmetric 4096-bit key, from which 256-bit keys for the stream ciphers AES and Twofish that run in parallel in counter mode are derived. The product is not Common Criteria certified. The solution is FIPS 197-certified for AES encryption algorithm. Several other awards and approvals tend to be regional or specialized. For example, GSMK is a preferred provider for several aircraft companies, military, police and public service agencies, the International Criminal Court, International Atomic Energy Agency and the United Nations. GSMK openly makes the source code of the solution available to all clients for independent review.

Secure Life Cycle Management

CryptoPhone provides dedicated hardware that is managed using a proprietary console. This console can control every aspect of the device, including device configuration and data wiping.

Hardened Platform

GSMK offers customized, hardened versions of Android and Windows Mobile devices bolstered by their own custom firmware. The firmware features GSMK's proprietary hardware controller and permission enforcement modules to control access to networks, sensors and peripherals. GSMK's Baseband Firewall is designed to prevent unauthorized access to the device and is particularly robust at preventing over-the-air attacks by malicious base stations and hostile network operators.

App Security

The CryptoPhone's central secure communications application covers voice encryption, message encryption and data encryption. The CryptoPhone also includes GSMK's Baseband Firewall, which is designed to prevent unauthorized access to the device via the air interface. The solution also recently added a distributed system to detect IMSI-catchers and other rogue base stations as part of the solution to mitigate MITM attacks.

Data Security

GSMK offers two-layer storage encryption consisting of full-device encryption, plus a dedicated secure storage container for particularly sensitive data. The secure container can be set to selectively lock on to different events or thresholds than the full device, such as the detection of tampering.

Authentication and Access Protocols

GSMK does not offer any additional authentication, but it can redirect all traffic over a gateway that performs additional authentication.

Attack Prevention and Mitigation

GSMK's hardened OS constantly monitors application and baseband processes for suspicious behavior. It works in combination with the GSMK permission enforcement module that restricts access to network, data and sensors. GSMK has presented detailed methods for detection and protection at the baseband layer against fake cell towers, IMSI catchers and SS7 trackers, using the Baseband Firewall.

Hardened VPN

CryptoPhone includes an IPsec client as part of the solution. This client can be configured to be activated on a per-IP domain request basis, but not per application. The solution does not include a VPN gateway.

Multiuser Device and Kiosk Mode

The solution does not offer multiuser support; however, it supports a limited kiosk mode that allows any of the base system applications to execute and no others. This solution lacks support for dedicated third-party applications.

Geo/Time Tracking and Fencing

The solution offers basic geofencing and time tracking. Because of the solution's design, data cannot be collected on a per-application basis, but only by a devicewide poll.

Forensics

CryptoPhone does not directly offer any export of log data to third-party tools; however, the solution is capable of being audited with physical device access in a manner that would support a forensic investigation.

Scalability and Portability

Because the CryptoPhone solution provides dedicated hardware, the cost of the product is higher than other software-only solutions with off-the-shelf hardware. However, because the hardware is provided, installation and support are easier to deploy and manage, compared with software-only solutions.

IBM

IBM offers MaaS360, a software EMM platform that can be managed on-premises or in the cloud. The product and development team were obtained through the acquisition of Fiberlink's MaaS360. IBM appears in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites." Building out some of the capabilities requires investing in several additional IBM product lines, such as the IAM framework, IBM Security AppScan, Cloud Security Enforcer and QRadar Security Intelligence Platform.

Product: MaaS360

Certifications and Awards

MaaS360 provides FIPS 140-2 Level 1 cryptography in software for Android, based on open-source OpenSSL. Apple's FIPS 140-2-embedded cryptography is used on iOS platforms. Management of Samsung Knox is supported. The product has been assigned a STIG, and also has U.S. FISMA Authority to Operate (ATO) approval for the cloud-based management platform. FIPS-level operation is active by default. Other awards include SOC-2 Type-II, FedRAMP, Cloud Security Alliance (CSA) STAR Registry and ISO 270001. Common Criteria certification is in process.

Secure Life Cycle Management

IBM provides sufficiently broad coverage of access control, encryption, data import/export, cloud controls and other key policies to provide effective cross-platform management. Some security policies can be applied to devices that do not have EMM profiles by associating users and apps with device identities. For supporting devices, IBM MaaS360 provides an API-driven ability to download and install OS updates. For nonsupporting devices, IBM MaaS360 can still take numerous compliance actions on a device that is not processing scheduled updates.

Hardened Platform

MaaS360 does not supply hardened device platforms or hardened OS versions; however, it will interface with policies and capabilities in Samsung Knox and Android for Work.

App Security

Managed apps operate in a policy framework that limits sharing among apps and movement out of the device on all supported platforms to destinations, including popular sync and share apps. Apps are subject to configurable, periodic static and dynamic verification tests and nonconforming programs can be remediated through enterprise app stores. In the event of a profile violation caused

by the user, malware or any other reason, access keys are withdrawn and apps can no longer access data. IBM AppScan and IBM Arxan can be separately purchased and integrated to provide scanning and vulnerability analysis capabilities for mobile application hardening and runtime protection. Third-party app reputation tools are supported through partnerships.

Data Security

A fully encrypted EFSS is included with access policies that are controlled by the included secure app framework. Support for AD RMS is provided for all supported OSs and platforms. Local device user data can be placed in encrypted containers for which app access is restricted by policy.

Authentication and Access Protocols

CAC, multifactor authentication and full IAM product lines including a cloud identity service are available from IBM as separate products and configurations that will integrate with MaaS360. Also available is a trusted roaming access broker that can find secure points of presence and detect simple, network-layer MITM attacks against remote access logins at public broadband service points. MaaS360 supports SAML for enrollment.

Attack Prevention and Mitigation

MaaS360 includes third-party-licensed app reputation services as standard to predict potential malware and other unwanted programs. IBM Trusteer, a business-grade web security tool, is fully integrated with MaaS360. Any indication of app problems, device profile corruption, rooting, jailbreaking or other activity will block access to encrypted data, interrupt network access, and invoke partial data wipe and device wipe. IBM has provided good evidence of rapid response to recent mobile security vulnerabilities.

Hardened VPN

MaaS360 uses platform-embedded VPN software and has some supported relationships with mainstream vendors. Manual and per-app VPN invocation is supported. MaaS360 provides proxy support, its own SWG and roaming access broker with certificate pinning to avoid MITM attacks, and maintains an aggressive VPN patching process.

Multiuser Device and Kiosk Mode

These capabilities are supported on Android and iOS. In the multiuser mode, the user profile, default user interface, permissions and behaviors (including device built-in buttons and features) will dynamically change, depending on the logged-in user, AD credentials, etc. Device-specific and container-specific policies can be altered as needed. MaaS360 supports public-facing kiosk apps on iOS. Android kiosks must be hardened with OEM extensions that are not available for all models.

Geo/Time Tracking and Fencing

Device behavior, time limit since last check-in, application access, network services and user interface/persona can be altered according to time of day and network. The interactive user/device mapping system is good enough to use for basic emergency monitoring and staff location management. A mobility consulting team provides special assistance for companies that want to set up complex tracking and fencing scenarios. A device can still be tracked after a selective wipe, if the agent was not removed.

Forensics

MaaS360's abilities to detect tampering and other actions provide real-time event notifications and data capture that can be input to IBM QRadar. This combination has been used to build mobile forensic cases for legal action.

Scalability and Portability

MaaS360 is straightforward to install and does not pose limitations for high-security use cases. This makes it feasible and affordable for large-scale implementations across Android and iOS populations. However, buyers will need to consider additional complexity because some mobile security features will require investment in additional IBM product lines.

Kaymera Technologies

Kaymera Technologies, based in Herzliya, Israel, delivers a customized and hardened version of Android that can be installed on leading high-end devices. Kaymera's framework is designed to separate out applications and data that require additional security, and have them execute in their own memory space. Kaymera 360° can be hosted or operated on-premises. The solution also delivers security for voice and data, offering applications for encrypted voice, text messaging and data.

Product: Kaymera 360° Mobile Cyber Defense System

Certifications and Awards

Kaymera uses some FIPS-certified components, and has been in the process of certifying its platform for FIPS 140-2 since last year. Kaymera uses the Snapdragon TrustZone, which is certified to FIPS 140-2 Level 1, as part of its solution. Kaymera's cryptographic components have been certified by the Israeli Ministry of Defense, as well as other governments.

Secure Life Cycle Management

Kaymera uses a proprietary management framework to control every aspect of the device, including device configuration, data wiping and application resource controls. Kaymera 360° can interoperate with and transfer management to AirWatch and MobileIron. Over-the-air updates are supported. Kaymera keeps current with Android OS updates to assure a good user experience. Kaymera adds

a real-time intrusion detection framework to evaluate and eliminate threats to the hardware, OS and apps.

Hardened Platform

Kaymera provides a hardened version of Android OS and must flash the firmware of an off-the-shelf device for installation. At this time, Kaymera 360° does not support Samsung devices. A future option will provide secure stand-alone applications for iOS. On platforms that include TrustZone, Kaymera can use the key store capabilities to protect its private key. The OS has event traps for suspicious behavior, which can be monitored.

App Security

Kaymera offers a proprietary voice dialer, VoIP and SMS applications for encrypted communications. The solution also includes behavioral analysis for web browsing, which works with the standard browser. Any application that requires additional security operates within the Kaymera framework, running in a separate memory space from other applications on the device. This framework is not using a container technology, but rather a resource control framework, allowing the server administrator to define unique policies for each application.

Data Security

All data stored on the device is encrypted. All processes that execute in the framework run in a separate memory space to ensure separation. The system features a panic mode, which is invoked by using a special PIN. In this mode, the device will show fake contacts and messages, and will notify the management server that there is an alarm condition. It will collect information about location and activity and report back to the server. Data will also be wiped if a device does not check back to the server within a predetermined time limit.

Authentication and Access Protocols

Kaymera can use a certification authority to issue device certificates during the provisioning process. VPN authentication uses TLS certificates. Kaymera does not support CAC, multifactor, or other typical high-security authentication types, nor does it name partners for these areas or for IAM, NAC, etc.

Attack Prevention and Mitigation

The solution includes real-time device detection of attacks starting at the boot level, as part of life cycle management. If an attack is detected, for example, files have been modified, Kaymera will alert the user that an attack is taking place. In the event of a compromise that cannot be prevented or reversed, then the boot loader is destroyed, so the device is no longer capable of starting, and all of the data stored on the device is wiped. Using its continuous VPN connection and dual TLS certificates, Kaymera can detect MITM attacks, such as Address Resolution Protocol (ARP)

spoofing, Secure Sockets Layer (SSL) splitting and rogue access points. Attempts to root the device will result in full wipe of the proprietary image.

Hardened VPN

Kaymera's remote connection solution includes a persistent TLS VPN tunnel that will link the device to its management server at a company premise when there is a stable internet connection. The VPN cannot be turned off and includes an automatic mechanism for adapting networking protocols and ports to avoid VPN network blockage. During operation, the VPN can also use IPsec. Direct internet access is impossible because of a mandatory proxy and forced closed tunnel. The VPN gateway is integrated into the management server and integrates a Snort-based IDS.

Multiuser Device and Kiosk Mode

Kaymera offers multiuser and kiosk mode support.

Geo/Time Tracking and Fencing

The solution offers full server-side configurable support for geofencing and time tracking. This includes access to applications, and data can be specified according to what can and cannot be accessed, based on configuration. In addition, the system offers a personal "panic" PIN code; when activated, this will display false data.

Forensics

The Kaymera management system records all attacks detected by the various on-device detection probes and records full audit trail on each attack identified for later analysis.

Scalability and Portability

Because the current solution requires loading custom firmware on all devices, this solution is designed for small deployments. However, the price per device is relatively low compared to other dedicated high-security solutions and it could scale affordably for mainstream companies who desire a strictly controlled platform. Device flashing can be set up for "DIY" self-service.

Microsoft

Microsoft's core EMM capabilities are provided by Intune, a cloud platform included in the Enterprise Mobility Suite (EMS). Intune can manage Android, iOS, OS X and its own Windows platforms. Out of scope for this research are tablets running Windows 10, because these are, in fact, workstation-class devices. Microsoft appears in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites." The ranking in this report places reduced emphasis on the Windows Phone, which, for the present, has a limited presence in enterprise markets. Microsoft will continue to develop Windows 10 mobile and will rely on hardware partners.

Product: Microsoft Intune

Certifications and Awards

Intune is not certified for FIPS, Common Criteria, etc.

Secure Life Cycle Management

As part of EMS, Intune is integrated with Azure Active Directory Premium, Advanced Threat Analytics, ConfigMgr, Azure Information Protection and Office 365. Hardware controls, such as blocking the camera, NFC and removable storage, will vary by platform. Intune does not support Android for Work. It is one of only two vendors ranked in the "Magic Quadrant for Endpoint Protection Platforms" that also qualified for inclusion in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites" (the other is Sophos).

Hardened Platform

Microsoft does not provide hardened mobile hardware or OS at this time. Intune can manage some Samsung Knox policies but does not offer support for other device maker custom APIs. It does not support Android for Work.

App Security

The Intune app-wrapping tool is available for Android and iOS, but not for Windows Phone. The Intune App SDK and Xamarin are available for iOS and Android. App sign-on, certificates and other basic MAM features are available natively for iOS and by SDK for Android, and are in development for the app-wrapping tool. Intune can manage security for Office mobile apps, particularly Office 365.

Data Security

Microsoft owns a well-known Rights Management System (RMS), managed on mobile devices through Azure Information Protection. Its functionality and availability are tied primarily to Microsoft apps. For example, Office 365 with RMS capability and OneDrive support is available for Android, iOS and Windows platforms, and is authenticated by Azure AD. Via Intune, Microsoft has exclusive control over the "save as" operation and can impose selected encryption rules.

Authentication and Access Protocols

Microsoft owns a competitive certificate authority, which combines with Azure Active Directory (AD) and Intune to create a strong authentication enrollment and access control environment for Windows that can synchronize with a company's on-premises AD credentials. Azure AD credentials can be used to log into Outlook and Office Mobile apps. Toward the end of the evaluation period, additional access capabilities were added, including per-app multifactor authentication tested against device identity, IP address ranges and group memberships.

Attack Prevention and Mitigation

Intune does not provide on-device malware defense features or app reputation for mobile device platforms, instead it relies on a partnership with Lookout. Advanced Threat Analytics is strongly oriented toward full Windows platforms and is primarily an alerting function rather than a mitigation solution.

Hardened VPN

Microsoft does not provide gateway support for its own VPN in connection to mobile device platforms, but can coexist with mainstream VPN providers to provide per-app VPN tunneling on iOS and Windows Phone 8.1.

Multiuser Device and Kiosk Mode

Secure sign-in for multiple users is not available for mobile platforms, nor is personalization based on user identity in a multiuser scenario. Multiple secure email accounts are supported for iOS, but not other platforms. Kiosk mode is supported on Windows Phone 8.1 through assigned access policies that can be set up through Intune.

Geo/Time Tracking and Fencing

These capabilities were in development for Intune, but are not available. Selective push of resources is possible by adding Web Application Proxy in Windows Server, a product line that is not integrated with Intune.

Forensics

Forensic capabilities are not provided, nor are they available through partners.

Scalability and Portability

Intune is feasible and affordable for large-scale implementations across Android and iOS populations. However, our review of current and publicly available case studies and analyst feedback suggests that higher-security mobile use cases for Windows are most often made by using Windows 10 on surface devices, which functionally operate as workstations rather than mobile devices.

MobileIron

MobileIron's Platinum bundle provides a complete management solution with high-security controls and hardened accessory apps that were developed in-house. Central management is available as a cloud and an on-premises system. MobileIron's high-security offerings are well-documented on its website and in implementation guides. MobileIron appears in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites." Many capabilities counted in this evaluation are included in the MobileIron Platinum bundle or could be purchased separately.

Product: MobileIron Platinum bundle

Certifications and Awards

MobileIron provides FIPS 140-2 overall Level 1 cryptography in software for Android and iOS platforms, based on open-source OpenSSL, supplemented with RSA BSAFE and RHEL OS certifications. Local cryptography is not used, which reduces risk of API vulnerabilities. MobileIron was the first EMM vendor to have validation completed for the NSA Commercial Solutions for Classified (CSfC) Components List. It also has ECCN 5D992 export control classification. MobileIron is the first EMM vendor to receive Common Criteria certification against Version 2.0 of the Mobile Device Management Protection Profile (MDMPP V2.0 and MDMPP Agent V2.0) from the National Information Assurance Partnership (NIAP). It has also been assigned a DISA STIG for MDM and has been awarded a three-year U.S. DISA contract through Patriot Technologies and SOC Type II for cloud service. A FedRAMP application is in process.

Secure Life Cycle Management

MobileIron provides consistent, cross-platform, device-level management of security baseline policies. MobileIron has an extremely well-written guide to secure mobile installations. The EMM console can install and monitor the use of trusted root certificates, and the Sentry gateway continuously authenticates user and device identities to prevent unauthorized migration of certificates.

Hardened Platform

MobileIron does not supply hardened user device platforms or hardened OS versions; however, it interfaces with policies and capabilities in Samsung Knox. Platform verification capabilities are mostly consistent across Android and iOS — for example, where data movement protection and partial wipes are not controlled by MobileIron's container. On the server side, MobileIron conducts periodic pen tests of their web and API interfaces using a third-party service. Results are shared with customers.

App Security

MobileIron's AppConnect container provides a solid and extensive set of app management capabilities for Android and iOS. AppConnect uses DLP design elements to set boundaries on data movement between apps and in and out of a mobile device when combined with Docs@Work. MobileIron partners with software-testing vendors to secure app development. Integration with third-party app security testing providers is offered.

Data Security

MobileIron provides default encryption for data at rest in its AppConnect container and extends protection to personal cloud services and its own MCM, Docs@Work. This encryption does not extend to Office 365 in the cloud. Support for AD-RMS is provided for all supported OS and

platforms. The Sentry gateway can selectively block or allow data and network access. Data in containers can be locked/wiped if a device does not check back to the server within a predetermined time limit.

Authentication and Access Protocols

CAC/PIV is supported for Android only under Samsung Knox. For iOS, a software partner is required, and there is no capability for Windows Phone. Touch ID, derived credentials and third-party NAC vendors are supported. As a plus, the Mobile@Work client can invoke biometric authentication of AppConnect containers on iOS8 and above. Strict use of certificates helps to identify devices and containers and helps avert MITM attacks. In addition to Active Directory, MobileIron supports Active Directory as well as Lightweight Directory Access Protocol (LDAP). MobileIron Access is an option that provides SAML-based access controls for cloud services and integrates with IAM vendors.

Attack Prevention and Mitigation

MobileIron interoperates with several mobile malware detection and app reputation vendors, and can perform lock or wipe operations, based on discovery status. The MobileIron EMM client, Mobile@Work, can identify and then block many known platform exploits for Android devices.

Hardened VPN

MobileIron Tunnel is a dedicated VPN client, VPN gateway and SWG, leveraging the Sentry infrastructure and is included in the Platinum bundle. It can also work with third-party VPNs. Proxy support is available to route traffic to third-party SWGs. Client and server-side certificates are used to avoid MITM attacks. Per-app and per-container VPN invocations are supported, and they can be enforced using a feature of AppConnect called AppTunnel. Personal traffic can be split from company app and container sessions.

Multiuser Device and Kiosk Mode

MobileIron uses native capabilities in Android and iOS to create kiosk user interfaces. On Samsung devices, SAFE APIs are leveraged to prevent breaking out to the OS. Example usage includes retail point of sale (POS), ticket scanning, shipments and deliveries, and retail banking. Multiuser mode functions are thoroughly supported and can dynamically alter the user experience, depending on the login for Android and iOS; however, they are not available for Windows 8.1.

Geo/Time Tracking and Fencing

Device behavior and, to a lesser extent, application behavior can be altered according to the time of day and location. These features are consistently available across Android and iOS. A device can be automatically wiped for not reporting past a maximum time limit.

Forensics

MobileIron does not have formal relationships with forensic companies, but it can provide data for input to several popular security information and event management (SIEM) and other data aggregation tools. Device and activity events are collected in a searchable, server-side database. Administrative bypass is also available for hands-on investigation.

Scalability and Portability

MobileIron's high security features are standard, not requiring additional investments. The Platinum bundle provides a rich set of tools in a single integrated installation. The Linux-based back end makes it feasible and affordable for large-scale implementations across multiple device populations. Isolation features are included for multitenant configurations. The company reports that more than 50% of its business goes to regulated and high-security industries.

Pulse Secure

Pulse Secure is a TLS VPN vendor that spun out of Juniper and has developed a secure mobile workspace to complement the VPN. Pulse Secure has focused on enabling secure communications for BYOD use cases and typically would be used in complement to an EMM solution. The company does not appear in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Pulse Secure Workspace

Certifications and Awards

Certified cryptography is available in all products, but is not activated by default. Pulse Secure relies primarily on the native crypto provided in Android and iOS platforms for certified operations. For high-security communications, Pulse Secure has FIPS Level 1 certification for its VPN and operates with a 2048-bit key length, which exceeds FIPS 140-2 requirements. In addition, SafeLogic's FIPS 140-2 Level 1 SDK was used to build Pulse Secure AppConnect, Pulse Connect Secure and Pulse Workspace. The VPN is also Common Criteria-certified (Network Device Protection Profile).

Secure Life Cycle Management

Pulse Secure provides a EMM solution for Android and iOS platforms. This allows basic policies to be set for encryption, PIN/password, container, DLP and VPN. A device that does not check back in cannot be wiped by a local/offline action.

Hardened Platform

Pulse Secure does not supply hardened user device platforms or hardened OS versions and it does not integrate with Samsung Knox. It can support Android for Work policies for Android, and provides a trusted client for Office 365, Box and other SaaS with federated identity management on both Android and iOS.

App Security

The Pulse Secure Workspace App works with native platform capabilities to create a controlled execution for Android and iOS apps. It provides a means to whitelist apps that will have access to the VPN, cloud and to enterprise data on Android and iOS.

Data Security

The Pulse Secure Workspace App controls access to data classified for business use. Included is a trusted client for Office 365 and other SaaS offerings mentioned above. Encryption is enforced as data moves from mobile devices to EFSS providers. Users can have business and personal Workspaces, and can move between these classifications without the interruption of dual persona or container experience.

Authentication and Access Protocols

Combined with their VPN and SWG infrastructure, Pulse Secure Workspace provides CASB-style trusted client relationships with many popular enterprise SaaS providers. Authentication across providers and local device single-sign on (SSO) is achieved through Pulse Connect Secure, a SAML Identity Provider. CAC/PIC is not supported. Pulse does offer inbuilt multifactor authentication (proprietary software token) and support for RSA tokens.

Attack Prevention and Mitigation

Pulse Secure provides basic root or jailbreak detection based on device behavior and signatures.

Hardened VPN

Pulse Secure is a mainstream provider of enterprise infrastructure VPNs and fully supports TLS and IPsec for Android and iOS platforms. The FIPS 140-2 and Common Criteria (Network Device Protection Profile) version of the VPN requires a specific gateway appliance. The VPN integrates with Pulse Workspace and also is compatible with many vendors in the EMM market, including some mentioned in this report.

Multiuser Device and Kiosk Mode

Pulse Secure does not support a kiosk mode. Tailored device settings and app permissions can be offered when different users sign in to a share device, but there is no integration for use of AD credentials.

Geo/Time Tracking and Fencing

Pulse Secure does not offer these capabilities.

Forensics

Pulse Secure does not offer forensics, nor partner with forensic providers.

Scalability and Portability

Pulse Secure is a lightweight solution that will be easy to scale. Subscription-based pricing is available.

Samsung

Samsung provides integrated hardware and software solutions that use silicon-embedded processing and attestation to guarantee the integrity of everything above the silicon layer — OS, application framework and secure container. These integrity guarantees occur during system boot (Trusted Boot, Secure Boot, and TrustZone Integrity Measurement Architecture) and system operation (Real-time Kernel Protection). The solution is a hardened Android OS called Knox, which can be installed only on supported Samsung devices. Samsung does not appear in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Samsung Knox

Certifications and Awards

Knox has FIPS 140-2 Level 1 certifications that apply to data at rest, data in motion, and for protecting key storage and user credentials. Selected Samsung models are certified for the Mobile Device Fundamentals Protection Profile (MDFPP) of the National Information Assurance Partnership (NIAP), which addresses the security requirements of mobile devices for use in enterprise. Knox is approved by the United States government as the first NIAP-validated consumer mobile devices (evaluated to the MDFPP) to handle the full range of classified information. DISA has approved select Knox-enabled devices to the U.S. DoD Approved Products List (APL). The NSA has approved Knox under the Commercial Solutions for Classified (CSfC) program, and its use has been covered in a DISA STIG.

Secure Life Cycle Management

Samsung's CellWe EMM offers basic life cycle management and is part of the NIAP certification. Samsung interoperates with many third-party EMMs that provide more-comprehensive solutions. Knox features a Common Criteria mode that will put a device into a policy state that aligns with the common criteria certification. However, it should be noted that this is a platform policy option, not an official function under Common Criteria.

Hardened Platform

Samsung Knox is a notable example of a platform that combines hardened hardware and OS. Knox provides easy access to Google Play for Work and other app stores, support for Android for Work, as well as a reasonably native personal user experience, while maintaining above average system integrity.

App Security

Knox offers an encrypted container (known as the Samsung Knox Workspace) that includes an email client. The container also offers the ability to install applications directly into it and apply container-specific policies to those applications. All data in the container is protected through Knox's hardware-based integrity checking and will automatically become inaccessible if an anomaly is detected. The container can be managed by Samsung's licensed and branded EMM or by other EMM vendors who have implemented support for it.

Data Security

All data stored in the container is encrypted. All processes that execute in the container run in a separate memory space to ensure separation with processes executing outside the container. Functionality has been added to keep sensitive data encrypted when the device is powered off and when it is in a locked state. The data is only decrypted when the device is unlocked.

Authentication and Access Protocols

Knox devices can integrate with strong authentication solutions, including CAC. As of Galaxy Note 7 and Knox 2.7, Samsung supports on-device iris recognition in addition to fingerprint recognition. The CellWe EMM provides additional support for multifactor authentication.

Attack Prevention and Mitigation

All Samsung devices run Knox feature TrustZone-based Integrity Measurement Architecture (TIMA). This architecture works as a joint process between the device's hardware and the Knox software to detect suspicious anomalies. If a rogue event occurs, then the device will permanently render all data stored in the Knox container inaccessible. This data can never be recovered, and the device's container is no longer usable without hardware servicing from Samsung.

Hardened VPN

Knox offers client SSL and IPsec VPN supports customizable on a per-app, Knox container or devicewide basis. Samsung does not offer a gateway to terminate the VPN connections but supports all major VPN providers.

Multiuser Device and Kiosk Mode

Knox devices can be configured for multiuser and kiosk mode and can be managed by the Samsung EMM and third-party EMMs.

Geo/Time Tracking and Fencing

Knox devices have numerous APIs available to configure geofencing and time tracking, including controls on a per-app or container basis.

Forensics

Core defense functionality for a Knox-enabled device is to detect tampering through the TIMA and eliminate container access in response. In addition, Samsung maintains threat analysis and incident response teams, which will work with customers to facilitate investigations. Samsung also partners with an asset recovery and forensic analysis provider. Devices can be recovered even after being fully reset.

Scalability and Portability

Although Knox devices can work with other EMMs at scale, Samsung's EMM is designed for smaller deployments and is only now starting to be seen in scale by Gartner. The Samsung EMM can be used on-premises or as a cloud offering.

Sikur

Sikur provides a proprietary smartphone based on hardened Android called GranitePhone, and secure environments for off-the-shelf Android and iOS platforms that provide encrypted texting, voice and email communications, as well as document collaboration. The iOS and Android self-defending apps create a secure environment. Sikur also offers a Windows desktop application with encrypted voice and video capabilities. The design is targeted to high-security enterprise contexts and it is intended for business and government use only. Sikur also has development plans for a platform-independent, browser-based solution, including Windows mobile. Sikur does not appear in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: GranitePhone, Sikur app for iOS and Android

Certifications and Awards

Granite uses a mix of symmetric (Rijndael 192 bits) and asymmetric (RSA 2048) encryption, and all data is signed. This architecture follows FIPS guidelines, although the product is not currently certified for FIPS. Sikur is approved under Brazil's Strategic Defense Product program.

Secure Life Cycle Management

Sikur provides mobile device management across three platforms. Strong authentication is applied at the time of any device enrollment. The GranitePhone is factory provisioned by Sikur to eliminate supply chain vulnerabilities. The GranitePhone is blocked from most local peripheral services including USB and removable media, and Bluetooth. Updates of the Sikur apps and OS can be audited and certified by Sikur on all platforms.

Hardened Platform

Sikur uses its own cryptographic libraries on all platforms, avoiding API vulnerabilities and improving consistency of protection. Also, Sikur conducts periodic security audits with third-party services. The GranitePhone is completely locked down in terms of apps and services, and performs

aggressive integrity self-checks. For iOS and Android, user installed apps are not contained, but are isolated from the Sikur App.

App Security

Sikur provides their own "leak-proof apps" for encrypted voice, chat, messages, file sharing and file viewing. File creation, editing, saving and moving are strictly controlled by signed apps and services bound to the user identity. As with other considerations, there are protections for the less-secure configurations of Android and iOS, with some loss of control.

Data Security

File sharing is bound to the Sikur secure cloud environment by default and automatically synced. DLP and rights management rules are applied to the information inside the Sikur platform, and data cannot transfer to external destinations. All transfers are based on user roles and credentials configured by a central administrator and can be linked to business context. There are no supported relationships for popular EFSS tools. There is a trust relationship arrangement between the Sikur application and the cloud infrastructure of Amazon AWS and of MS Azure.

Authentication and Access Protocols

Strong and multifactor authentication are standard for all platforms. Each service request from an app receives a unique session key. CAC support is not included. Sikur provides its own authentication and IAM solutions, and does not partner. There is also no support or partnerships for NAC.

Attack Prevention and Mitigation

Sikur does not offer secure web gateway nor other anti-malware or reputation services. However, it does apply certificate pinning to avoid man-in-the-middle attacks, and other hardening techniques such as content communication signing and memory keys encryption. For iOS and Android, the Sikur app provides self-defense.

Hardened VPN

Sikur does not provide a general-purpose VPN, but its secure communication apps are end-to-end encrypted, and the communication channel is also tunneled over HTTPS using proprietary encryption adding another security layer. The design goal for strongly encrypted stored data and signed apps is considered to be the necessary level of defense.

Multiuser Device and Kiosk Mode

Kiosk modes are not offered. Multiuser operation is partially implemented through the Sikur apps and container. On the plus side, there are strong cleanup rules for destroying data after users log out.

Geo/Time Tracking and Fencing

Geofencing is supported on all platforms in terms of changing device options and features based on location, date and time. An added benefit is the ability to fully track device locations and status in emergency situations and the possibility to locate users on interactive emergency mapping systems.

Forensics

Forensic capabilities are not provided or available through partners. Encrypted log files and audit capability are offered.

Scalability and Portability

Sikur gives buyers some flexibility of device choice in hardened usage scenarios. Pricing is high, and the target markets are anticipated to be extremely niche at this time; however, the product is tightly controlled, which would make rollouts more stable for high-security end users.

Silent Circle

Silent Circle offers two solutions: a secure communication app, and a stand-alone smartphone that provides secure communications. The secure communication app is called Silent Phone and provides voice and video calls, as well as messaging and file transfer. The smartphone device is called Blackphone 2 and is based on a modified version of Android, called Silent OS. Silent Circle does not appear in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Silent Suite

Certifications and Awards

Silent Circle's mobile application cryptographic module is FIPS 140-2-validated. The cryptographic module provides encryption for Silent Circle's apps.

Secure Life Cycle Management

Silent Circle does not provide an EMM tool, but its Silent Manager administrative console can integrate with an EMM tool. Blackphone 2 can be managed with an EMM tool as well.

Hardened Platform

Blackphone runs Silent OS, which is an Android-based operating system. The platform provides Silent Space, which is an isolated portion of the device achieved through OS virtualization. Silent Space does not have Google services enabled. Spaces is an implementation of Secure Spaces from Graphite Software and is based on virtualization. Silent OS also allows setting individual app permissions.

App Security

Silent Circle provides encryption for its secure communications app community. Silent Circle provides Spaces, which allows for creating and managing separate containers for work (Managed Space) and personal apps and data on Blackphone.

Data Security

Silent Phone provides encrypted file transfer capabilities. Silent Circle does not provide any DLP or DRM capabilities.

Authentication and Access Protocols

Silent Circle provides two-factor authentication for Silent Phone via Google Authenticator for iOS, Android and Blackphone and HDE OTP for iOS.

Attack Prevention and Mitigation

Silent OS is patched within 72 hours of detection or reporting of vulnerabilities but does not provide an active defense against malware. Updates come directly from Silent Circle with no carrier involvement.

Hardened VPN

Silent Circle's solution revolves around ZRTP, which is a key agreement protocol tailored for secure real-time multimedia communications, such as SRTP. ZRTP places increased attention on minimizing risks by employing key agreements based on ephemeral keys and perfect forward secrecy.

Multiuser Device and Kiosk Mode

Apart from the general functionality in Spaces, Silent Circle does not provide any particular functionality for multiuser scenarios. Silent Circle does not support kiosk mode.

Geo/Time Tracking and Fencing

Silent Circle does not provide geolocation functionality as such, but Silent OS provides Smarter Wi-Fi. This is a mechanism that turns Wi-Fi off when a location is not near previously used Wi-Fi networks and turns Wi-Fi back on when a user approaches a location with a previously used Wi-Fi network.

Forensics

Silent Circle does not provide forensics capabilities.

Scalability and Portability

Silent Phone runs on iOS and Android, as well as the Blackphone 2. Blackphone 2 allows for COPE scenarios where some private usage of the device is combined with personal use, as well as for frequent travelers to high-concern regions. Silent Circle operates the secure communication solution with the aid of a server component that can run in the cloud.

Sophos

Sophos, based in Oxford, England, offers Sophos Mobile Control (SMC) for EMM, a secure web gateway (SWG) and a VPN, considered together in this report. It is one of only two vendors ranked in the "Magic Quadrant for Endpoint Protection Platforms" that also qualified for inclusion in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites" (the other is Microsoft). Supported platforms are Android and iOS with some support for Windows 10 Mobile and Windows Desktop.

Product: SMC Advanced

Certifications and Awards

Sophos provides FIPS 140-2 overall Level 1 cryptography in software for Android and iOS platforms and also uses local platform crypto for Android and iOS. Management of Samsung Knox is supported.

Secure Life Cycle Management

Sophos provides consistent and broad cross-platform, device-level management of security baseline policies across Android and iOS platforms, including network settings and peripherals. Sophos cannot apply strong authentication when a device is enrolled but subsequent updates are protected, especially from MITM attacks, by certificate pinning. Devices can lock immediately if critical profile settings are changed.

Hardened Platform

Sophos does not supply hardened user device platforms or hardened OS versions. It will interface with policies and capabilities in Samsung Knox and provides recommended settings for high-security use cases. Sophos also supports security APIs specific to Samsung, Sony and LG devices.

App Security

As a vendor originating in the anti-malware market, Sophos provides an anti-malware defense product for Android platforms that may be appealing in situations where app controls are hard to enforce. The anti-malware solution is fully integrated into SMC. A secure app SDK is available for Android and iOS. Sophos' native protection emphasizes data security and access control. Sophos will manage app containers under Samsung Knox. The Sophos secure email app is an OEM product from Virtual Solution.

Data Security

Sophos emphasizes data security and access control as the primary high-security defense. Sophos inserts encryption in the system file handlers, so that all data that is written becomes protected by default. In the event of a local policy violation, keys are removed, making data inaccessible. Data written to external destinations, such as cloud storage, is similarly protected, and a large number of popular EFSS solutions are supported, as well as handy basic file shares such as WebDAV. This model achieves user and app transparency, and it will not interfere with access to company data on devices that have been authorized through the installation of Sophos management. It is also compatible with Sophos security on Windows and Mac workstation-class devices. However, all apps need to be recompiled to use the feature.

Authentication and Access Protocols

Standard EMM enrollment authentication is available via SCEP. In addition to Active Directory, Sophos supports Notes Directory and LDAP, interoperates with mainstream NAC vendors and supports fingerprint readers as biometric authentication.

Attack Prevention and Mitigation

Sophos interoperates with several mobile app reputation vendors, and can use this information to set whitelists and blacklists in app stores. Several secure gateway offerings can be used to set up filtering, which involves adding Sophos Web Appliance (an enterprise gateway), Sophos UTM (a VPN) or Sophos Cloud Web Gateway. Separate mobile security apps are available to protect users from mobile malware and malicious websites.

Hardened VPN

On Android and iOS, Sophos will support native platform VPN clients, as well as mainstream third-party vendors, and also owns its own UTM and SWG solutions. Manual, continuous and per-app connections are supported. MITM VPN attacks may be detected through use of certificate pinning.

Multiuser Device and Kiosk Mode

Sophos can manage kiosk mode using Samsung, LG or Sony extensions to Android and native iOS functions, and users can be prevented from exiting the kiosk. Multiuser mode functions are not supported.

Geo/Time Tracking and Fencing

Sophos can apply location, time and network tests at an individual, project or organizational level to determine if a data container may be accessed. Additionally, Sophos now offers its own location-aware alarm and emergency notification solution that will integrate with SMC, called Sophos Mobile Alert.

Forensics

Sophos did not offer forensic capability at the time of the study, but can interoperate with mainstream forensics providers.

Scalability and Portability

Sophos is feasible for large-scale automated implementations across Android and iOS. Buyers may need to invest in several product lines to obtain all of the capabilities. SMC is available at relatively low subscription costs.

Soti

Based in Mississauga, Canada, Soti is an EMM vendor that offers solutions for Android, iOS and Windows, including legacy Windows Mobile. While Soti supports enterprise mobility deployments, it is known for its specialization in solutions for vertical and dedicated purpose tasks, as well as ruggedized platforms and connected peripherals. Soti is a major player in the Android and legacy Windows Mobile market. Soti appears in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Soti MobiControl

Certifications and Awards

Soti has no certifications and relies on the certifications of the platforms under management.

Secure Life Cycle Management

Soti offers life cycle management for Android, iOS and Windows Mobile. Because the solution has key differentiation in Android management, it has less iOS deployments when compared with other EMM vendors. However, Soti is especially strong in Android support compared with other EMM vendors, being one of the first vendors to support Android for Work on its release date. Because of the need for auditing in a vertical environment, Soti offers an audit, log and dependency strategy to track software install, install date/time, and who authorized and approved workflow and policy changes. Soti offers a feature called Android+, which reduces functional management differences among major Android platform providers. Android+ was developed cooperatively with Android device makers and ensures that Soti management policies will be applied consistently to reduce fragmentation. Additionally, Soti can directly manage rugged handheld printers and scanners, as well as appliances, ATMs and other task-specific endpoints.

Hardened Platform

Soti does not supply hardened device platforms or hardened OS versions. It will interface with policies and capabilities in Samsung Knox.

App Security

Soti offers a secure browser, app wrapping, content management (Soti hub), collaboration content management, and antivirus software for Android. Soti also fully supports and manages Android for Work, LG's Gate and Samsung's Knox. Soti licenses app wrapping from Mocana and antivirus from Webroot.

Data Security

Soti does not offer encryption for data at rest for its solution. However, Soti can manage Samsung's Knox data containers. Soti recommends the use of Mocana app wrapping; however, this is not integrated or sold as part of MobiControl.

Authentication and Access Protocols

MobiControl can integrate with Honeywell and Samsung's CAC solution for strong authentication, but does not offer additional authentication in the product.

Attack Prevention and Mitigation

Soti provides comprehensive Samsung Knox management with device integrity functionality. Soti also bundles in antivirus software for Android with several remediation and recovery choices.

Hardened VPN

MobiControl includes the ability to configure IPsec and TLS-based VPNs for Samsung's Knox and iOS. MobiControl offers a web proxy gateway for Android, but not iOS; however, it can manage an HTTP proxy setting for a .pac file URL. It does not offer a VPN gateway, but will work with several leading vendors.

Multiuser Device and Kiosk Mode

MobiControl's kiosk mode supports a new interface, multiple applications and JavaScript-based logic for scripting — for example, at work time, allow certain applications and, at home time, allow different ones. Soti's kiosk mode is used with hotels, restaurants, retailers, homecare providers, rental car companies and digital signage solutions. Soti offers multiuser support for Android and Windows Mobile, but not for iOS. Microsoft's kiosk feature (Assigned Access) can be adapted to dynamically restrict the user interface as different individuals log in and out.

Geo/Time Tracking and Fencing

MobiControl can view/track devices in real time on a map, and also mass send emergency notification messages for Android and Windows Mobile. The system can set a geofence of the wanted location(s) for applications and check that the device is within the geofence for Android and Windows Mobile. For iOS, geofencing is done on a per-device basis only. Geo and time controls combine with scripting, as mentioned above.

Forensics

MobiControl offers some interesting details for log analysis, such as software install date/time, and who authorized and approved workflow. However, there is no forensic capability and there are no partners.

Scalability and Portability

Soti has proven, large-scale special purpose deployments across multiple vertical markets. These deployments are typically Android- or Windows-Mobile-based. Soti's largest base of devices under contract use Windows Mobile, an obsolete platform still found in industrial settings.

Thales Group

Thales Group offers Teopad, a dual persona solution that provides a secure workspace for Android and iOS devices. Thales Teopad also provides a proprietary secure VoIP and messaging client. In addition, Thales provides TEO-XC, which is a custom Android device where organizations need to comply with higher security schemes. Thales does not appear in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Teopad, TEO-XC

Certifications and Awards

Thales Teopad is CSPN-certified from the French ANSSI. TEO-XC EAL3+ certification is in progress, as well as French "Diffusion Restreinte" (Restricted), which will lead to NATO-restricted and EU-restricted status. FIPS certification has been taken off the near-term roadmap.

Secure Life Cycle Management

Teopad provides Teopad Management Center (TMC), which is its own mobile device management tool for Android and iOS. Teopad supports a large number of device, app and data security policies and rules. TEO-XC supports certain additional advanced policies, such as lockdown of USB port. TMC can perform remote wipe and provide proof of deletion, as well as a selective wipe of business data only if needed.

Hardened Platform

Thales Group does not supply hardened device platforms. TEO-XC is a hardened Android OS targeted for Sony devices.

App Security

Teopad and TEO-XC provide a secure PIM out of the box. Also, Thales Group employs its own nonintrusive wrapping solution, making it possible for the Teopad container to host any third-party app, either commercial or custom, without any code modification. Wrapping provides copy/paste

restrictions from app to app. Thales recommends Pradeo for evaluating the riskiness of apps before installation on a device, but does not provide any particular integration or partnership with a mobile app reputation vendor. The solution also provides an enterprise application store.

Data Security

Teopad provides encryption for data at rest and in motion, but no IRM functionality. The container isolates professional data from the rest of the device. Enterprise file sync and share functionality is not provided, but can be integrated in the Teopad container. When using Office 365, attachments in Teopad are encrypted and stored in a specific Thales Group cloud via an Outlook plugin.

Authentication and Access Protocols

Teopad and TEO-XC provide strong authentication. Authentication and key storage can rely on a physical token, for example, a microSD card.

Attack Prevention and Mitigation

Teopad provides a proprietary trusted keyboard for PIN authentication. There are no particular hardening measures against attacks.

Hardened VPN

Teopad offers a TLS-based VPN, with a TLS gateway. The VPN is activated automatically when needed.

Multiuser Device and Kiosk Mode

Teopad does not provide kiosk functionality. Teopad and TEO-XC are not multiuser systems, although Teopad can be personalized based on user identity and shared settings.

Geo/Time Tracking and Fencing

Teopad does not support geofencing or tracking.

Forensics

Teopad does not provide any forensic functionality.

Scalability and Portability

Thales Teopad works on both iOS and Android. Its pricing is slightly higher than most secure PIM clients. The Teopad solution is typically used by groups of government high-ranked officials or top executives. Companies that are looking for a secure PIM solution that provides a stand-alone VPN as well as secure voice are good candidates for this solution.

Virtual Solution

Virtual Solution, based in Germany, offers a mobile security solution consisting of a software container called SecurePIM that includes email, contacts, calendar, note taking and mobile content management for iOS and Android. Windows is planned for the near future. What distinguishes SecurePIM from other PIM clients is the natural interface and the ability to transparently enable S/MIME for any user. This solution is ideal for any organization looking to do data separation and/or secure email on a mobile device.

Product: SecurePIM

Certifications and Awards

For iOS, SecurePIM's container, data transport and encryption solutions are certified for BSI (German Federal Office for Information Security). It also has a FIPS 140-2 Level 1 certification in process.

Secure Life Cycle Management

SecurePIM's console offers basic life cycle management. In addition, the application will work seamlessly with existing EMM solutions.

Hardened Platform

Virtual Solution is a software-based high security PIM and does not take steps to harden the platform.

App Security

SecurePIM offers jail-break/rooting detection upon execution of the application.

Data Security

SecurePIM stores all data at rest under its own encryption. It is known for transparently enabling S/MIME for users.

Authentication and Access Protocols

SecurePIM works with strong authentication solutions such as CAC. In addition, it offers the easiest way to enable S/MIME that Gartner has seen by transparently enrolling the user. The S/MIME solution works across all mobile platforms and also desktop.

Attack Prevention and Mitigation

SecurePIM stores all data at rest as encrypted and offers jail-break/rooting detection upon execution of the application.

Hardened VPN

SecurePIM provides a TLS connection to critical back-end systems. It does not offer device-level VPN technology but can utilize a per-app VPN when the application is used together with an EMM or MDM and a VPN gateway.

Multiuser Device and Kiosk Mode

SecurePIM does not offer kiosk or multiuser mode at time of this writing.

Geo/Time Tracking and Fencing

SecurePIM does not currently offer geofencing.

Forensics

SecurePIM does not currently offer forensic services, but does keep a log of security-related activities.

Scalability and Portability

SecurePIM can use its own management console or work with other EMMs at scale. Since it is an application with a native look and feel interface, it has a much lower need for support than a solution that manages the entire device or that looks radically different than the included email clients in the mobile OSs.

VMware

AirWatch is a leading EMM platform targeted for general-purpose uses for enterprise customers and is not typically used for high-security environments. High-security functionality requires either the blue or yellow product bundles. AirWatch appears in the 2016 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: AirWatch

Certifications and Awards

AirWatch's offering does not hold any security certifications for its solution, although it has been assigned a Strategic Technology Implementation Guide (STIG). However, the VMware AirWatch software is currently undergoing FIPS 140-2 and Common Criteria certifications.

Secure Life Cycle Management

AirWatch provides comprehensive cross-platform device management for iOS and Android. The solution also includes its own certificate server and can integrate with leading certificate authorities (CAs).

Hardened Platform

AirWatch does not supply hardened device platforms nor hardened OS versions. However, it will interface with policies and capabilities in Samsung Knox and supports Android for Work.

App Security

AirWatch bundles a full suite of products, including a PIM client, browser and IM. All clients feature basic DLP controls. The solution also includes AirWatch's own app wrapping and software development kit (SDK) for in-house-developed apps.

Data Security

VMware AirWatch offers basic DLP protection of cut/copy/paste with its Inbox and Secure Content Locker applications. Secure Content Locker can be purchased stand-alone if desired. It also allows rights management with Microsoft AD RMS and Azure RMS. Data at rest is encrypted using Apple's Core Crypto (iOS), OpenSSL (Android) and Microsoft Data Protection API (DPAPI; Windows) libraries using the AES-256 cryptography algorithm.

Authentication and Access Protocols

Multifactor authentication is available through Rivest-Shamir-Adleman (RSA). The solution includes VMware Identity Manager to act as an IDaaS. The solution also integrates with several leading IAM and NAC vendors and offers basic IAM and NAC functionality natively. Customers who need CAC cards are supported by means of delivery of derived credentials that can be automatically pushed to mobile devices.

Attack Prevention and Mitigation

AirWatch can interoperate with several mobile malware detection and app reputation vendors, and can remediate based on discovery status.

Hardened VPN

AirWatch integrates with most leading VPN vendors. In addition, a Transport Layer Security (TLS)-based, per-app VPN is available for Android and iOS, which terminates on the AirWatch gateway. VMware's NSX can be used in conjunction for certain apps to only have access to limited, back-end endpoints.

Multiuser Device and Kiosk Mode

AirWatch offers complete multiuser and kiosk mode support for iOS and Android. AirWatch is also the only product to offer additional multiuser tools specifically for the educational and healthcare markets.

Geo/Time Tracking and Fencing

AirWatch offers complete geo/time tracking and fencing functionality across Android and iOS. This includes the ability to remediate against a device that is out of range or has not checked in during a required interval.

Forensics

AirWatch does not offer any forensics but will directly integrate its log data into several third-party tools. The product also can detect tampering with its own agent.

Scalability and Portability

The AirWatch product has proven, large-scale global deployments. Improved since last year, updates for on-premises solutions have been synchronized with the cloud solution.

Context

Every organization has business processes that are required to operate at a high level of security. This research considers vendors for those cases where the levels of protection are critical and extreme. When these critical needs pertain to mobile devices, a management and security framework must be selected to meet appropriate standards and goals, including audit, regulatory and contractual requirements. This critical capabilities analysis gives readers suggestions on how to compare products based on practical interpretations of use cases representing frequently asked questions. Vendors that do not appear in this report may also be appropriate for your enterprise's needs and budget.

Product/Service Class Definition

High-security mobile products do not neatly fit into mainstream market definitions. For this research, a wide, representative assortment of companies was considered; however, the final list is neither complete nor exhaustive, so prospective buyers must not discount companies that are not mentioned. Products considered for this report consist of central and local (device) components. A central console controls client installations and activations, pushes data protection policies, interfaces with the help desk, acts as a key management facility, and generates alerts and compliance reports. The endpoint components manage protection policies on the target device. Managed endpoints can respond to central server directives, or they take local action to lock, wipe and recover a device that falls out of compliance.

The definition of the mobile platform is flexible. Hardware and software products that provide similar high-security experiences are compared to one another. Vendors operating in this space must first and foremost provide managed frameworks for high-security operations that can address realistic needs on one or more mainstream mobile platforms. Most importantly, vendors are expected to maximize security values for all platforms they advertise to support and minimize functional gaps among those platforms. Features may include configuration and policy management, secure versions of commonly needed apps such as email and browser, and means to control app and data

behavior in ways that meet high-security goals. Capabilities should be delivered as simply as possible, preferably not requiring complex bundling of several product lines.

Critical Capabilities Definition

Certifications and Awards

Vendors are expected to meet or exceed FIPS 140-2 Level 1 (at minimum) encryption as the default cryptography of their product set. High-security buyers value official certifications, approvals and awards. Encryption should be enabled by default.

Inclusion is allowed for companies that manage qualified embedded crypto, and those offering cryptography that exceeds FIPS 140-2 requirements. A vendor score in this capability is then incremented as a result of additional levels of qualification. These include FIPS 140-2 Overall Level 2 and Level 3, Common Criteria, and other certificates and approvals for various countries worldwide. Cryptography that is fully owned by the vendor and regularly recertified to the product line is preferred.

The most competitive vendors in this capability will have a broad set of accreditations, making them agile choices in multiple countries, and may be cited in preferred government and other industry-preferred buying programs. Use of OpenSSL is frequently chosen for data at rest, as well as VPN in mobile settings. Buyers must be satisfied with the level of support and certification guaranteed by the vendor. Extra value is given to companies that own their own cryptography and have a long history of Common Criteria certifications. Journalistic and best-in-show award categories improve stature, and are most valuable in commercial contexts.

Several vendors either have not obtained their own FIPS certification, or are in the process of obtaining certification. Buyers should be careful to consider the roadmap commitments of these vendors and potential issues that may arise if certifications are not met in a timely way. Examples include:

- Relying on a hardware and/or OS platform that has been separately certified for some of its capabilities
- Relying on other app partners to provide certified cryptography
- Claiming to have robust, equivalent cryptography, but not having official documentation

Although OpenSSL is acceptable for local encryption, SSL is no longer safe as a network privacy and authentication solution as a result of attacks, such as Poodle. Vendors should be verified before purchase to be able to support the latest versions of TLS (the successor to SSL) and to block requests to downgrade to earlier TLS or SSL versions. Within this research, TLS is the designation used.

Secure Life Cycle Management

Vendors are expected to provide life cycle management features that emphasize high-security practices and maximize security values across all the platforms they promise or advertise to support.

The vendor's baseline device management policies must be geared to high trust and verification, and must be reasonably consistent across all supported platforms. Vendors earn consideration by fulfilling requirements completely and consistently on all the platforms they support. Variance in capabilities, such as missing features or different/incompatible implementations on one platform versus another, has the opposite effect. Consideration is given to vendors that provide thoughtful and thorough recommendations for secure device settings.

Hardened Platform

Vendors that rely on and/or own device platforms to define their high-security offerings are expected to take advantage of embedded hardware, firmware and OS features. In a high-security setting, hardening of the device, as well as the OS, is important to consider.

Vendors that score well in this capability can offer robust system lockdown on one or more platforms, beyond the usual APIs and services, although they may sacrifice portability and scalability as a result. Examples may include hardened versions of Android, VMs and high-trust policy management servers.

App Security

App security is a software capability in which vendors demonstrate their ability to create programs that inherently fulfill security goals, and various forms of MAM should be present.

MAM should include app wrapping, app containers, app whitelisting and blacklisting, private app stores and owned or licensed app reputation. Testing should be appropriate to the platforms that are supported. Tamper defenses should be present, such as disabling apps after a profile violation (e.g., an unauthorized certificate migration). OS APIs may be supported, though some vendors avoid OS APIs as a potential source of vulnerability.

Data Security

Data security is the last line of defense and should be addressed by combining encryption for data at rest with access controls, leak prevention and rights management. Mobile content management (MCM) will be considered with regard to strong defense.

App-independent data security is of particular interest, because users have many ways to store, share and transfer stored (at rest) data that results in breach conditions that may not be detected by security-aware apps. Locked file folders are only a starting point. Data needs to be defensible on its own. Consideration is given to companies that have DLP features, rights-aware data containers and rights management systems. Vendors receive additional consideration toward data security if they provide additional protection avenues, such as compatibility with a mainstream rights management system. Data in motion is also considered under VPN.

Authentication and Access Protocols

Authentication and access protocols are the foundation capabilities for maintaining security. Authentication is the bane of high-security mobile installations, because strong methods interfere with the user experience.

Vendors in this research are expected to support device defaults for PIN and fingerprint at a minimum, according to platform availability, but these are not counted as "strong" authentication. Additional factors and tests will increase value, up to and including advanced biometrics and mobile smart card solutions for the most vigilant scenarios.

Attack Prevention and Mitigation

Mobile endpoint defenses must consider defense against malware and intrusion, as well as remedies in a strong security scenario. Anti-malware and IPS defenses are of elevated concern in high-security contexts, even if the amount of seriously bad code is debatably small.

High-security buyers are more concerned with targeted boutique exploits than they are with public nuisance apps. Consideration is given to fully owned and third-party defense solutions beyond basic configuration management.

Hardened VPN

VPNs provide strong defenses for data in motion by encrypting tunnels and messages to keep communications safe from hackers and verifying the trustworthiness of remote connections subject to MITM attacks. Vendors should have strong authentication choices and support several methods of VPN operation.

VPN operations can include manual start/stop, activation by domain and activation by an app or container, known as per-app VPN. Use of native platform APIs, as well as mainstream VPN partners, is typical and not remarkable in terms of affecting score. Ownership of either or both dedicated mobile VPN client and a VPN gateway improves the evaluation, as does ownership of secure web gateways (SWGs) and/or client access security brokers (CASBs), and MITM defense stories beyond basic certificate checks.

Multiuser Device and Kiosk Mode

Mobile devices are frequently shared and/or set up as public terminals/kiosks, creating extreme vulnerability for business data and additional loss or misuse opportunities. Multiuser scenarios depend on changing device operations, depending on the user identity, role and other factors.

A legacy Windows concept, for comparison, is the roaming profile. Kiosk mode also has analogous concepts, such as Windows Assigned Access, whereby a single app or select group of apps are made available in a public-facing mode for users signing on as guests or generic authorized users, while preventing access to other files, data and functionality of the platform.

Geo/Time Tracking and Fencing

User experience and access to data and services can change with location. More so when legal and business process decisions can set limits on the use of information. Highly secure, mobile defenses can depend on having access at the right place and the right time.

Vendors with this capability can alter their platform behaviors to varying degrees, including app launch, data access and other platform permissions. Situations that arise include public kiosks, POS, tactical devices for use in government, factory, finance, healthcare and export restrictions. Consideration was given to vendors who go beyond network checking to use methods such as GPS for more accurate location checks.

Forensics

Computer forensics is a specialized field in which evidence must be gathered without contaminating a potential cybercrime scene.

Most vendors offer device and configuration reporting capabilities, but few offer methods for testing, collecting and evaluating information in the legal context of a computer forensics investigation. This could involve both internal tools and partners with reputations in forensics.

Scalability and Portability

Scalability and portability are not always feasible in high-security situations. Clearly, they must be considered as increasing variations of mobile platforms come into play. Scalability and portability tend to be at odds in the mobile high-security context.

Vendors with the most dedicated solutions may not score well in this category; however, many are not intending to garner a significant chunk of the mobile market. Vendors that can secure one platform well, and are in a position to supply large installations, may score, as well as vendors that provide multiplatform support (for example, portability) with a high degree of functional consistency.

Use Cases

High-Security Government Grade

The core motivation for high-security mobile solutions is driven by government operations.

Government-related certifications and awards are critical to meeting the requirements for this use case, which reflects strict protection rules such as munitions, export controls, military personnel records and other conditions that invoke the highest levels of legal compliance. Mobile breaches in these contexts tend to lead to criminal actions.

High-Security Commercial

High-security commercial usage contexts can include regulated, nongovernment industries, such as retail and healthcare, and high-value competitive IP.

Some of the largest breach events of recent history have happened in commercial settings. Retail, healthcare and financial organizations are facing mounting fines and penalties, and insurance companies are re-evaluating their exclusion criteria. Mobile breaches in these contexts would tend to lead to civil actions. Government certifications and awards are also important to this use case.

Shared Data

Shared data is a fact of life in the connected, cloud world, where users interconnect with common file shares, as well as through more than one device at a given moment.

Users have many ways to share data with others. Given that even the most conservative organizations must adapt to the principles of a holacracy, the business process requires flexibility, even if high security is a priority. For context, it can be considered in parallel with other use cases in this research, rather than as an exclusive use case. Vendors are expected to have methods and suggestions for trusted and verified data sharing. Users in this case value authentication and broad, data-centric protection that doesn't depend on predicting every leak condition and rights managed data, but can be location- and time-sensitive.

Shared Devices

This is a long-running use case in which users access devices and data, but are kept in separate system work zones.

The shared devices use case was commonly served through specialized mobile devices used as industrial handheld terminals. It was able to scale up in nonindustrial settings through Windows tablets with roaming profiles; however, companies now need good solutions on smaller, simpler mobile devices that can even range into the bring your own (BYO) use case. Examples include public information terminals (that is, kiosks), shared (multiuser) retail POS terminals and shared medical terminals in hospitals. This context can also be applied to the nonemployee and BYO use cases.

Nonemployee

Nonemployee use cases typically involve partners, contractors and service providers. Users may not be conventionally manageable.

Nonemployee use cases involve devices that cannot be technically and legally controlled. Software portability and defense without local control are important considerations for this use case. Some buyers may decide that a completely no-footprint approach is simply not feasible. In this case, none of the typical EMM-oriented solutions may be suitable. Another consideration is that nonemployees may already have EMM frameworks in place, supplied by their own employers.

BYO

BYO is an employee-supplied use case that is difficult to manage, but nonetheless must participate in a high-security mobile context.

Primarily, employee platforms are in scope, but there is clearly a relationship with the nonemployee use case described elsewhere. Basic consideration requires a credible plan for dealing with devices that cannot accept an agent. Examples include users who refuse to accept management, and situations in which the user works under legal jurisdictions that would prevent or interfere with management and potentially invalidate the company's security obligations.

Vendors Added and Dropped

Added

- Cyber adAPT has acquired Mobile Active Defense and is evaluated as Cyber adAPT
- Pulse Secure
- Silent Circle
- Virtual Solution

Dropped

- Globo has gone out of business
- Good Technology was acquired by BlackBerry and is no longer tracked separately
- Oracle has exited the EMM market at this time

Inclusion Criteria

Vendors included in this Critical Capabilities research were picked from a representative, but not exhaustive, list of those that were qualified for inclusion in the "Magic Quadrant for Enterprise Mobility Management Suites." Additional vendors were selected on the basis of offering software and hardware products that specifically appeal to high-security buyers. Inclusion criteria include:

- Owned, licensed, or used embedded FIPS 140-2 certification for all encryption operations of the product, provided full support for crypto maintenance and updates, and recertified regularly. FIPS mode operation must be the default. Vendors using crypto that exceeds FIPS 140-2 requirements will also be considered.
- Commercially supported, with centrally managed security controls, lockouts and key management/recover and system recovery methods that operate in FIPS mode by default.
- Provided basic mobile management functions as part of the platform, with recommendations for high-security configurations.
- Showed compelling evidence for targeting high-security buyers.
- Offered products that operate on at least one of the current mobile OS platforms.
- Fully released, available and shipping prior to July 2016. Future products are not assessed.

Products from these vendors may play a future role in the high-security managed mobility topic area:

- Google Android for Work is Google's program for providing software-based, business-oriented app security and management platforms. Features include securely provisioning and isolating company apps and data, granular VPN, a suite of integrated PIM apps and blocking measures against copy/paste and screen capture, as well as against app-side loading. Android for Work can be managed through EMMs, including several represented in this report.
- Kaprica Security's Tachyon, launched in 2015, facilitates automated provisioning of Samsung Android devices. Its licensing model works as an additional fee on top of an EMM or Samsung Knox cost. Kaprica Security may appeal to organizations that are looking to adopt Samsung Knox as their primary platform and want basic provisioning and configuration assistance. Buyers may need to supplement other features, such as app and data security, with an additional EMM tool.

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	High-Security Government Grade	High-Security Commercial	Shared Data	Shared Devices	Nonemployee	BYO
Certifications and Awards	15%	15%	10%	10%	15%	0%
Secure Life Cycle Management	15%	10%	10%	10%	18%	5%
Hardened Platform	10%	5%	0%	5%	0%	0%
App Security	7%	10%	5%	8%	5%	20%
Data Security	7%	10%	15%	10%	5%	20%
Authentication and Access Protocols	5%	7%	10%	10%	15%	10%
Attack Prevention and Mitigation	10%	5%	5%	10%	15%	2%
Hardened VPN	15%	3%	2%	2%	10%	10%
Multiuser Device and Kiosk Mode	0%	15%	10%	20%	0%	0%
Geo/Time Tracking and Fencing	10%	5%	13%	5%	15%	3%
Forensics	6%	5%	0%	0%	0%	10%
Scalability and Portability	0%	10%	20%	10%	2%	20%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**
						As of August 2016

Source: Gartner (August 2016)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	VMware	Atos	BlackBerry	Check Point Software Technologies	Citrix	Cyber adAPT	GSMK	IBM	Kaymera Technologies	Microsoft	MobileIron	Pulse Secure	Samsung	Sikur	Silent Circle	Sophos	Soti	Thales Group	Virtual Solution
Certifications and Awards	1.3	4.5	4.3	4.0	2.5	3.5	3.0	3.0	2.5	1.8	4.3	2.5	3.8	2.0	2.0	2.3	1.0	3.0	2.3
Secure Life Cycle Management	3.8	4.0	4.0	2.0	3.5	3.5	2.5	3.8	3.0	2.3	3.8	2.0	2.5	4.0	1.5	3.0	3.3	3.5	2.0
Hardened Platform	1.5	4.0	3.5	2.0	1.5	1.0	4.0	1.5	2.8	1.8	2.3	1.8	4.0	4.0	3.0	1.8	1.3	3.0	1.0
App Security	2.5	4.0	4.0	3.0	3.5	3.5	4.0	3.0	3.5	3.0	3.0	2.0	4.0	3.8	2.5	3.0	3.0	3.5	3.0
Data Security	2.3	2.0	4.0	3.0	4.0	2.5	3.0	3.0	3.3	3.5	3.0	2.5	4.0	3.5	2.0	4.0	2.0	2.5	3.5
Authentication and Access Protocols	3.0	4.0	4.0	2.5	4.0	3.0	1.5	3.8	1.5	3.0	3.3	2.0	3.0	3.0	2.5	2.3	2.0	2.3	4.0
Attack Prevention and Mitigation	2.0	3.5	4.0	3.5	1.8	3.5	3.5	3.5	3.0	1.8	2.8	1.5	3.5	1.5	2.0	3.0	2.8	2.0	3.0
Hardened VPN	3.0	4.0	3.8	2.3	4.0	4.0	2.0	2.5	3.3	1.3	3.5	3.5	3.0	1.5	3.0	2.5	2.0	3.0	1.5
Multiuser Device and Kiosk Mode	3.0	1.0	2.3	1.0	3.0	3.0	2.0	3.0	1.5	1.0	2.8	1.5	3.0	1.5	1.0	1.5	3.5	2.0	1.0
Geo/Time Tracking and Fencing	4.0	1.0	2.3	1.5	3.0	4.0	2.5	3.5	4.0	1.5	2.8	1.0	3.5	4.0	1.5	2.8	3.0	1.0	1.0

Critical Capabilities	VMware	Atos	BlackBerry	Check Point Software Technologies	Citrix	Cyber adAPT	GSMK	IBM	Kaymera Technologies	Microsoft	MobileIron	Pulse Secure	Samsung	Sikur	Silent Circle	Sophos	Soti	Thales Group	Virtual Solution
Forensics	2.5	1.3	2.0	2.0	2.0	2.0	2.0	2.5	2.5	1.0	2.0	1.0	3.5	1.5	1.0	1.5	1.5	1.0	2.0
Scalability and Portability	3.8	1.0	4.0	3.0	4.0	3.5	3.5	3.8	2.5	3.5	4.0	3.0	2.5	3.0	2.5	4.0	3.3	3.0	4.0
As of August 2016																			

Source: Gartner (August 2016)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	VMware	Atos	BlackBerry	Check Point Software Technologies	Citrix	Cyber adAPT	GSMK	IBM	Kaymera Technologies	Microsoft	MobileIron	Pulse Secure	Samsung	Sikur	Silent Circle	Sophos	Soti	Thales Group	Virtual Solution
High-Security Government Grade	2.60	3.42	3.68	2.61	2.98	3.19	2.81	3.01	3.00	1.99	3.24	2.11	3.42	2.83	2.13	2.63	2.20	2.62	2.15
High-Security Commercial	2.69	2.82	3.57	2.54	3.14	3.13	2.82	3.15	2.65	2.20	3.28	2.06	3.35	2.76	1.94	2.66	2.47	2.60	2.42
Shared Data	3.02	2.44	3.64	2.57	3.44	3.33	2.79	3.40	2.76	2.50	3.39	2.15	3.22	2.99	1.98	3.02	2.66	2.52	2.72
Shared Devices	2.76	2.75	3.58	2.46	3.17	3.16	2.79	3.23	2.57	2.22	3.25	2.02	3.29	2.73	1.94	2.68	2.64	2.57	2.45
Nonemployee	2.85	3.39	3.77	2.68	3.18	3.50	2.65	3.38	2.91	2.15	3.39	2.05	3.27	2.87	2.05	2.78	2.43	2.54	2.46
BYO	2.92	2.63	3.73	2.70	3.60	3.17	2.92	3.21	2.92	2.73	3.21	2.31	3.35	3.01	2.21	3.12	2.52	2.68	3.04
As of August 2016																			

Source: Gartner (August 2016)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrant for Enterprise Mobility Management Suites"

"Critical Capabilities for Enterprise Mobility Management Suites"

"Mobile Device Security: A Comparison of Platforms"

"How to Avoid the Top 10 EMM/MDM Deployment Mistakes"

"How Products and Services Are Evaluated in Gartner Critical Capabilities"

Evidence

Readers may click here to view a white paper from Google, describing Android for Work.

Readers may click here to view a white paper from Samsung, comparing Knox to Android for Work.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each

capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp