

# THE MOBILE HELIX® DATA SECURITY PLATFORM

A MOBILE HELIX WHITEPAPER

---

# THE MOBILE HELIX DATA SECURITY PLATFORM

## Introduction

Enterprise mobility creates a tremendous opportunity to deliver access to resources and applications that drive top-line and bottom-line results. These benefits do not come without risks, however. Foremost amongst those risks is the challenge in securing corporate data in a mobile world.

This challenge is composed of several distinct parts:

- Mobile devices operate on a public network, and that network is inherently untrustworthy. Any data security solution over-the-air must account not only for standard network conditions, but also creative attempts to compromise the network via technical and social attacks.
- Mobile devices are lost and stolen at a far higher pace than corporate laptops. In addition, mobile devices are often owned by the employee and shared amongst family members and friends.
- Mobile devices blend personal functionality and corporate functionality in a way that IT cannot control. Mobile Device Management solutions may be suitable for wiping and locking a device yet fail to ensure Data-Loss Prevention (DLP).

The Mobile Helix Data Security platform offers a compelling solution to these challenges and a compelling alternative to device management solutions. By focusing on protecting corporate data and creating an impermeable encryption barrier surrounding that data, both at rest and in transit, the Mobile Helix Data Security Platform protects corporate data regardless of the device operating system or device state (e.g., rooted/jailbroken, protected with a device management policy or not, etc.). In addition, the Mobile Helix Data Security Platform offers a level of policy flexibility that enables corporate IT to determine what data is available on a device based on the source of that data and the role of the device user. Finally, by routing all communication to and from the device through the corporate intranet infrastructure, existing DLP solutions are naturally integrated into the Mobile Helix solution ensuring that IT's investments in DLP are not rendered ineffective in a mobile world.

This paper describes the Mobile Helix Data Security Platform in depth, starting with an introduction to the LINK system and the Mobile Helix technology architecture, followed by a deep dive into the technology underlying the Data Security Platform.

## Mobile Helix LINK System Overview

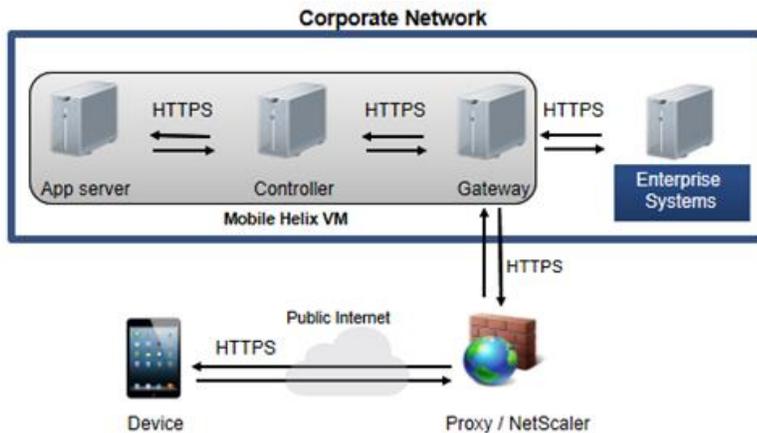


Figure 1: The Mobile Helix System Overview

### THE MOBILE HELIX LINK SYSTEM CONSISTS OF 4 COMPONENTS:

1. LINK Gateway
2. LINK Controller
3. LINK Application Server
4. LINK Secure Container App

### The Mobile Helix LINK system consists of four components:

**The LINK Gateway**, which is a reverse proxy that is the central entry point to the enterprise network. The Gateway controls and optimizes traffic between the external, public Internet and the private, corporate Intranet. A large-scale deployment will have many Gateways for redundancy and load balancing.

**The LINK Controller** is the system management console. The Controller manages all users, all devices, and all apps available on a mobile device via the LINK system. The Controller integrates with Active Directory (AD) or LDAP to import users and groups, and the Controller manages authentication via AD or LDAP. The Controller uses a role-based security and policy architecture to enable IT administrators to set flexible device, applications, and data policies from a central console. The Controller also monitors the LINK system and collects audit data and analytics in a central database.

**The LINK Application Server** hosts Mobile Helix's HTML5 apps. Each app is built using the LINK HTML5 SDK. Examples of LINK apps include LINK Filebox and LINK Email. Enterprises can host their own HTML5 apps, built with or without the LINK HTML5 SDK. Enterprises may also host legacy web applications available for mobile access using existing web server, application server, or portal infrastructure. The LINK Application Servers are firewall protected and integrate with standard HTTPS load balancers.

**The LINK Secure Container App** (also referred to as the "LINK App") runs on mobile devices and ensures secure access to corporate assets by encrypting data at rest and in motion. The LINK App includes browser technology supporting critical HTML5 features

including offline storage and video. In addition, the LINK App is enhanced with Apache Cordova (formerly PhoneGap) to enable browser access to device features that are not available across platforms via the HTML5 standard.

LINK is deployed fully on-premises.

## Mobile Helix Technology Architecture Overview



Figure 2: The Mobile Helix Technology Architecture

The Mobile Helix technology architecture shown above outlines how different technology platforms, implemented across the LINK system components described in the previous section, work together to enable the development and delivery of HTML5 apps, to protect corporate data, and to apply policies to the LINK system. The Mobile Helix technology architecture includes:

- **The LINK HTML5 SDK**, which is a fully standards-compliant HTML5 SDK for creating rich mobile apps that are intuitive, cross platform, and, when integrated with the LINK system, transparently secured.
- **The Mobile Helix Secure Delivery Platform**, which ensures end-to-end secure delivery of HTML5 mobile apps, enterprise web applications, and enterprise content and data.
- **The Mobile Helix Data Security Platform**, which ensures that data is uniformly protected at-rest on all supported devices and enables granular policy and role-based control of enterprise data stored on mobile devices.
- **The Mobile Helix Administration Platform**, which enables IT to manage and provision users and endpoints accessing the LINK system, track and audit data delivered to mobile devices, provision HTML5 mobile apps and enterprise web applications for mobile access, and monitor the LINK system.

## Mobile Helix Data Security Platform

### Introduction

The Mobile Helix Data Security Platform describes a series of integrated technologies across each component of the LINK system whose role is to protect corporate data and to implement secure policies governing that data. The Data Security Platform particularly focuses on the most real and present threats to sensitive corporate data that is available on a mobile device. We begin by describing those threats. In light of those threats, we then describe how data is secured over-the-air, how data is secured at rest, and how data policies govern the availability and lifetime of data:



Figure 3: The Mobile Helix Data Security Platform

### Threats to Corporate Data

Mobile Helix's Data Security Platform and key management protocols adhere to a handful of important principals based on the types of threats a corporation must defend against. There are four major threat categories accounted for in LINK's architecture:

- Data attacks over-the-air, which consist primarily of transparent proxies designed to fool an application into routing https traffic through a proxy that decrypts that traffic before forwarding it to the intended destination.
- Malware-born attacks against corporate data at-rest on the device. These attacks use social engineering, browser vulnerabilities, or other application vulnerabilities to inject rogue code into a device and steal data that is at-rest on that device. These attacks are increasingly sophisticated in their targeting, but they are limited by the fact that they must be automated. They may be launched directly

against the device or against a desktop computer with the intent to propagate to the device via iTunes or a USB connection to that device.

- Espionage via a lost or stolen device. In this case, a sophisticated attacker can devote an extended period of time to attack a device. During the initial period of attack, the device owner may not yet realize the device is lost or stolen. After a certain period of time, IT will have deleted the device and issued a remote wipe. The device must be kept offline by the attacker to avoid the wipe command.
- The final major category of threat is an insider attack. While an insider is still employed and in good standing this attack category is an independent threat. Once the rogue employee is identified as such, an insider attack is no different than an act of espionage targeting a stolen device.

To protect against these attacks, the Mobile Helix Data Security Platform adheres to a few essential principals, each of which is explored in further detail below:

- All data must be encrypted, in-transit and at-rest, and all encryption keys must be generated from strong credentials.
- All sessions must be authenticated with strong credentials, and IT must be able to implement secure session management policies.
- All communications must be verified, end-to-end, precluding the possibility of unauthorized proxy access along the way.
- IT must have the tools available to implement the principle of least privilege. Data should be available to mobile employees who have a legitimate business case for using that data on a mobile device, and it should only be available under the circumstances (online/offline, location) justified by that business case.
- All encryption technology is implemented independently of the underlying device platform, ensuring that attacks against the device OS runtime do not impact the Data Security Platform.

## Data Encryption

Fundamental to any data security strategy are the encryption algorithm and the associated key management architecture. Mobile Helix utilizes AES-256 encryption to protect all data at-rest, and TLS with 2048-bit RSA keys to protect all data in-transit. Once encrypted, data is protected using state-of-the-art algorithms that are infeasible to compromise. However, data protection is only as good as the associated key, and it is

Mobile Helix's key management architecture that ensures that sensitive corporate data is safe.

Mobile Helix generates all encryption keys from strong credentials. Strong credentials are very expensive to guess via an automated attack, and they are secrets that users are trained to protect from unauthorized disclosure. As discussed in the next section, IT already manages such a strong credential (a user's Active Directory or LDAP username and password), with the associated data security and education to protect that credential. Hence, by default, all Mobile Helix sessions are initiated with the user's corporate credentials.

Once a session is authenticated, Mobile Helix adds an additional layer of data protection and policy flexibility with the Data Security Platform's unique key hierarchy. The Data Security Platform uses four different types of keys to protect data during a session:

- The online-only key is generated from a 32 byte, secure, random string that is encrypted and stored in the Mobile Helix Controller. This key cannot be generated from any secret that an employee knows. The reason for this protection is to ensure that even insiders cannot compromise data marked "online-only" by policy once access to the corporate network is revoked.
- The offline persistent key is generated from a user's active directory credentials and, optionally, an additional PIN code credential. This offline persistent key is used to protect data that should be persistent online indefinitely (as defined by policy) and to protect offline transient keys (described next).
- The offline transient keys are used to protect data on the device that has a limited lifetime, as specified by IT policies applied to the user, the user's device, or the application that is the source or the data. Data policies are described in further detail below. As offline transient keys expire, the key and all data encrypted with that key are deleted from the device.
- The session key is a 32 byte, randomly generated encryption key that is only used for the lifetime of the current session. All session-specific data is encrypted with this key, and all session data along with the key is destroyed when the session expires or the session is terminated via the LINK Controller.

Encryption keys are only stored in transient memory on the device, and they are explicitly cleared from memory when the application terminates or when a session ends.

Using this combination of keys, the Mobile Helix Data Security Platform ensures that (a) data is protected from all other applications on the device, even if the device is compromised, and (b) IT has the flexibility to define policies that govern when data can

be consumed, by whom, and how often a user must re-authenticate in an online session to preserve data on the device.

### **Authentication and Authorization**

The best and first line of defense against any attack is a good password. IT has invested a significant amount of time, training, and technology in ensuring that corporate credentials (i.e., users' LDAP or Active Directory credentials) are strong. It is essential to leverage that same credential for authentication on the device to ensure that when each online session is initiated it begins with an effective authentication event.

By integrating with an organization's existing authentication and SSO infrastructure, the Data Security Platform extends the enterprise's existing investment in strong authentication to the mobile realm. In addition, because the Data Security Platform integrates directly with the existing corporate intranet infrastructure, all authorization policies that apply to existing servers and services are seamlessly extended to mobile access. While IT can place more restrictive policies on mobile data access, the Data Security Platform does not allow a user to access any more data than she could access from her laptop at her desk.

When a device is offline, any offline sessions must be authenticated without involving the corporate infrastructure. The Mobile Helix Data Security Platform uses the bcrypt hash algorithm to safely hash credentials and store them for offline comparison. IT may have a policy that corporate credentials should never be cached on a personal device. In this case or when a second authentication factor is desired, LINK allows IT to require users to create an offline PIN code, which is a strong credential used exclusively for offline access. IT can set a policy to ensure the PIN code is of sufficient length and complexity to properly protect the device. LINK synchronizes a user's offline PIN code across devices on each online authentication, hence IT can enforce PIN code expiration policies for offline PIN codes without deleting a user's offline data, and users can define a single offline PIN code of sufficient strength rather than using simpler PIN codes per device to make it easier to remember them.

Once a user is authenticated via corporate systems, the LINK Controller applies an additional layer of authorization and policy to that user's session. These additional policies are determined based on the device's location, the specific device, and the user's role. The data protection policies available in LINK are described further below.

### **Session Management**

The Mobile Helix Data Security Platform provides a flexible policy infrastructure for implementing session management policies that apply to online and offline sessions. Session management policies govern how long a session is active and under what

circumstances a user must re-authenticate. IT can create separate session management policies that control:

- How long a user session persists when the session is initiated via an online authentication
- How long a user session persists when the session is initiated via an offline authentication
- What credentials are used to protect offline sessions (corporate password/separate offline PIN code/both)
- The composition of offline PIN codes and how often they expire
- What circumstances trigger re-authentication

With these policy options IT can flexibly balance user experience with security, making context-aware decisions regarding how a user authenticates and how often that user must re-authenticate.

### **Protecting the Integrity of Communications to the LINK Gateway**

TLS-based encryption is effective for over-the-air communications because it ensures that data is protected against common network-born attacks, such as man-in-the-middle and replay attacks. However, without proper care, TLS-based communication is vulnerable to transparent proxy attacks.

This category of attacks refers to placing a proxy server in between the device and the intended destination of its communications. Such a proxy could quietly establish a secured TLS session with the device and the destination, while inserting itself in the middle and decrypting data that it receives from the device. The most common way to implement such an attack is by deploying a rogue wireless access point, then using a social attack to convince a user to install the proxy for communication via the rogue access point.

Preventing such attacks is simply a matter of verifying that validity of the destination of all TLS communications before sending any data. The Data Security Platform does so by ensuring that all LINK Gateways and the LINK Controller must be installed with certificates that are either signed by an enterprise's own certificate authority or by Mobile Helix. The LINK App verifies these certificates prior to any communications to the corporate infrastructure.

## Implementing Data Policies

The Mobile Helix Data Security Platform divides data into 3 categories – online data, offline persistent data, and offline transient data. IT uses role-based policies to segregate data from each application into one of the 3 categories. Online data is only accessible during an online session, which begins with an authentication request to the LINK Controller and continues as long as the session has not expired and the device is online. Offline data is accessible both during an online session and during an offline session. Offline sessions begin with a local authentication on the device, either using the user's corporate credentials or the user's offline PIN code as described above.

Offline data is further segregated into two categories – offline persistent data, and offline transient data. Offline persistent data is available indefinitely on the device, although it may be deleted from the device if the local cache storage quota is exceeded or the device is wiped remotely (for a further discussion of application-specific offline data, see the paper entitled "LINK Offline Data Architecture."). Offline transient data is available for a specified period of time on the device. If that data is not refreshed during an online session prior to the expiration, then the data is automatically deleted from the device. IT has the option to specify that all offline data is transient.

Data policies may be attached to user groups (via a role-based scheme), devices or applications. During any given session, the most restrictive intersection of these policies is determined based on the user's device, the user's role, and the application that is providing the data. Policies may be further refined to only apply when the user authenticates from certain locations, allowing context aware policy definitions. Once data is categorized via policy, it is protected at rest according to the categorized encryption keys described above.

## Remote Data Wipe

The LINK Controller enables IT to issue a remote wipe command to any single device or to all devices owned by a single user in order to delete the data stored in the LINK App. This command does not impact a user's personal data in any way – it will only wipe corporate data from the device. This remote wipe command is delivered as a push notification to the device, and the push notification is re-sent until the device is confirmed as wiped or IT chooses to stop the wipe command. Once a device or user is deleted, all online access to the LINK system is instantly revoked for that device or user respectively.

## Protecting the LINK App

In the event that a device is compromised via a malware that "jailbreaks" or "roots" the device, that malware can subsequently disable all attempts to detect compromised devices (via a device management technology) and it can attempt to compromise the device Operating System's runtime system to interfere with encryption. Both iOS and

Android use runtime systems (for Objective-C and Java respectively) that create a single point of failure for compromising the runtime system. While this category of attack requires sophisticated technology to implement, it is devastating in its effect if successful.

To protect against this category of attack, all LINK encryption algorithms and APIs are implemented directly in the LINK App, without reference to or usage of the underlying device runtime. This design decision ensures that no automated attacks against the device OS will succeed in compromising LINK and it ensures a uniform level of data protection across all supported platforms, regardless of the particular device OS.

In addition, by using static linking, inlining, and other obfuscation techniques to create the LINK binaries, LINK further ensures that compromising the LINK App requires extended, direct contact with a device by an expert hacker and cannot be launched via automated malware. While no application is safe from a sophisticated, determined hacker with a debugger and a compromised device, we apply the industry's best techniques to protect the LINK App binaries from compromise.

### **Data Loss Prevention (DLP)**

Fundamental to any data protection strategy is a DLP solution. IT uses DLP solutions to filter email content and web traffic and ensure that sensitive data is not leaked outside the enterprise in emails, email attachments, webmail, web storage services, or other websites. LINK is designed to extend existing DLP infrastructure to the mobile device by routing all traffic through corporate infrastructure, including Exchange servers and existing web proxies. This ensures that the mobile device is not an escape from the corporate DLP infrastructure.

## **Conclusion**

The mobile data protection strategy should be the strongest link in the enterprise's data security strategy. The Mobile Helix Data Security Platform is designed to protect sensitive data from today's most advanced threats. Mobile Helix employs state-of-the-art techniques in encryption and in the implementation of each component of LINK to keep enterprise data protected. By integrating with the investments IT has already made in data protection, Mobile Helix extends the enterprise's existing security infrastructure and best practices to the mobile endpoint.

## About Mobile Helix® LINK

Mobile Helix, Inc. provides software solutions which make it easy for lawyers and other professionals to be productive from smartphones and tablets. The LINK system integrates document management systems/ECM, email, network file shares, SharePoint, and the firm intranet in a single encrypted container app. Mobile Helix' solutions deliver the high level of security required by clients in regulated industries yet are simple to use and affordable to deploy.

To learn more about Mobile Helix LINK please visit us at [www.mobilehelix.com](http://www.mobilehelix.com).

### MOBILE HELIX INC.

Mobile Helix Inc.

650 Castro St.

Suite 120-342

Mountain View, CA

USA

Phone: +1 (347) 508-0967

[contact@mobilehelix.com](mailto:contact@mobilehelix.com)

[www.mobilehelix.com](http://www.mobilehelix.com)