Gartner LICENSED FOR DISTRIBUTION

Critical Capabilities for High-Security Mobility Management

Published: 24 August 2017 **ID:** G00315906

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

Summary

High-security mobility management is a subset of the enterprise mobility management market, which serves organizations with stringent requirements. When security is a high priority, security and risk management leaders should pursue best-of-breed solutions for each platform they plan to support.

Overview

Key Findings

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

Recommendations

Security and risk management leaders responsible for endpoint and mobile security strategies should:

- Choose best-of-breed solutions for each platform they plan to support, if security is their highest priority.
- Choose products that will support business processes without undue disruptions or interference, because solutions with high-security qualifications may not meet usability expectations.
- Plan tiers of access that support less-secure configurations for less-sensitive tasks, especially in high-security organizations.

Strategic Planning Assumption

Through 2022, organizations that require the highest levels of security will prefer platforms that rely on dedicated security hardware and software that leverage trusted environments.

What You Need to Know

This document was revised on 7 September 2017. For more information, see the Corrections page .

The decision to pursue the highest levels of security and privacy on small mobile devices that do not run workstation-class OSs 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 a subset of providers covered in the 2017 "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 qualify to manage high-security use cases. These vendors do not represent an exhaustive list and are limited to a representative sample.

There are various methods for creating secure environments in software and hardware, using a combination of containers, hardened apps, rights methodologies, server-side controls 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 and expensive, and they usually 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.

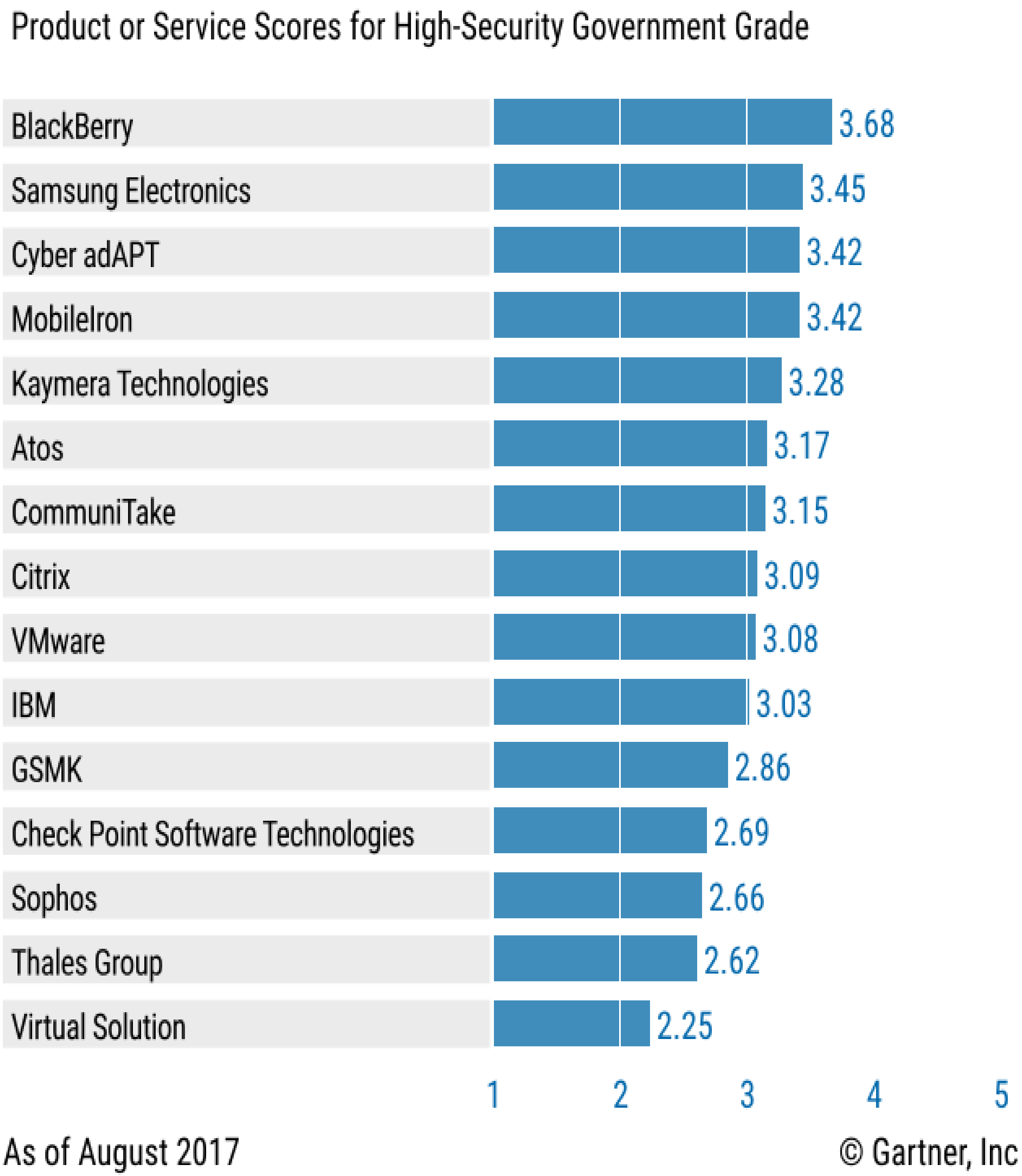
This research assesses the following six use cases that are described in a later section:

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

Analysis

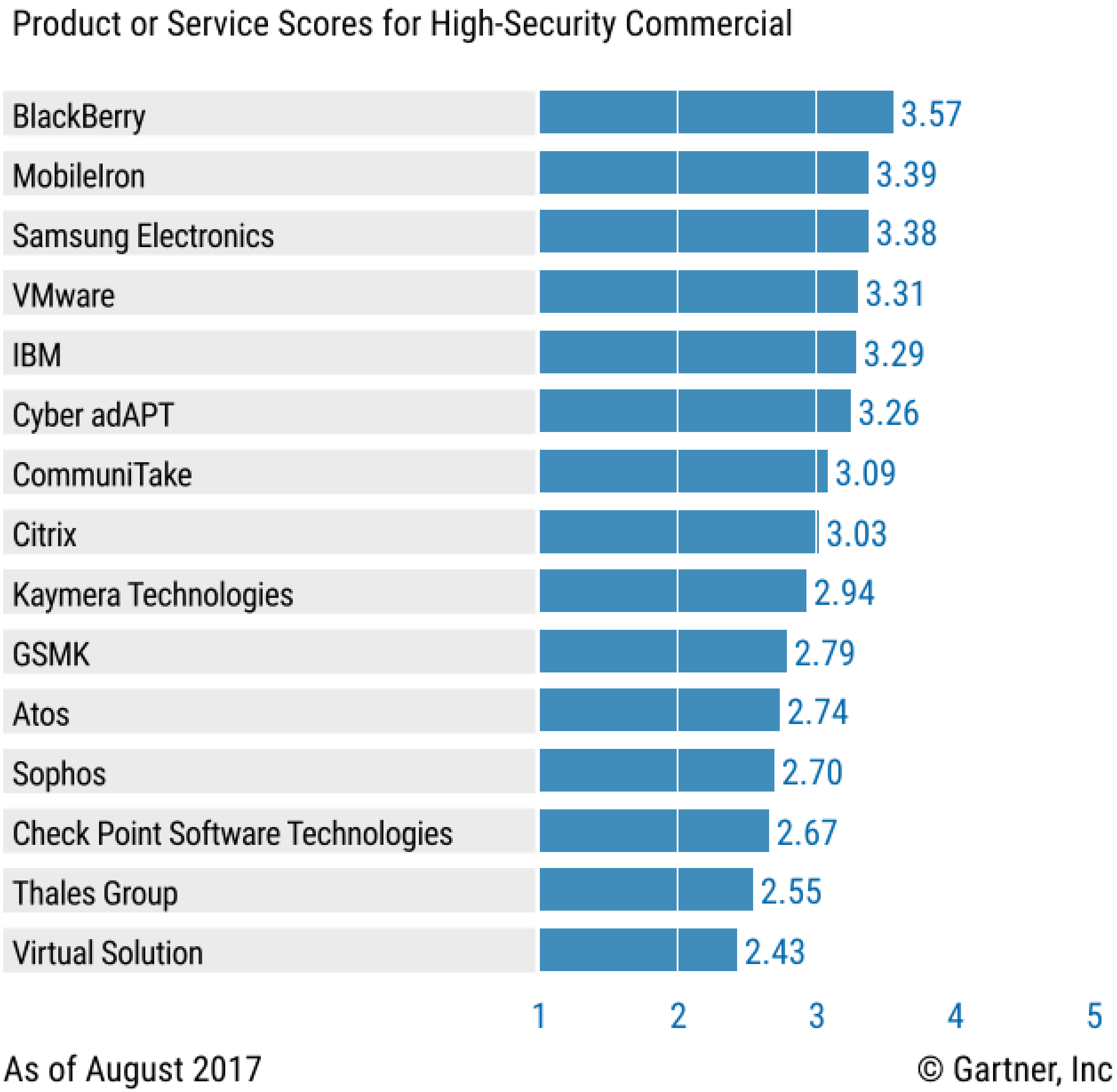
Critical Capabilities Use-Case Graphics

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



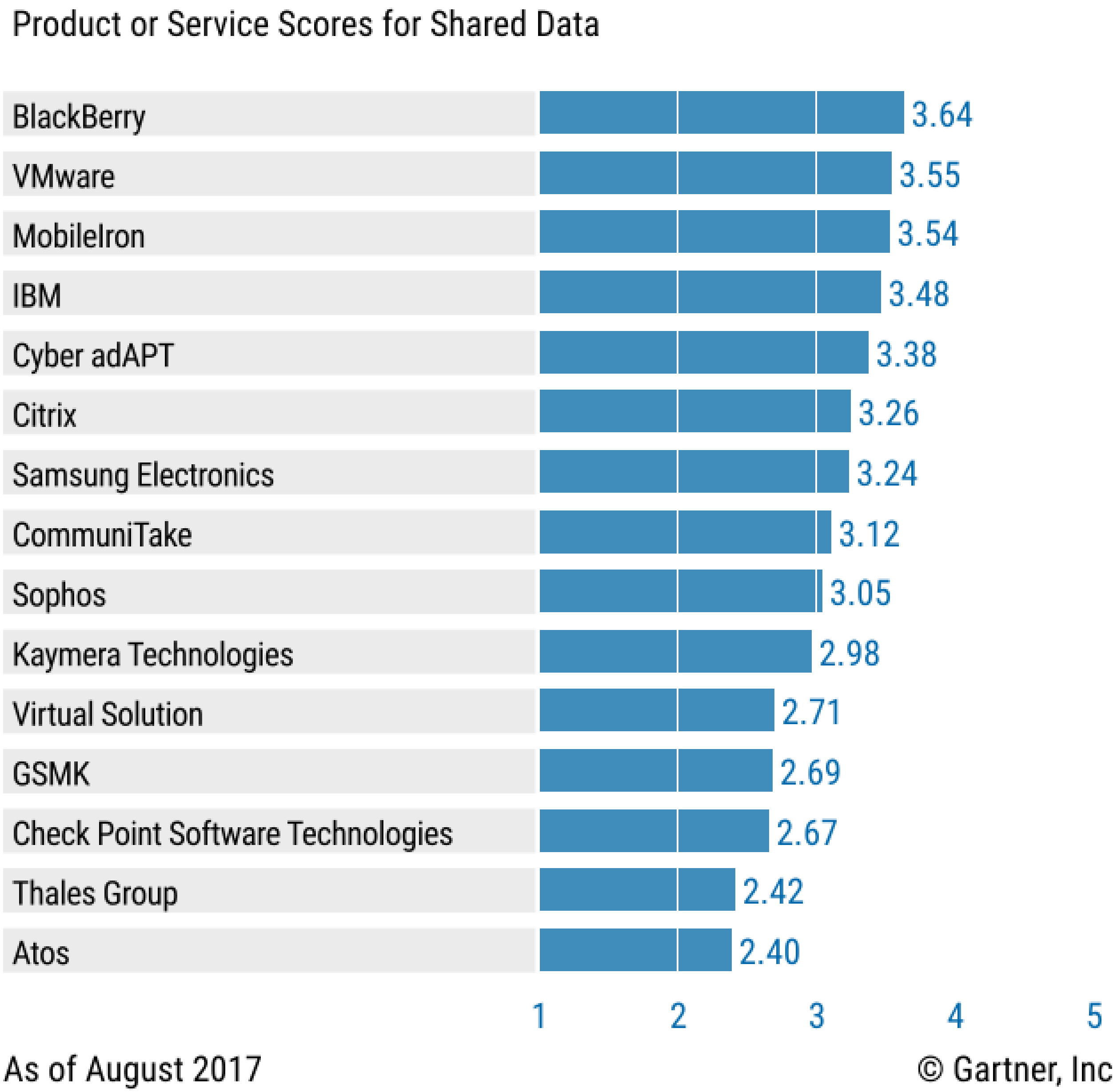
Source: Gartner (August 2017)

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



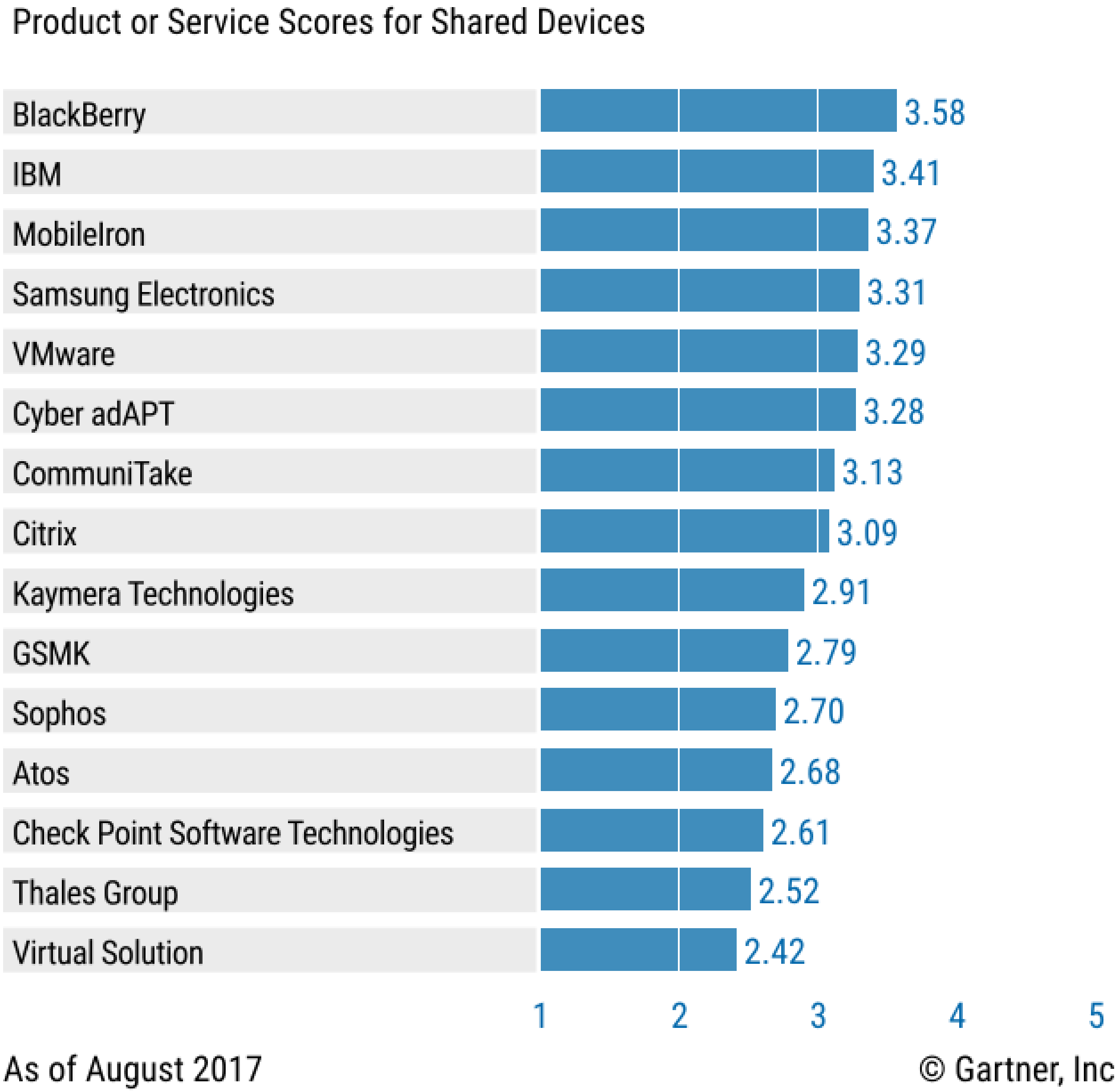
Source: Gartner (August 2017)

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



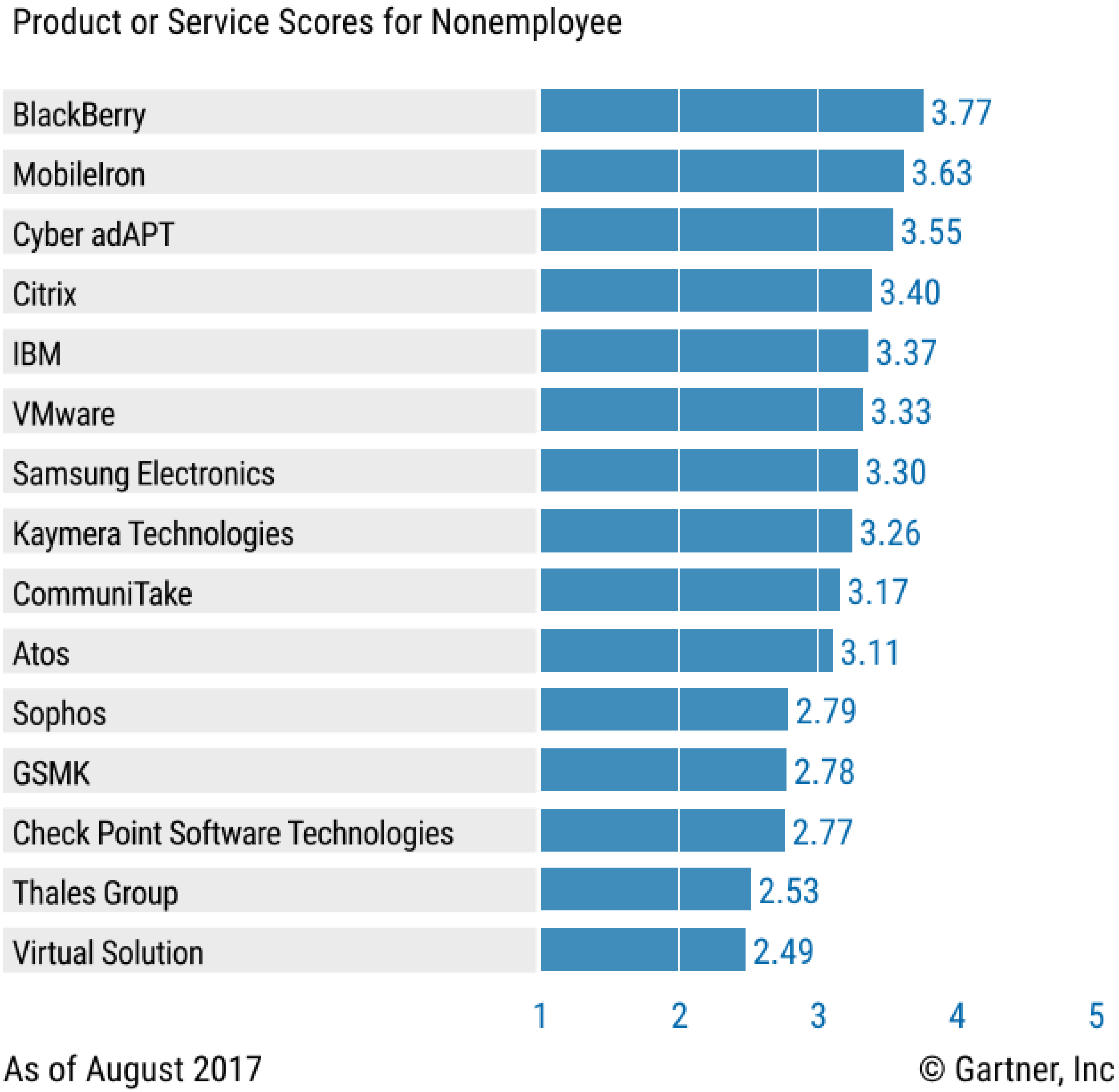
Source: Gartner (August 2017)

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



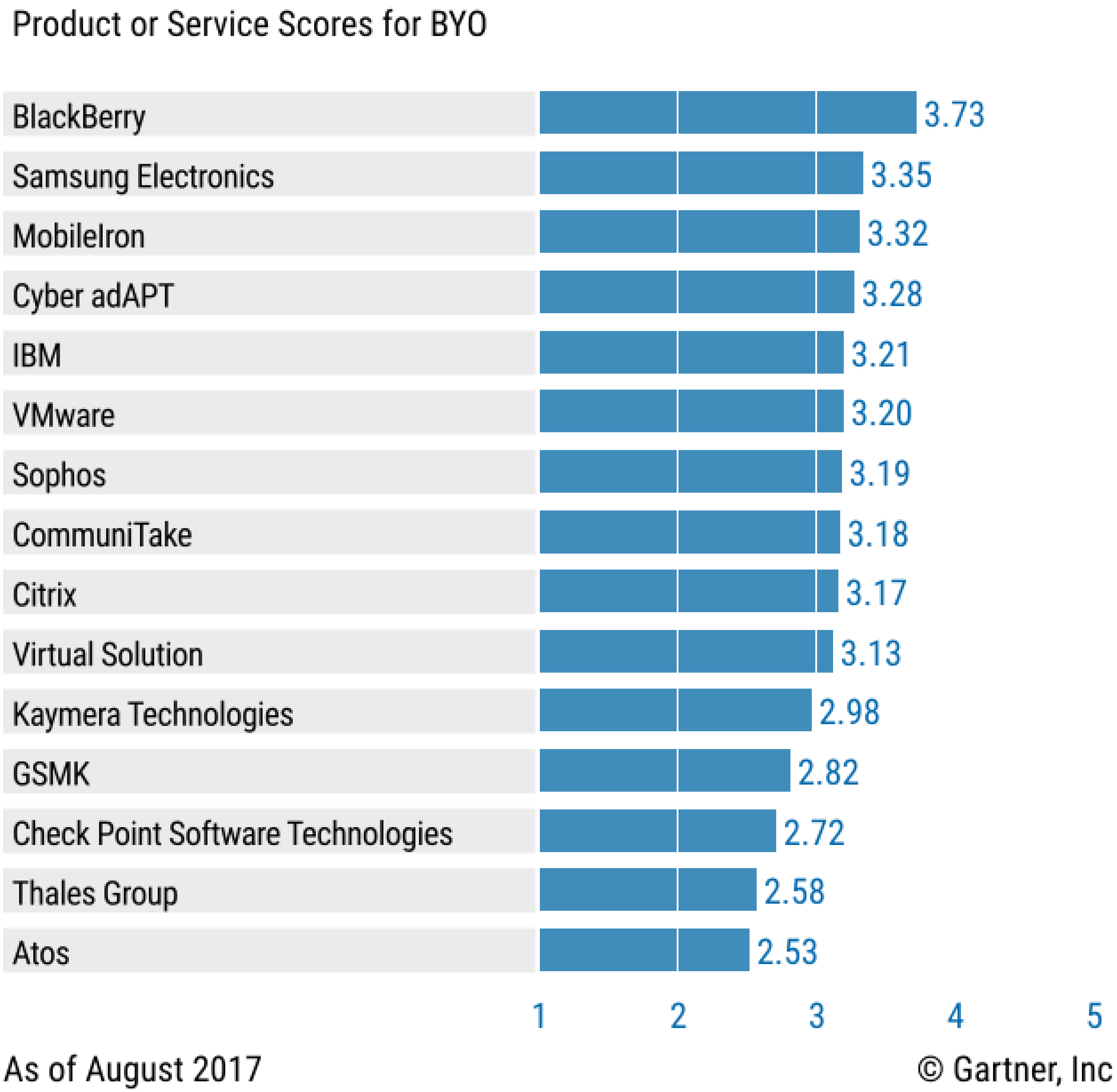
Source: Gartner (August 2017)

Figure 5. Vendors' Product Scores for the Nonemployee Use Case



Source: Gartner (August 2017)

Figure 6. Vendors' Product Scores for the BYO Use Case



Source: Gartner (August 2017)

Vendors

Atos

Headquartered in Bezons, France, Atos provides Hoox for Business, a self-contained mobile platform for protecting enterprise communications and data, based on a range of trusted smartphone devices and infrastructure. In addition to a hardened platform and mobility management, Hoox for Business provides functionality, such as secure voice conferencing, secure instant group messaging and secure voice mail. It also helps ensure compliance with regulations, including European (e.g., GDPR, NIS and MIFID II).

The Hoox k3 and k30 devices are built for high-security enterprise contexts, with an option to support personal use. Atos did not appear in the 2017 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Hoox

Certifications and Awards

The Atos Hoox is certified to EAL4+ HSM Proteccio for key management. The device is HSM Proteccio approved in France Restricted (ANSSI) and NATO Secret on FIPS 140-2 Level 3.

Secure Life Cycle Management

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

Hardened Platform

Atos provides a locked-down platform, where peripheral connections, such as Near Field Communication (NFC), have been disabled, and Bluetooth device support can be limited, for example, to nonsensitive calls. Google services are removed on Hoox devices, although third-party apps can 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 will support information rights management and content-based data loss prevention (DLP). File transfer leverages the hardware security module (HSM), which is used for secure voice calls and messaging. 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

Two-factor authentication (2FA) is natively present and nonremovable. Authentication is based on a combination of a challenge and a passcode or a fingerprint scan. Hoox uses its own certificate authority (CA), and it supports certificate revocation. Common Access Card (CAC) is not natively supported, because it is not a European Union or NATO standard.

Attack Prevention and Mitigation

The device offers a reduced attack surface; therefore, attention to detail focuses on disabling many functionalities, such as NFC, Google services and AT commands. The device performs an OS authentication and integrity test at boot time and runtime, providing a permanent control of integrity by block, as well as for checking apps before use.

Hardened VPN

The solution leverages open virtual private network (VPN) and mutual authentication. Full tunnel mode is enforced. The system uses device APIs to prevent network communication if the VPN fails or is disabled.

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 a hardened solution that is a good choice for high-security use cases. Pricing for the Hoox devices is comparable to mainstream high-security commercial solutions. The typical deployment will involve small, targeted user groups; however, the solution scales to thousands of devices.

BlackBerry

BlackBerry, headquartered in Waterloo, Canada, now offers the BlackBerry Enterprise Mobility Suite (BEMS). This is now a mature integration of BES, Good Technology and WatchDox capabilities. BlackBerry appears in the 2017 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: BlackBerry Enterprise Mobility Suite

Certifications and Awards

BlackBerry has worked to build consistency of certification from acquired products now integrated in BEMS. This includes consistent compliance testing for Common Criteria EAL4+, and FIPS 140-2 Level 1. BMS supports a large range of keys and key sizes to meet government needs, and is undergoing NIAP certification. BlackBerry provides its own encryption for Android, iOS and Windows platforms. Other certifications and awards 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, and a DISA STIG. NSA NIAP MDM validation for BEMS is in process.

Secure Life Cycle Management

BlackBerry provides a variety of baseline secure enterprise mobility management (EMM) functions for Android, iOS, OS X, Windows 10 and BB10 OS. Guidelines are offered for default high-security EMM configurations. BlackBerry Dynamics is completely manageable as a container by BlackBerry's unified endpoint management (UEM), with the same policies on multiple platforms and unmanaged devices. BlackBerry 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. In addition, BlackBerry Dynamics can detect exploit attempts, jailbreaking/rooting, and locking or wiping exploited, lost or unauthorized containers.

Hardened Platform

BlackBerry offers a hardened version of Android for its DTEK60, KEYone and future BlackBerry Android devices, and supports Samsung Knox and Android enterprise features (formerly known as Android for Work). BlackBerry's Android distribution is maintained directly by BlackBerry on a monthly patch and update schedule. 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. BlackBerry Dynamics apps, such as Work and Access, can run within the Knox Workspace, and device health attestation is supported for verifying device integrity. Keys may be stored in the Trusted Execution Environment (TEE).

App Security

BlackBerry securely manages apps in its security container framework and via native OS capabilities in Android and Samsung Knox. In the event of a profile violation caused by the user, malware or some other reason, access keys are withdrawn. Locked, containerized data is not recoverable by local action, and can be selectively or fully wiped. Trusted root certificates can be associated with individual apps, as well as containerized apps, and additional app passwords can be required.

Data Security

The BlackBerry Workspaces (formerly WatchDox) component provides a secure enterprise synchronization and sharing (EFSS) solution and incorporates a rich set of digital rights management (DRM) tools that run on mobile platforms, as well as PCs (Windows and Mac) and web browsers to provide functional controls (e.g., no print or no copy/paste) 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 container framework. Several popular third-party EFSS systems 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

BSM natively supports various 2FA solutions, as well as biometrics and CACI. 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 (MFA), TrustZone and various biometrics. Partnerships with NAC vendors defend container access to internal networks. BlackBerry's network operations center (NOC) provides high-assurance registration of Samsung devices via International Mobile Equipment Identity (IMEI).

Attack Prevention and Mitigation

BSM relies on strict app controls as the primary line of defense. Container network connections can be directed into several secure web gateway (SWG) and app reputation vendors, so that users can perform additional tests. Third-party apps approved for the container are tested and signed with Veracode and are guaranteed to be certified when downloaded from commercial app stores. BlackBerry Dynamics integration with Zimperium is available 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, then 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, and supports proxies for third-party SWGs on Android and iOS. The container can work with device-embedded VPN clients; however, the preferred communications method associates a fully contained micro-VPN with each managed app. Secure per-app sessions can be alternately managed on a per-app basis by the NOC, allowing secure communication without raising a VPN.

Multiuser Device and Kiosk Mode

BlackBerry can create a basic multiuser mode on a per-user basis for Android and iOS. 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 for Android, iOS and Windows. Additional tracking features including time tracking is handle via third parties. 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 that is integrated with BlackBerry Dynamics and can be deployed via BlackBerry's UEM.

Forensics

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

Scalability and Portability

BlackBerry is feasible and affordable for large-scale implementations, and it provides a good level of 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

Headquartered in Tel Aviv, Israel, Check Point is a leading global firewall and VPN vendor. Its mobile security solution consists of a software container called Capsule (Workspace, Docs and Cloud) for both iOS and Android, a threat prevention solution called SandBlast Mobile, and Capsule Connect/VPN. The Capsule Workspace is a traditional product information management (PIM) client and Capsule Docs offering basic mobile content management (MCM) functionality and access to internal resources. SandBlast Mobile offers real-time detection of OS exploits and malware, as well as network, SMS and cellular attacks. Check Point Capsule Connect/VPN offers secure remote access for mobile devices. Check Point does not appear in the 2017 "Magic Quadrant for Enterprise Mobility Management Suites."

Products: Check Point Capsule Docs, Sandblast Mobile, Capsule Connect, Capsule Connect/VPN, 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

Capsule Workspace does not offer any device management functionality; however, 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 in 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 in the container.

Data Security

Check Point Capsule Workspace can protect 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

Capsule Workspace and SandBlast Mobile offer 2FA for access to its container. However, it does not support high-security solutions, such as CACs. There is no third-party identity and access management (IAM) support, nor is IAM as a service (IDaaS) provided.

Attack Prevention and Mitigation

SandBlast Mobile Prevention offers software-based, real-time malware, network attacks, SMS attacks, jailbreak and root detection for 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. There are no direct remediation capabilities between the SandBlast Mobile detection module and Check Point gateways.

Hardened VPN

Capsule Connect and Capsule VPN offer IPsec and Transport Layer Security (TLS) VPN connections to Check Point gateways. The VPN is IP- or domain-activated, but does not offer per-app VPN. Users can disable this VPN at any time, which is a serious caution for high-security environments.

Multiuser Device and Kiosk Mode

Capsule Workspace supports multiple users.

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 additional forensics. SandBlast Mobile can export 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 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

Headquartered in Fort Lauderdale, Florida, Citrix offers XenMobile Enterprise. XenMobile is a comprehensive mobile management solution that also integrates with the company's server-based computing, virtual desktop and VPN products, including Android, iOS, Mac OSX and Windows 10 platform management. Citrix has announced a major partnership with Microsoft aimed at marketing the XenMobile solution to customers migrating to or using Microsoft's Intune EMM product. In these scenarios, Citrix positions XenMobile EMM as an additive tool to Intune, when the latter is deployed in a "without enrollment" configuration. Citrix appears in the 2017 "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 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 CAs. 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 or hardened OS versions. However, it allows for the leveraging of policies and capabilities in Samsung Knox and Android.

App Security

In addition to an included set of apps, such as secure email and browser, the XenMobile MDX wrapper works across all supported platforms, 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 input/output (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 cloud access security broker (CASB) vendors, making it easier to direct business processes away from vulnerable sync and share platforms. On iOS, key data is not saved in the OS keychain.

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, and the ability to perform remote posture assessment via SmartAccess. Commercial apps that have been wrapped for Multidimensional Expressions (MDX) are trusted and signed in the Citrix Worx Home Store. Citrix has validated integrations with an ecosystem of mobile threat detection vendors.

Hardened VPN

Citrix NetScaler, an application delivery controller that has been optimized for Xen Desktop and XenMobile users, provides VPN and SWG 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 should specify their requirements.

XenMobile establishes platform authentication prior to the first use of the VPN, which means that certificate data is pinned and never exposed, reducing the possibility of network layer, man in the middle (MITM) attacks against remote access logins. Direct, app-to-server, encrypted connections are supported by the Citrix Micro VPN, and do not require other VPN hardware or gateways.

Multiuser Device and Kiosk Mode

XenMobile offers a comprehensive set of features for configuring and managing multiuser mobile platforms shared apps, 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 the 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 the time of day and location for Android and iOS only. On all supported platforms, Citrix can apply location decisions to restrict access to data 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 the 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.

CommuniTake

Headquartered in Yokneam, Israel, CommuniTake provides an integrated range of enterprise mobility solutions to provision and protect enterprise data over mobile devices. CommuniTake's offering includes CommuniTake Intact Mobile Security (CIMS), which acts as the EMM platform; IntactPhone, a purpose-built mobile device; IntactOS, a custom-built security-rich OS; as well as ancillary tools, such as IntactDialog for secure instant communications; IntactCC, which acts as control center; IntactApps for security utilities; and IntactCare for support services. (CommuniTake does not appear in the 2017"Magic Quadrant for Enterprise Mobility Management Suites.")

Products: CIMS, IntactPhone, IntactOS, IntactDialog, IntactCC, IntactApps

Certifications and Awards

CommuniTake uses components in its solutions, including OpenSSL and Open VPN, validated to FIPS 140-2 Level 1. The company is in the process for obtaining common criteria certification. It is used by various government agencies, including ones in Mexico and Argentina and several in the Asia/Pacific region.

Secure Life Cycle Management

CommuniTake provides its own centrally managed EMM tool, CIMS, and a nonremovable, on-device agent embedded within IntactOS. CommuniTake also provides management for Android and iOS devices. Beyond basic MDM policies, CIMS offers SIM card changing alerts, app management controls, roaming or usage plan violations, peripheral lockdown and internet connection disabling, text blocking, and archiving.

Hardened Platform

IntactPhone runs a locked and hardened version of Android, called IntactOS. It leverages a hardware-based root of trust, including the EAL7 criteria for Trustzone, and performs continuous integrity checks. CommuniTake has full control of the supply chain for all software and components. Individual controls for USB, removable media, Bluetooth, etc., are centrally enforced by CIMS and locally managed through enhanced proprietary drivers, and may not be changed by the user. Google services are disabled and replaced with a private app store and proprietary push services. In the case of apps that won't run without access to a specific peripheral, such as a camera, IntactOS can spoof devices and return blank data.

App Security

CommuniTake provides containment and a set of IntactApps inside the container. Apps include secure instant communications, panic button, self-troubleshooting app, remote control and secure browsing. CommuniTake does not provide app wrapping or SDK functionality for enterprises to add more apps into its container. Third-party apps cannot be installed, unless certified and uploaded to the private app store by the admin. A proprietary hardware controller prevents from unauthorized apps and networks (rogue Wi-Fi, malicious cellular antennae) from accessing the device's sensors or peripherals.

The secure instant communication apps leverage the Z and Real-time Transport Protocol (ZRTP) protocol for key agreement and Secure Real-time Transport Protocol (SRTP) for encryption of the video and audio communications. For texting, it uses PKI and AES-256 encryption. Complete archiving functionality is provided, if needed, as well as PBX integration.

Data Security

CommuniTake provides trusted viewing and monitoring for file transfers, in addition to secure file transfer. IntactPhone automatically detects attempts (and alerts) to physically extract data from the device and automatically wipes all secure data. EMM policies may be set to obfuscate data in use by apps.

Authentication and Access Protocols

A rigorous authentication process is used to register devices at enrollment and to perform periodic ongoing checks, involving a progress of unique PINs, certificate creation and hash-based message authentication codes (HMAC). Passcode protection can be enforced on various levels, including device and app level. Multifactor strong authentication is supported, but CAC is not supported. Mutual authentication is implemented for transport security. Certificates may be set to automatically expire and trigger recertification, for example, to protect devices that do not check in.

Attack Prevention and Mitigation

CommuniTake can lock down devices, especially its own IntactOS ones, by disabling peripherals, such as NFC or Bluetooth. In addition, CommuniTake provides capabilities to detect rogue Wi-Fi networks IMSI catchers, as well as exploits leveraging SS7 vulnerabilities. CommuniTake leverages Sophos' mobile anti-malware solution.

Hardened VPN

CommuniTake's VPN leverages TLS and uses IKEv2 for key agreement. Certificate pinning is implemented, as well as additional protections for MITM attacks. The VPN is persistent and does not allow split tunneling. CIMS can also accommodate third-party VPNs and act as a VPN aggregator in the back end.

Multiuser Device and Kiosk Mode

CommuniTake supports kiosk mode with third-party apps, or with several of its in-built, contained apps. Many of CommuniTake's use cases involve purpose-built devices used in kiosk mode.

Geo/Time Tracking and Fencing

CIMS can locate the device and enforce policies, such as blocking the use of specific applications, visiting certain URLs or domains, and restricting (limited to Android) the use of specific resources (e.g., the camera or microphone). The system power administrator can enable a bring your own device (BYOD) privacy policy that, once enabled, halts collection of location and service usage data, but alerts the system administrator, if the device violates geofencing or time-fencing restrictions.

Forensics

CIMS can record user and device history, including recorded voice calls and messages. It can log anomalies and provide an audit trail to a forensics equipment company. CommuniTake also collaborates with Cellebrite (an investor in CommuniTake) when there is a need for a forensic examination. Cellebrite is also one of CommuniTake's salient investors.

Scalability and Portability

CommuniTake's CIMS can be delivered on-premises, as well as a cloud solution. CommuniTake can integrate with an existing EMM suite or provide its own device management. CIMS will appeal in high-security environments requiring strict device and traffic controls. The product design supports quick setup and is suited to situations in which buyers prioritize high-security solutions for COPE and BYO devices.

Cyber adAPT

Cyber adAPT is headquartered in Half Moon Bay, California. Cyber adAPT's EMM platform, skwiid Mobile, was developed via the acquisition of Mobile Active Defense. Skwiid Mobile 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 skwiid Server gateway applies security policies and provides identity management and authentication, although skwiid Mobile's client provides on-device, tamper-resistant connectivity to the skwiid Detection Platform for behavior-based threat detection. Cyber adAPT does not appear in the 2017 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: Cyber adAPT skwiid Platform

Certifications and Awards

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

Secure Life Cycle Management

Skwiid Mobile supports granular EMM policies for iOS, Android, Mac OS and Windows, including complex passcodes, and partial and full device wipe, as well as blocking external media and cloud storage. In addition, skwiid Mobile can interoperate with other EMM suites.

Hardened Platform

Cyber adAPT's skwiid Server is built on a hardened Debian Linux platform, with an integrated stateful firewall. On the device, the skwiid Mobile 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, skwiid can prevent the removal of the VPN. A hardened version of Android is available for customers who want to replace the off-the-shelf image.

App Security

Skwiid Mobile manages a list of blacklisted apps and integrates with RiskIQ. Any apps that exhibit anomalous behavior will be identified by the skwiid threat detection system and can be blocked or the device quarantined. In addition, Cyber adAPT can provide a secure PIM client, by Virtual Solution's SecurePIM. Skwiid Mobile also provides application whitelisting, as well as SWG functionality.

Data Security

Cyber adAPT can provide Adaptive DLP capabilities (context/content-aware DLP with Adaptive Redaction that can remove visible and invisible content within documents) provided by RAUG Security's Clearswift DLP. The skwiid Mobile VPN can also be rerouted to any solution if customer investments have already been made in DLP. Also, Cyber adAPT can integrate with a number of EFSS solutions, including Salesforce, Box and Dropbox. The built-in firewall can allow/deny access to network storage resources. Secure connections to public services can be enabled, forcing all Office365 traffic through the VPN and built-in threat detection, for example.

Authentication and Access Protocols

The Cyber adAPT skwiid 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.

Attack Prevention and Mitigation

Cyber adAPT's skwiid Mobile solution includes an integrated behavior-based mobile threat detection system. Because skwiid enforces a VPN, all traffic is analyzed in real time for data and process behavior aspects that indicate attacks, for example an MITM attack. In addition, the skwiid mobile firewall can also block IP addresses and domains based on reputation.

Hardened VPN

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

Multiuser Device and Kiosk Mode

Cyber adAPT's offering provides 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, which is built into the skwiid platform. Skwiid Mobile is a fully integrated component of the platform and can pass real-time syslogs of all IP traffic for full inspection and real-time monitoring to any auditing party. Syslog can also be tailored to specific information .

Scalability and Portability

Skwiid Mobile can be delivered on-premises or as a cloud solution and can integrate with an existing EMM suite or provide its own device management. Skwiid 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. On-premises high-availability using multiple gateways can be configured, as well as multiple network connections providing failover and/or automated roaming for private networks. Cloud deployments provide automated and transparent failover. A connection option enables roaming users to connect to the closest available gateway.

GSMK

Headquartered in Berlin, Germany, GSMK 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, because it has been designed as a corporate-owned solution. GSMK also 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. GSMK's 600 series adds secure boot protection, Trusted Platform Module (TPM) support and tamper protection.

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 International Mobile Subscriber Identity (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

The GSMK CryptoPhone offers MFA; certification controls. including the detection of moving certificates to an unauthorized device; user authentication required for enrollment; and a trusted restoration. CAC, fingerprints, separate passphrases and BSI security chip card are also supported.

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

Headquartered in Armonk, New York, IBM offers MaaS360, a software EMM platform that is only available in the cloud, but offers an on-premises access gateway for email and applications. IBM's EMM strategy has evolved from being security-centric to being focused on user productivity as well. A big part of IBM's strategy is to take advantage of the broader IBM software and service functions, and establish a "better together" offering of MaaS360 with adjacent IBM products in areas such as mobile threat detection, CASB and IAM. One of the most significant MaaS360 releases during the past year provided cognitive insights — a capability that combines Watson analytics with customer EMM data to help customers understand their mobile environment and make decisions. IBM appears in the 2017 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: MaaS360

Certifications and Awards

MaaS360 provides FIPS 140-2 Level 1 cryptography in software for Android and Windows Phone 10, based on open-source OpenSSL. IBM uses Apple's FIPS 140-2-embedded cryptography in iOS and macOS 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 unsupported 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.

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 Microsoft rights management 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, MFA and full IAM product lines including a cloud identity service are available from IBM as separate products and configurations that will integrate with MaaS360. In addition, the MaaS360 proprietary browser uses a workplace technology specific VPN that can be configured to require the user to have a certificate and AD credentials before being allowed access to the corporate resources. In the case of email, an email access gateway solution can be implemented to ensure that only trusted and secure endpoints and users are accessing email servers. MaaS360 can employ 2FA for enrollment, administrator access and access to the container. MaaS360 includes in the packaging a full cloud Identity solution, which provides single sign-on (SSO), conditional access to mobile, native and cloud based apps. This identity solution can integrate with NAC solutions and intrusion detection and prevention (IDP) systems (Ping, Okta, Azure, etc.) for federated authentication requests, or it can be used as a stand-alone IDP to provide these capabilities. This cloud identity solution can integrate with IBM Verify to provide MFA using biometrics and other forms of identity.

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. In 2017, IBM added MaaS360 Advisor, a cognitive engine that may assist some administrators in identifying and predicting threats.

Hardened VPN

MaaS360 uses platform-embedded VPN software and a secure browser with integrated health checks, and has supported relationships with mainstream VPN and NAC 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 it 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, physical location 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.

Kaymera Technologies

Based in Herzliya, Israel, Kaymera Technologies 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 FIPS-certified cryptography and Common Criteria-certified app dev. Kaymera can also run secure apps in the Snapdragon TrustZone, which is certified to FIPS 140-2 Level 1. Kaymera's cryptographic components have been certified by the Israeli Ministry of Defense, as well as other governments. High-assurance algorithms are used for key exchange, Voice over Internet Protocol (VoIP) and secure messaging.

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 activities to AirWatch and MobileIron. Over-the-air updates are supported. Kaymera keeps current with Android OS updates to ensure 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 that must be flashed over the firmware of an off-the-shelf device for installation. At this time, Kaymera 360° supports several Android models, but not Samsung devices. Devices so configured will be kept up to date on Android releases through Kaymera Unlike many high-security vendors, Kaymera wants users to have as normal and native experience as possible. A future option that will provide secure stand-alone applications for iOS has not appeared. 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 in 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. Kaymera now also offers a mobile threat defense (MTD) system that's unique in its solution by using gamification as a means to engage the end user. Gartner feels that this has the potential to interest users in mobile security that were previously unaware of the risks of mobility.

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 Panic 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 during a predetermined time frame.

Authentication and Access Protocols

Kaymera can use a certification authority to issue device certificates during the provisioning process. VPN authentication uses TLS certificates. Kaymera supports CAC, multifactor and other typical high-security authentication methods. The Kaymera system provides a built-in MFA framework using the secured device as "something you have" to generate restricted OTPs per demand or use built-in biometric readers as a mean for an additional factor of authentication. That MFA mechanism can be used to limit and control access into various resources at the corporate level. In addition, all system portals and management consoles are protected using this 2FA mechanism by default and are compatible with OTP and 2FA mechanisms, including third-party software authenticators (Google), SSO and IAM (Octa) and 2FA hardware vendors (RSA, Vasco).

Attack Prevention and Mitigation

The Kaymera system includes multiple layers of protection to prevent it from being compromised. The core security system is embedded in the Kaymera secure OS. The Kaymera OS protects, prevents and detects attempts in multiple attack scenarios (both in an online and offline network status).

Kaymera constantly monitors risk and posture levels and reports to the IT team and/or a security information and event management (SIEM) system. User interaction provides IT with a means to monitor behavior. On the network side, Kaymera analyzes the device traffic with an IDS system to detect malicious activities, and provide information both to the IT team and SIEMs to perform mitigation when needed. IT administration can see each indication of compromise (IoC) detail origin and time stamp it for further risk analysis.

If an attack is detected, for example, if files have been modified, then Kaymera will alert the user that an attack is taking place. In the event of a compromise that cannot be prevented or reversed, the boot loader is destroyed, so the device is no longer capable of starting, and all 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 OpenVPN/OpenSSL 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

The Kaymera secured device supports a multiuser environment. Each device has a backup, reset and restore built-in functionality that enables one user to securely back up personal device data, reset and wipe the device into initial settings, and then hand it over to the next user to restore the device from the secured backup infrastructure.

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.

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 with 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 do-it-yourself self-service.

MobileIron

Based in Mountain View, California, MobileIron offers a Platinum bundle that 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 2017 "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. It is also noted that the company's references represent some extremely high-security customers.

Product: MobileIron Platinum bundle

Certifications and Awards

MobileIron provides FIPS 140-2 overall Level 1 cryptography in software for agents on Android and iOS platforms, based on open-source OpenSSL, supplemented with RSA BSAFE and RHEL OS certifications. MobileIron's Core and Sentry Servers also use FIPS 140-2 certified crypto. Local cryptography is not used, which reduces risk of API vulnerabilities. MobileIron is certified on the NSA Commercial Solutions for Classified (CSfC) Components List. It also has ECCN 5D992 export control classification. MobileIron was 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 received U.S. FedRAMP certification, and has been assigned a DISA STIG for MDM. MobileIron was awarded the three-year U.S. DISA contract for Mobile Device Management (MDM) and Mobile Application Store (MAS) and SOC 2 Type II for cloud service. It is the only vendor of record for the DISA MDM/MAS contract.

Secure Life Cycle Management

MobileIron provides consistent, cross-platform, device-level management of baseline and advanced security policies and certificates. 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. MobileIron developed its own in-house Product Security Incident Response Team (PSIRT).

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. Windows 10 support includes app execution, USB DLP controls, Bitlocker Management and patch/update enforcement.

App Security

MobileIron's AppConnect container provides a solid and extensive set of app management capabilities for Android and iOS. MobileIron partners with software-testing vendors to secure app development. Integration with third-party app security testing providers is offered. MobileIron recently released unmanaged device support for its bundled applications. Due to the newness of this functionality, Gartner has not verified the new feature.

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. AppConnect uses DLP design elements to set boundaries on data movement between apps and in and out of a mobile device. Support for Microsoft rights management 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. Additional controls are offered for workstation encryption and external media.

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, NIST-compliant derived credentials and third-party NAC vendors are supported. New Derived Credentials (PIV-D) support on Android and iOS may be used as an alternative to CAC. 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. MobileIron supports AD, 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. A full policy engine is available for conditional access, plus audit logs of all authentication requests.

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. MobileIron has formal proxy support for SWGs from Blue Coat, Check Point, F5, McAfee and Proofpoint.

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 and authorization 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 audit logs for input to several popular 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 targets customers in regulated and high-security industries.

Samsung Electronics

Headquartered in Suwon, South Korea, 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 called Knox, and is a Samsung exclusive platform, consisting of a hardened Android OS combined with the Tizen OS. It is implemented on supported Samsung devices. Samsung did not appear in the 2017 "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 U.S. 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. Knox is included as part of the U.S. DMCC-S access to select DoD voice and data networks. Samsung continues to broaden its range of security approvals, including the Netherlands "AIVD" and Kazakhstan "OTAN."

Secure Life Cycle Management

Samsung's CellWe EMM offers basic life cycle management and is part of the NIAP certification. Knox Mobile Enrollment and Knox Configure are separately licensed utilities that offer additional features. Knox Mobile Enrollment is supported by most EMM providers. Knox Configure provides comprehensive device configuration, typically for single-purpose uses. 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. Samsung SDS, its sister division, also offers its own separate mobility management solution, Samsung SDS EMM, which is more comprehensive and can manage iOS, Android and Windows devices.

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 OS's enterprise capabilities, as well as a reasonably native personal user experience, while maintaining above-average system security and integrity. Hardened platform and attack prevention capabilities are interrelated (see the Attack Prevention and Mitigation section below).

App Security

Knox Workspace is an enterprise-grade, encrypted container that operates in enterprise and government/defense modes. For consumers, a Knox container called Secure Folder is available, along with a secure backup and migration service called Samsung Cloud. 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. If an anomaly is detected, then it will automatically become inaccessible. The container can be managed by Samsung SDS EMM or by other EMM vendors that 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 MFA.

Attack Prevention and Mitigation

All Samsung devices offer Real Time Kernel Protection (RKP), which protects the kernel after boot. A Knox feature known as TrustZone-based Integrity Measurement Architecture (TIMA) works as a joint process between the device's hardware and the Knox software that uses periodic kernel measurement (PKM) to detect suspicious anomalies and periodically retest the kernel integrity. 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. RKP and PKM execute in an environment inaccessible to the kernel, so potential kernel exploitation cannot be extended to compromise these safeguards. This environment is hardware-protected and isolated from the Android OS.

Hardened VPN

Knox offers client SSL and IPsec VPN, which can be customized on a per-app, Knox container or device-wide basis. Samsung does not offer a gateway to terminate the VPN connections, but it supports all major VPN providers. The VPN cannot be bypassed by the user or as a result of a dropped VPN connection. Client activity can be monitored to provide detailed analysis of traffic patterns, app utilization, quality of service, etc. Multiple simultaneous tunnels may be used. VPN APIs provide information that can be used by third-party threat defense tools.

Multiuser Device and Kiosk Mode

Knox devices can be configured for multiuser and kiosk mode and can be managed by the Samsung SDS 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, RKP and PKM subsystems 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 and provides APIs for trusted data collection. Devices can be recovered even after being fully reset; however, an encrypted Knox container cannot be recovered.

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.

Sophos

Based in Oxford, England, Sophos offers Sophos Mobile (SM) for EMM, an SWG and a VPN, considered together in this research. It is one of only two vendors ranked in the "Magic Quadrant for Endpoint Protection Platforms" that also qualified for inclusion in the 2017 "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, as well as newly released support for EMM-manageable IoT devices.

Product: Sophos Mobile

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 Mobile provides a complete EMM solution for broad cross-platform, device-level management of security baseline policies across Android and iOS platforms, including network settings and peripherals and Windows 10, via the Windows MDM interface. Sophos cannot apply strong authentication when a device is enrolled, but subsequent updates are protected, especially from MITM attacks, by certificate pinning. Devices can be locked down immediately and isolated from the network, 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 all Android security APIs and those 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 SM. 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. Apps loaded from enterprise stores may be additionally checked by several third-party partner solutions. 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. Individual file and container protections are included, and are compatible across all supported platforms. 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 and external media (e.g., SD cards and USB flash drives), 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 endpoint 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 AD, 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/Firewall or Sophos Cloud Web Gateway. Separate mobile security apps are available to protect users from mobile malware and malicious websites. On Android devices, Sophos is a mainstream anti-malware market player.

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. In addition, Sophos now offers its own location-aware alarm and emergency notification solution, called Sophos Mobile Alert, which will integrate with SM.

Forensics

Sophos did not offer forensic capability at the time of the study, but can interoperate with mainstream forensics providers. Its risk analysis subsystem can generate compliance reports and feed data to SIEM systems.

Scalability and Portability

Although Sophos' solution scales to 50,000 devices, Sophos targets the small or midsize business (SMB) market. Larger customers must ensure that its functionality and product support levels meet their requirements. SM is available at relatively low subscription costs, even in small license quantities.

Thales Group

Headquartered in La Défense, France, 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. Citadel provides a secure group messaging app to replace products such as Whatsapp and Wechat. In addition, Thales provides TEO-XC, which is a custom Android device for organizations that need to comply with higher-security schemes. Thales does not appear in the 2017 "Magic Quadrant for Enterprise Mobility Management Suites."

Products: Teopad, Citadel, TEO-XC

Certifications and Awards

Thales Teopad is CSPN-certified from the French ANSSI. Additional steps are in progress for TEO-XC to receive ANSSI "standard qualification" and for Citadel to receive "elementary qualification." Previous plans for Common Criteria and FIPS are not being pursued at this time.

Secure Life Cycle Management

Teopad provides Teopad Management Center (TMC), which is its own MDM tool for Android and iOS. Teopad supports a large number of device, app and data security policies and rules. TEO-XC supports 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 provides TEO-XC, which is a hardened Android OS that can work on 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 information rights management (IRM) functionality. The container isolates professional data from the rest of the device. EFSS 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 MTD functionalities, nor does Thales Group partner with MTD vendors to offer these.

Hardened VPN

Teopad offers a TLS-based VPN, with a TLS gateway. The VPN is activated automatically when needed and cannot be deactivated or bypassed by the user.

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 forensic functionality.

Scalability and Portability

Thales Teopad works on both iOS and Android. It is slightly higher priced 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

Based in Germany, Virtual Solution offers a mobile security solution consisting of a software container called SecurePIM that includes email, contacts, calendar, note taking and MCM for iOS and Android. What distinguishes SecurePIM from other PIM clients is use of natural user interface (NUI) techniques and the ability to transparently enable Secure Multipurpose Internet Mail Exchange (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. Domino email is also supported.

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 jailbreak/rooting detection upon execution of the application.

Data Security

SecurePIM stores all data at rest under its own encryption. For S/MIME, it is transparently enabled. Containment extends to documents in email, with some capabilities for editing and secure image capture with a device camera.

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 jailbreak/rooting detection upon execution of the application. There is also some ability to detect MITM attacks against the email traffic.

Hardened VPN

SecurePIM provides a TLS connection to critical back-end systems. It does not offer device-level VPN technology, but can use a per-app VPN when the application is used together with an EMM or MDM and a VPN gateway. As of August 2017, a secure Gateway is available that creates a SecurePIM App tunnel without the need of a VPN based on TLS 1.2 with prepopulated public keys.

Multiuser Device and Kiosk Mode

SecurePIM does not offer kiosk or multiuser mode.

Geo/Time Tracking and Fencing

SecurePIM does not offer geo-fencing.

Forensics

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

Scalability and Portability

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

VMware

VMware is headquartered in Palo Alto, California. WMware's AirWatch product is one of the most functionally complete EMM offerings in the market. VMware has made substantial strides toward becoming a full-featured UEM, with significant advances in managing Windows 10 and macOS in a single console. In addition, VMware has invested in improving its product for high-security use cases during the past year. High-security functionality requires either the blue or yellow product bundles. AirWatch appears in the 2017 "Magic Quadrant for Enterprise Mobility Management Suites."

Product: AirWatch

Certifications and Awards

VMware uses OpenSSL in FIPS mode. No other/unsupported cryptographic modules are used. AirWatch is certified on the NSA Commercial Solutions for Classified (CSfC) Components List and has been assigned an updated DISA STIG for MDM VMware has also completed the NIAP MDM and Agent Extension v2.0. VMware is listed in the U.K. CESG End User Devices Security and Configuration Guidance.

Secure Life Cycle Management

AirWatch provides comprehensive cross-platform device management for iOS, Windows 10, and Android. The solution also includes its own certificate server and can integrate with leading certificate authorities.

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 Android.

App Security

AirWatch bundles a full suite of products, including a PIM client, browser and IM. The solution also includes AirWatch's 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 AIP, and prevents container leakage through print controls, saving, cut and pastes and so on. 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. Boxer supports reading and enforcing, as well as composing Microsoft Information Rights Management (IRM) and Azure Information Protection (AIP) secured emails. Rights management keys can be disseminated and revoked via email or by profile synchronization. Policies can be shared with several third-party DLP providers.

Authentication and Access Protocols

MFA and step-up 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 that need CAC cards are supported by means of delivery of derived credentials that can be automatically pushed to mobile devices. In addition to supporting AD and LDAP, Airwatch can integrate with Domino. VMware Identity Manager provides its on-premises and/or cloud-hosted IDP, as well as an on-premises NAC (NSX). The Workspace One bundle combines AW, VIM and NSX.

Attack Prevention and Mitigation

AirWatch can interoperate with several mobile malware detection and app reputation vendors, and can remediate based on discovery status. Its mobile security alliance contains partners for mobile and nonmobile threat defense. MITM attempts are detected and reported to the AW console.

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. The VPN provides function and policy parity across all major mobile and nonmobile OSs, including Windows 10 and OS X.

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, iOS, Windows 10 Phone, Windows 10 and Mac OS. 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 forensics, but it will directly integrate its log data into several third-party tools. The product can also detect tampering with its own agent.

Scalability and Portability

The AirWatch product has proven, large-scale global deployments. The console itself is one of the easiest to use, with embedded training videos, links and a wizardlike approach to help new administrators become productive quickly.

Context

Every organization has business processes that must operate at a high level of security. This research considers vendors for those cases in which 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 with 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 the complex bundling of several product lines.

Critical Capabilities Definition

Certifications and Awards

The most competitive vendors in this capability will have a broad set of accreditations and a history of pursuing certifications, making them agile choices in multiple countries, and they may be cited in preferred government and other industry-preferred buying programs.

In high security use cases, the use of open standards and on-device crypto are acceptable, but proprietary crypto at increased levels of strength and certification will count more strongly. Vendors are expected to meet or exceed FIPS 140-2 Level 1 as the default cryptography of their product set. High-security encryption must be enabled by default.

A vendor's standing 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, and evidence that certifications are refreshed periodically.

The certification process may be incremental and incomplete. Buyers should be careful to consider the roadmap commitments of candidate vendors. Warnings include:

- Relying on a hardware and/or OS platform that has been separately certified for some, but not all of its capabilities
- Relying on other app partners to provide certified cryptography
- Claiming to have robust, equivalent cryptography, but not having official documentation
- Relying on outdated crypto, such as SSL, which was replaced by TLS, or unsupported, end-of-life crypto, such as TrueCrypt

Secure Life Cycle Management

Vendors are expected to provide basic life cycle management features that emphasize high-security practices and maximize security values across supported platforms.

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 consistently on all of 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 recommendations for secure device settings and compatibility with third-party EMM vendors.

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. Various forms of mobile application management (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. 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 intrusion prevention system (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, generic open source, as well as mainstream VPN partners, is typical and not scored highly. Ownership of either or both dedicated mobile VPN clients and a VPN gateway improves the high-security evaluation, as does ownership of 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 that 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 well. Consideration is also given to 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. In this use case, scalability and portability may conflict with the importance of total platform control.

High-Security Commercial

High-security commercial usage contexts can include regulated, nongovernment industries, such as retail, 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 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. Users interconnect with common file shares to exchange information as sensitive as court case files.

Such files may be used selectively among different roles in a trial, such as defender, prosecutor, judge and detectives. 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 (e.g., devices used by different roles in a hospital).

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 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 can't 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 device use case that will sometimes have a role in a high-security mobile context — for example, emergency access to mission-critical business processes.

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

- CommuniTake

Dropped

- Microsoft is not specifically pursuing the high-security mobility market for small mobile devices.
- Pulse Secure is not specifically pursuing the high-security mobility market.
- Soti is not targeting high-security mobility buyers or markets.
- Silent Circle and Sikur do not provide their own solutions to meet the high-security management capability. The mobile management capability requirement is interpreted more strictly in the 2017 report.

Other Companies

- Google offers a series of enterprise features in Android, formerly labeled "Android for Work" (AfW). These features are used by some vendors in this research. Examples include a solution to securely provision and isolate company apps, data and VPN, and a suite of integrated PIM apps and blocking measures against copy/paste, screen capture and app-side loading.

Additional vendors active in the general space of high-security mobility (e.g., Dark Matter and SyncDog) were not profiled in this research; however, we can discuss them during Gartner client inquiries.

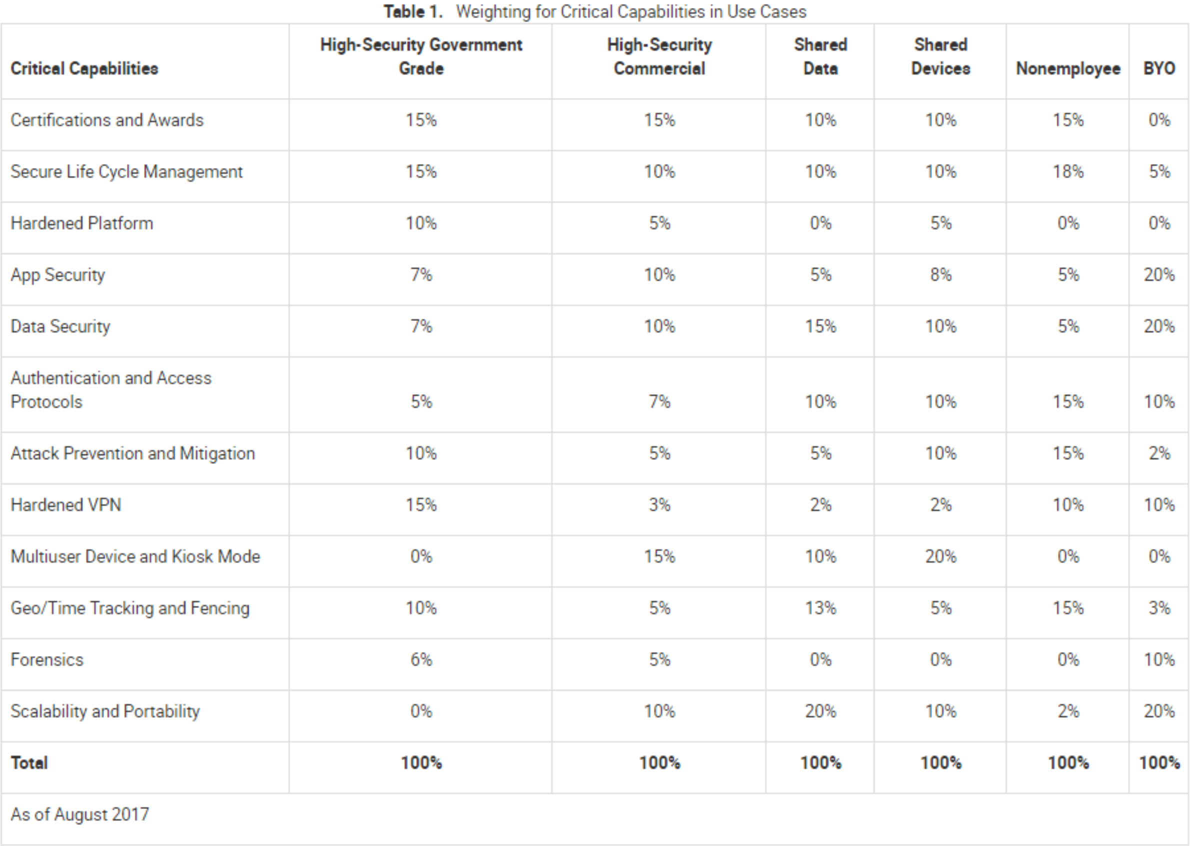
Inclusion Criteria

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 appeal specifically to high-security buyers. Inclusion criteria include:

- Owned, licensed or used embedded FIPS 140-2 certification or stronger, specialized certifications for all encryption operations of the product, provided full support for crypto maintenance and updates, and recertified regularly. High certification mode operation must be the default.
- 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. Compatibility with third-party EMM solutions is an additional benefit.
- 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 June 2017. Future products are not assessed.

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 2017						

Source: Gartner (August 2017)

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).

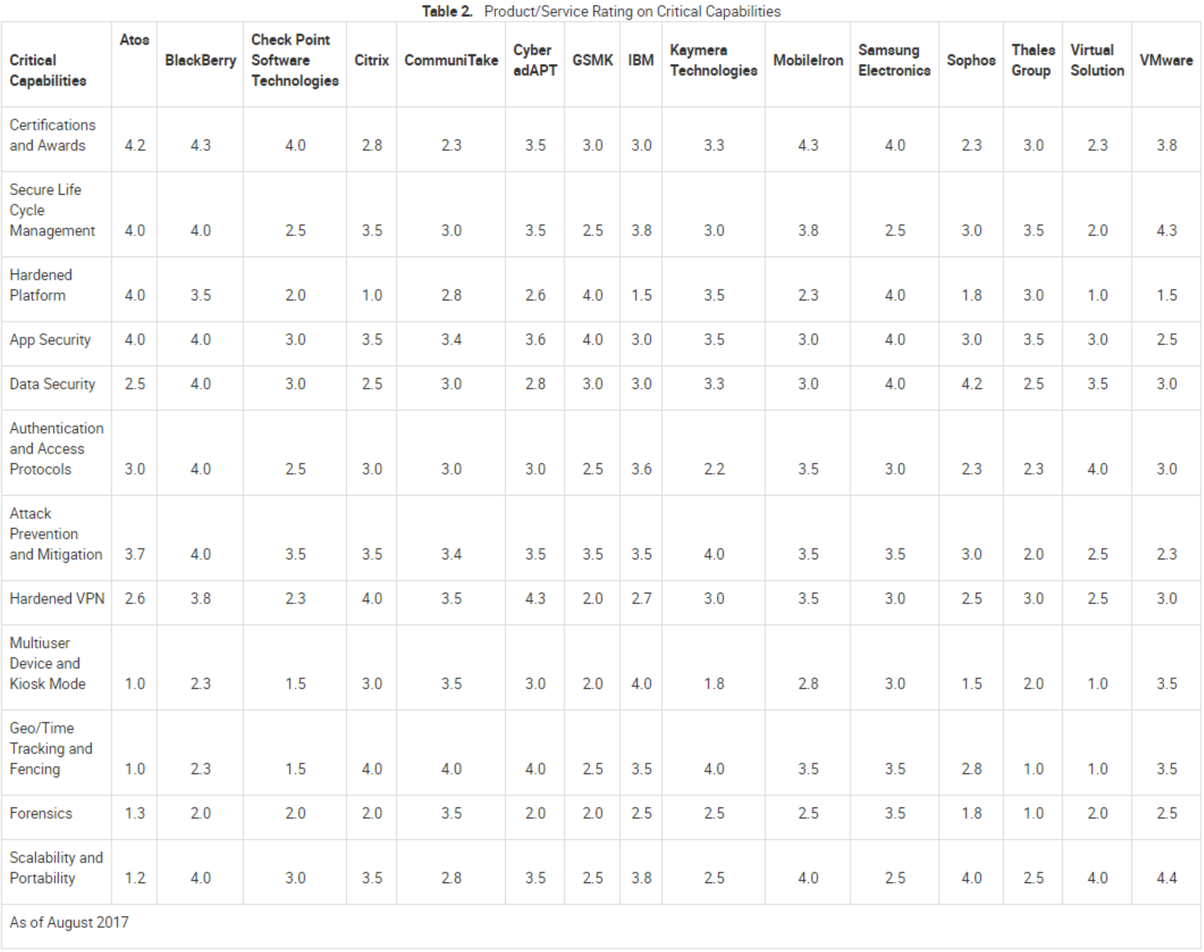


Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	**Atos**	**BlackBerry**	**Check Point Software Technologies**	**Citrix**	**CommuniTake**	**Cyber adAPT**	**GSMK**	**IBM**	**Kaymera Technologies**	**MobileIron**	**Samsung Electronics**	**Sophos**	**Thales Group**	**Virtual Solution**	**VMware**
Certifications and Awards	4.2	4.3	4.0	2.8	2.3	3.5	3.0	3.0	3.3	4.3	4.0	2.3	3.0	2.3	3.8
Secure Life Cycle Management	4.0	4.0	2.5	3.5	3.0	3.5	2.5	3.8	3.0	3.8	2.5	3.0	3.5	2.0	4.3
Hardened Platform	4.0	3.5	2.0	1.0	2.8	2.6	4.0	1.5	3.5	2.3	4.0	1.8	3.0	1.0	1.5
App Security	4.0	4.0	3.0	3.5	3.4	3.6	4.0	3.0	3.5	3.0	4.0	3.0	3.5	3.0	2.5
Data Security	2.5	4.0	3.0	2.5	3.0	2.8	3.0	3.0	3.3	3.0	4.0	4.2	2.5	3.5	3.0
Authentication and Access Protocols	3.0	4.0	2.5	3.0	3.0	3.0	2.5	3.6	2.2	3.5	3.0	2.3	2.3	4.0	3.0
Attack Prevention and Mitigation	3.7	4.0	3.5	3.5	3.4	3.5	3.5	3.5	4.0	3.5	3.5	3.0	2.0	2.5	2.3
Hardened VPN	2.6	3.8	2.3	4.0	3.5	4.3	2.0	2.7	3.0	3.5	3.0	2.5	3.0	2.5	3.0
Multiuser Device and Kiosk Mode	1.0	2.3	1.5	3.0	3.5	3.0	2.0	4.0	1.8	2.8	3.0	1.5	2.0	1.0	3.5
Geo/Time Tracking and Fencing	1.0	2.3	1.5	4.0	4.0	4.0	2.5	3.5	4.0	3.5	3.5	2.8	1.0	1.0	3.5
Forensics	1.3	2.0	2.0	2.0	3.5	2.0	2.0	2.5	2.5	2.5	3.5	1.8	1.0	2.0	2.5
Scalability and Portability	1.2	4.0	3.0	3.5	2.8	3.5	2.5	3.8	2.5	4.0	2.5	4.0	2.5	4.0	4.4
As of August 2017															

Source: Gartner (August 2017)

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.

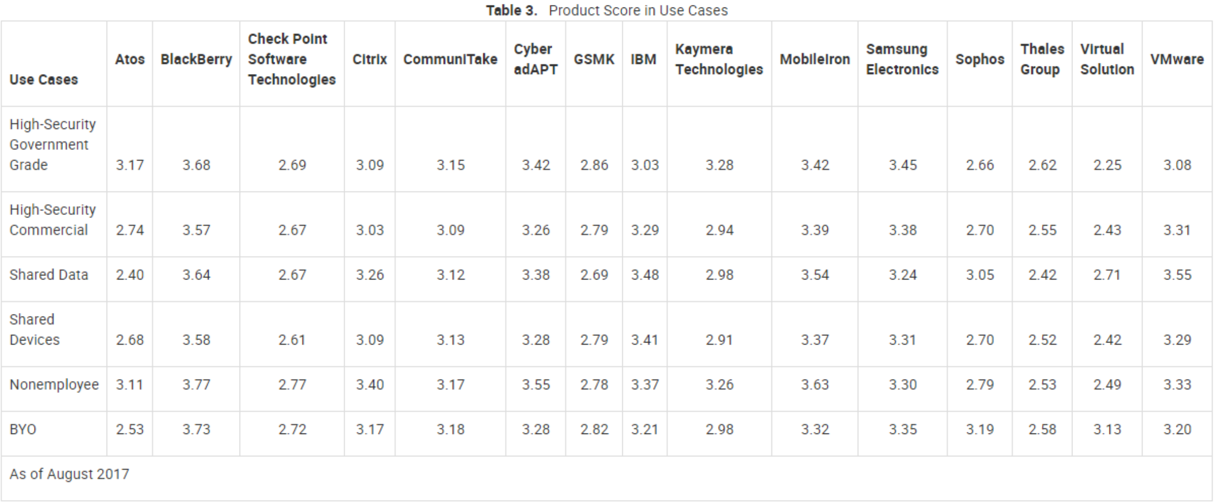


Table 3. Product Score in Use Cases

Use Cases	**Atos**	**BlackBerry**	**Check Point Software Technologies**	**Citrix**	**CommuniTake**	**Cyber adAPT**	**GSMK**	**IBM**	**Kaymera Technologies**	**MobileIron**	**Samsung Electronics**	**Sophos**	**Thales Group**	**Virtual Solution**	**VMware**
High-Security Government Grade	3.17	3.68	2.69	3.09	3.15	3.42	2.86	3.03	3.28	3.42	3.45	2.66	2.62	2.25	3.08
High-Security Commercial	2.74	3.57	2.67	3.03	3.09	3.26	2.79	3.29	2.94	3.39	3.38	2.70	2.55	2.43	3.31
Shared Data	2.40	3.64	2.67	3.26	3.12	3.38	2.69	3.48	2.98	3.54	3.24	3.05	2.42	2.71	3.55
Shared Devices	2.68	3.58	2.61	3.09	3.13	3.28	2.79	3.41	2.91	3.37	3.31	2.70	2.52	2.42	3.29
Nonemployee	3.11	3.77	2.77	3.40	3.17	3.55	2.78	3.37	3.26	3.63	3.30	2.79	2.53	2.49	3.33
BYO	2.53	3.73	2.72	3.17	3.18	3.28	2.82	3.21	2.98	3.32	3.35	3.19	2.58	3.13	3.20
As of August 2017															

Source: Gartner (August 2017)

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.

Evidence

Click here to view a white paper describing the name change for Android for Work .

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.