SECURE YOUR MOBILE WORLD

MOTOROLA SOLUTIONS

THE RISE AND RISK OF COMMERCIAL SMARTPHONES

In the Bring Your Own Device (BYOD) environment your workforce uses their own commercial smartphones and tablets for work related activities, and BYOD is a growing phenomenon. According to a survey of over 4,900 IT decision makers across 18 industries around the globe, “89% of IT departments enable BYOD in some form.[1]” This trend leaves your IT administrators without the necessary security controls that could ultimately put your sensitive information at risk to cyber attacks and data leaks. Over 60% of network breaches are due to a lost or stolen device.[2] And in the United States someone loses a cell phone every 3.5 seconds.[3]

86% INDICATED FIRST RESPONDERS USE THEIR OWN CONSUMER-GRADE DEVICES FOR WORK-RELATED ACTIVITIES[4]

75% OF FEDERAL IT PROFESSIONALS WITH RESPONSIBILITY FOR MOBILE SECURITY SAY THEIR ADOPTION OF MOBILE DEVICES HAS INCREASED THEIR SECURITY RISKS[5]

TOP CONCERNS FOR ALLOWING BYOD[6]

65%	55%	50%
Mobile Device Security	Mobile Data Security	Mobile Application Security

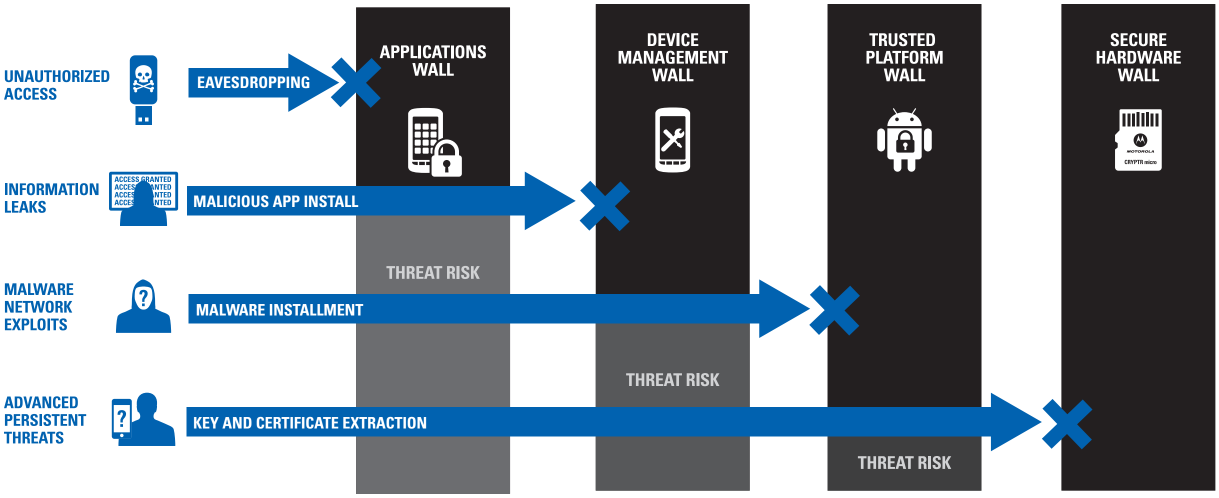
Commercially available smartphones are susceptible to various attacks which can ultimately jeopardize your mission critical operations. Consumer-grade smartphones are designed and built for everyone. Something that is designed and built for everyone is built for no one. Additionally, according to a recent survey of IT decision makers some of the top concerns with allowing commercial smartphones in the workplace are concerns about mobile device security, mobile data security, and mobile application security.

An unavoidable consequence of the explosive expansion of commercial devices within your organization is the proportional elevation in vulnerability to security breaches and data leaks. In order to protect your information from increased exposure to attacks and data loss through either accidental or malicious means, you need a comprehensive security solution, but one that does not sacrifice productivity in terms of group collaboration or mission critical features. **Our end-to-end security solution is purpose-built to deliver optimal protection of your mission critical environments, ensuring your sensitive information is safeguarded from adversaries.**

THREAT	TREND
Lost or Stolen Device	Millions of smartphones are lost or stolen every year. Approximately 22% of all smartphones produced will be lost or stolen during their lifetime and over 50% of these will never be recovered.[7]
Mobile Malware	Mobile Malware attacks have nearly doubled to 8.19 billion with Android ecosystem being the prime target, putting a large percent of smartphones at risk.[8]
Rogue Device	A malicious adversary using a rouge device can perform illegitimate actions including, (a) listening to private communications (b) modifying, deleting, or replaying messages and (c) spoofing and behaving as a repeater relaying signaling and user data between two communicating parties.
Advanced Persistent Threats (APT)	APT are attacks where an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.

INTRODUCING THE LEX L10
YOUR SECURE MOBILE DEVICE PLATFORM

The LEX L10 redefines the broadband experience for your mobile users. This purpose-built handheld combines loud and clear audio, exceptional durability, and provides the high-assurance security features that safeguard your mission critical communications. The LEX L10 Secure Mobile Platform utilizes a defense-in-depth approach to security. It combines multiple layers of advanced defensive walls that stop adversaries from accessing your mission critical voice and data communications. The LEX L10 Secure Mobile Platform provides your personnel with the confidence that they can communicate, collaborate and share, within a secured environment.



A defense in depth approach to security insulates your most vulnerable assets and ensures protection from the kernel to the application layer.

APPLICATION WALL
PROTECTION FROM EAVESDROPPING

Encryption built in the application layer is a good first-step at protecting your sensitive information. For added security, the LEX L10 includes a single sign-on client that provides multi-factor authentication across your mission critical applications. In order to ensure data-in-transit protection the application wall utilize the Mobile Virtual Private Network (MVPN). The MVPN establishes a secure connection between the LEX L10 and your enterprise network significantly reducing the threat of eavesdropping. Built off of IPsec and MOBIKE open standards, the MVPN ensures a continuous connection for your applications while users move across the network, ultimately saving time and increasing your users efficiency.

DEVICE MANAGEMENT WALL
REMOTE MANAGEMENT AND CONTROL

This wall provides support for device management based on industry standards. In this wall, you are in complete control over the LEX L10 with over-the-air monitoring and control capability including: remote configuration, remote firmware and software upgrades, application whitelisting and over-the-air wipe and lock capability.

The LEX L10 supports 4G LTE (Bands 3, 4, 5, 7, 8, 20, 26, 28), 3G UTMS (Bands 1, 2, 4, 5, 8) and Quad Band GSM (850 MHz, 900 MHz, 1800 MHz, and 1900 MHz)

TRUSTED PLATFORM WALL
PREVENT AND DETECT MALWARE INSTALL

The Trusted Platform Wall offers multiple layers of protection in order to protect and to provide an assured platform.

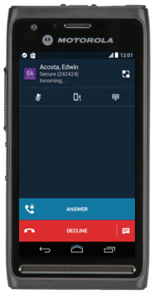
- **Secure Boot:** During the power up process the secure boot ensures there is no unauthorized malicious code operating on the LEX L10.
- **Secure Enhanced Android:** The LEX L10 comes with a preconfigured security policy that blocks malicious applications from accessing the LEX L10's resources for example; camera, microphone, and contacts.
- **Data-At-Rest Protection:** All data residing on the LEX L10 is encrypted via AES 256 encryption.
- **Malware Blocker:** The malware blocker inhibits malware from manipulating the LEX L10 operating system and gaining control of the device while automatically blocking any attempts to root the device.
- **Integrity Monitoring (IM):** IM continuously monitors for any unauthorized changes to the LEX L10's operating system files. If a threat is detected IM automatically posts an alert.

SECURE HARDWARE WALL
TAMPER PROTECTION OF CERTIFICATES AND KEYS

Software based applications typically have lower levels of encryption protection which may be more vulnerable to more sophisticated attacks. To address this vulnerability the LEX L10 includes a FIPS-140-2 Level 3 validated CRYPTR micro HSM. The CRYPTR micro is a microSD card that provides tamper evident protection of encryption keys and authentication certificates while performing cryptographic services like AES 256 encryption. The CRYPTR micro provides the highest levels of assurance without sacrificing the size, weight, or power of the device.

SECURE APPLICATION ECOSYSTEM
COMMUNICATE WITH CONFIDENCE

Secure your in-field mobile productivity and collaboration with a secure application ecosystem. Via an integrated easy to use user interface, your personnel will have access to all of their secure communication services that are available across telephony, messaging, and Push-to-Talk (PTT) communications. Applications leverage the FIPS 140-2 Level 3 CRYPTR micro HSM enabling you and your personnel to communicate securely in real-time.

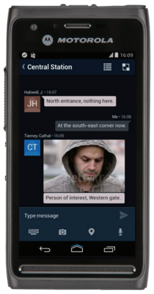


PSX SECURE CALLING
COMMUNICATE WITH CONFIDENCE

PSX Secure Calling provides secure, encrypted and completely private voice communications. With a centrally managed common address book users can quickly and easily initiate an encrypted secure one-to-one call. PSX Secure Calling leverages the LEX L10's FIPS 140-2 Level 3 validated CRYPTR micro stored within the secure hardware wall and provides AES-256 end-to-end encryption.

WAVE WORKGROUP COMMUNICATIONS
EVERY TEAM SECURELY CONNECTED LIKE NEVER BEFORE

WAVE provides a communication interoperability platform for PTT between all of your devices and networks. WAVE leverages the FIPS 140-2 Level 3 validated CRYPTR micro HSM providing AES-256 end-to-end PTT encryption between LMR and LTE devices. WAVE ensures your communications stay private and secure, keeping your workforce more coordinated enabling smarter decisions and providing safer outcomes.



North entrance, nothing here.

At the south-east corner now.

Person of interest, Western gate.

PSX SECURE MESSAGING
WHEN VOICE IS NOT AN OPTION RELY ON SECURE MESSAGING

PSX Secure Messaging provides secure, encrypted and completely private one-to-one and group text messaging. The application leverages the integrated user-interface and common address book ensuring ease of use for your personnel.

IDENTITY MANAGEMENT
A SEAMLESS SECURE USER EXPERIENCE STARTS WITH IDENTITY

Identity Management provides your personnel with a unified single sign-on and authentication experience across all your applications. This significantly reduces the need to remember multiple usernames and passwords. Reduce the complexity of managing identities and increase your security posture by centrally managing password policies like structure, length, special characters, and change frequency across all applications within your ecosystem. Give your personnel simple and secure access to the applications they need with identity management.

Our suite of mobile applications leverage the power of the LEX L10 Secure Mobile Platform. By using the secure hardware wall applications benefit from tamper evident protection of encryption keys and digital certificates and are safeguarded with cryptographic services for true end-to-end encryption.

STAY AHEAD OF THREATS WITH ONGOING SECURITY MANAGEMENT

Maintaining security in a constantly changing environment is a complex endeavor. The growing threat of internal and external attacks demand a new approach to managing security. Your ability to retain and ensure high assurance security across your devices, applications, and networks will depend on your ability to effectively manage it.

Our secure management ecosystem helps you effectively manage and maintain security across your entire operation. With greater visibility and more control you can remediate vulnerabilities faster, minimize risk, and stay ahead of cyber attacks.

UNIFIED PROVISIONING MANAGEMENT

CENTRALIZED AND SECURE PROVISIONING OF USERS

The Unified Provisioning Manager (UPM) provides you with a comprehensive platform for provisioning users with LTE, PTT, VoIP, and messaging services. Easily provision users across all of the services and applications they will need while in the field via an intuitive web-based portal. The entire provisioning process is completed from a single centralized location versus having to do it across every individual application server. The UPM enables the provisioning of users to be more efficient and user-friendly meaning administrators are less prone to error resulting in quick, easy, and secure provisioning.

MOBILE DEVICE MANAGEMENT

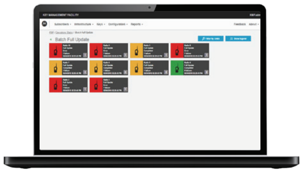
CONFIGURE, MANAGE, AND SECURE YOUR MOBILE DEVICES

Mobile Device Management (MDM) allows you to securely manage and monitor all of your mobile devices across your operations. Providing greater visibility and the necessary control mechanisms you need to securely deploy, manage, and terminate devices. We provide the flexibility to choose among industry leading MDM vendors to ensure convenience and seamless integration with your operations.

CERTIFICATE MANAGEMENT SOLUTION

SECURELY PROTECT AND MANAGE YOUR DIGITAL CERTIFICATES

Without a secure authentication mechanism your security environment is incomplete and susceptible to threats like unauthorized access and man-in-the-middle attacks. Strong authentication relies on the use of Public Key Infrastructure (PKI). PKI inherently adds complexity especially if mutual authentication is utilized. The Certificate Management Solution (CMS) provides you with the products and processes to manage the complete certificate life-cycle. Via the CMS web base portal you can monitor and manage all of your deployed certificates including defining the PKI hierarchy, issue certificates, and revoke certificates in case of a compromise device.

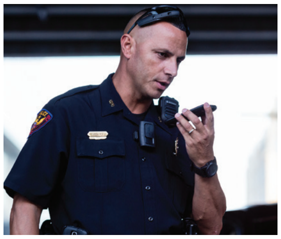


KEY MANAGEMENT FACILITY

SECURE, SCALABLE, AND PROVEN KEY MANAGEMENT SOLUTION

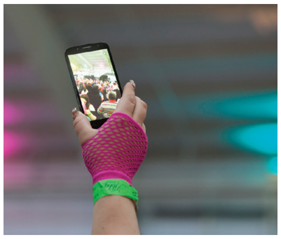
Managing encryption keys throughout your organization is a complex and time consuming process. The KMF removes the inherent complexity out of administrating and managing encryption keys across all of your secure devices. The KMF keeps your voice and data communications secure with encryption keys that update over-the-air without the delays, inconvenience or administrative costs of having users bring their devices into the shop for manual rekeying. With the KMF you can easily and quickly manage encrypted interoperable communications from a single centralized platform. Perform over-the-air rekeying (OTAR) across P25 two-way radios and the LEX L10 with CRYPTR micro, enabling secure cross platform group communications.

LEX L10 SECURE MOBILE PLATFORM PROVIDES HIGH ASSURANCE SECURITY DURING THE FOLLOWING SCENARIOS



ENABLE SECURE INTEROPERABLE GROUP COMMUNICATIONS

Project 25 (P25) systems utilize voice encryption in order to protect sensitive talk-group communications. As agencies begin to deploy LTE enabled devices with interoperable PTT clients, agencies will need to be able to ensure that the same level of security is in place across both P25 systems and LTE networks. They will need true cross platform end-to-end encryption. In this scenario, a police commander with a LEX L10 equipped with a CRYPTR micro HSM and WAVE PTT client can participate in end-to-end encrypted talk-group conversations with the rest of his team who use P25 radios. He can rest assured knowing that the audio can not be picked up by malicious actors because his audio is protected with true end-to-end encryption that spans across the P25 radio to the LEX L10. Good security practices recommend to periodically rotate encryption keys. The security IT administrator can centrally manage all of the encryption keys across both P25 and LTE devices. With a single gesture a new key can be sent to all members of a secure group via OTAR.



LOST OR STOLEN DEVICE

If your personnel should lose their LEX L10, either accidentally or maliciously stolen, you can rest assured that you have multiple device management mechanisms to ensure sensitive information is safeguarded in the device. Using the MDM, you can remotely lock the LEX L10 which renders the original PIN code useless. Additionally you can use the remote wipe functionality to remove any and all sensitive data from the LEX L10 including: pictures, videos, contact information, notes, and all post-loaded applications and their configurations. In order to preserve your secure interoperable group communications, you use the KMF to over-the-air erase the encryption keys in order to prevent any unauthorized misuse. Additionally use the CMS to revoke the digital certificates. If the LEX L10 is powered off or is unable to accept the remote commands you can rest assured that the CRYPTR micro HSM provides the tamper proof protection of the digital certificates and encryption keys ensuring adversaries can not physically access this confidential information.

COMPROMISED DEVICE VIA MALWARE

In this example, one of your personnel accidentally downloaded a malicious software onto their consumer-grade smartphone. The malware penetrates the device's security and embeds itself within the operating system. The malware can now hide within the device and redirect audio before it gets encrypted. It can also access your confidential contact information or remotely operate the camera or microphone. If the user was equipped with the LEX L10 Secure Mobile Platform malware would be stopped at the Trusted Platform Wall. The trusted platform wall ensures that malware does not take over your operating system.

SECURE COMMUNICATION HERITAGE
OVER 40 YEARS OF EXPERIENCE IN ENCRYPTED GOVERNMENT COMMUNICATIONS

Why look to Motorola Solutions? It starts with the industry-leading techniques we pioneered to provide end-to-end encryption in the P25 environment for millions of mission-critical users around the world. We have a history of firsts and have introduced various solutions that ensure the confidentiality, availability and integrity of mission critical communications. We've served the state, local and federal governments for 80 years strong with innovative technology, proven platforms and complete solutions. What's more, for 40 years our team has worked closely with military, intelligence, federal law enforcement and public safety communities to deliver secure interoperable communications.

1973	Development of Digital Voice Protection (DVP) encryption
1976	**INTRODUCES DIGITAL VOICE PROTECTION (DVP) PRODUCTS TO THE MARKET**
1977	Encrypted two-way mobile and portable radio products sold into Europe
1979	**INTRODUCES DATA ENCRYPTION STANDARD (DES) FOR LAND MOBILE RADIO NETWORKS**
1987	Introduces DES-XL, DVP-XL and DVI-XL encryption
1989	**INTRODUCES ASTRO™ DIGITAL ENCRYPTION**
1989	Introduces NSA Type 1 FASCINATOR
1989	Introduces Advanced SECURENET™
1996	**GRANTED FIPS 140-1 CERTIFICATE #2 FROM NIST**
1999	Ships Over-the-Air Rekeying (OTAR) on Digital APCO P25 system
1999	**INTRODUCES UNIVERSAL CRYPTO MODULE (UCM) SOFTWARE-DRIVEN ENCRYPTION DEVICE**
2000	**APCO PROJECT 25 COMPLIANT NSA TYPE 1 ENCRYPTION CERTIFICATION**
2002	Introduces AES encryption in ASTRO products (FIPS-197 certificate #2)
2002	**INTRODUCES THE FIRST HARDWARE ROOT OF TRUST IN COMMERCIAL CELLULAR DEVICES**
2003	Developed First TETRA Class 3 Air interface encryption
2004	First TETRA end-to-end encryption and Over-the-Air Rekeying products
2005	Introduces "Tactical OTAR"
2009	**GRANTED FIRST FIPS-140-2 LEVEL 3 CERTIFICATE IN LMR (#1181)**
2012	**DEVELOPED THE CRYPTR MICRO HSM: FIRST MICRO-SD ENCRYPTION MODULE CERTIFIED TO FIPS 140-2 LEVEL 3 BY NIST**
2012	Introduces the Assured Mobile Environment secure mobility solution
2013	CRYPTR 2 certified by NSA for classified use
2015	**INTRODUCES THE LEX L10 WITH CRYPTR MICRO FIPS 140-2 LEVEL 3**

SECURE YOUR MOBILE WORLD WITH MOTOROLA SOLUTIONS

At Motorola Solutions, we understand the challenges you face to balance the desire of your personnel to use consumer-grade smartphones in the workplace with the need for protecting your sensitive information. For decades, we have seamlessly and securely connected people, assets and information to help government agencies and the military achieve secure mobility.

Teaming up with customer and partners, drawing on our mission-critical expertise and game-changing technologies, we are bringing smarter security across our devices, applications and networks. Our solutions assures information is always available and always secure to support critical decisions, the moment you need them

SOURCES

1. Cisco IBSG "BYOD and Virtualization Horizons Study" January 2012
2. Ponemon Institute, "The Cost of Insecure Mobile Devices in the Workplace" March 2014
3. Loutout Study Projects "Lost and Stolen Phones Report" 2012
4. Motorola Solutions "Public Safety Data Communication Technology Survey", February 2012
5. Dimensional Research, "The Impact of Mobile Devices on Information Security: A survey of IT professionals" June 2013
6. EY "Insights on Governance Risk and Compliance Report" September 2013
7. EY "BYOD Security and Risk Considerations for Your Mobile Device Program" September 2011
8. Source 2015 Annual Threat Report Dell Security

For more information, contact your Motorola representative
or visit www.motorolasolutions.com/publicsafetylte

Motorola Solutions, Inc. 1301 East Algonquin Road Schaumburg, Illinois 60196, U.S.A. 800-323-3982 **motorolasolutions.com**

MOTOROLA SOLUTIONS