
DISASTER AVOIDANCE AND DATA SECURITY IN THE MOBILE ENVIRONMENT



Table of Contents

Introduction	2
Hosted Solution	3
Data Center Connectivity	3
Handset Security and Connectivity	4
Data Movement	5
Aircllic Application Integration	6
Aircllic Physical Security	8
Conclusion	8
Contact	9

© Aircllic 2010. All Rights Reserved.
No reprints without permission.

Introduction

For those involved in making major technology decisions for their organizations, disaster avoidance and data security are primary concerns. Because the data managed by an enterprise is often one of its greatest assets, that information must not fall into the wrong hands or be compromised in any way. Protecting this asset becomes increasingly complex when a corporate infrastructure takes on a mobile component. The challenge is to maintain the same high level of security without incurring significant additional overhead. Airclic can help organizations achieve this balance, enabling them to make use of new technology without having to reinvent security systems or make additional investments in infrastructure. Airclic realizes that disasters will threaten, so our approach is to minimize the impact by offering controls and redundancy throughout the architecture.

“ We stay up at night so our customers don't have to. ”

Rick Pontin, CEO of Airclic

Hosted Solution

Airclic's Perform products are hosted on our Software-as-a-Service (SaaS) Mobile Performance Platform™ which includes best in class security, disaster avoidance and data connectivity. Airclic recognizes that not all customers have the ability to invest in and manage a mobility solution that supports their mobile supply chain management and logistics operations, but that mobility needs to be embraced by the enterprise to continue growth, manage costs and meet customer demands. Guided by the concerns of our customers, we have created an infrastructure that provides the highest levels of security and up-time, while making sure that our customers' existing processes are not compromised in any way. We ensure that any components that interact with your existing infrastructure are protected by multiple levels of security and data redundancy. Instead of worrying about firewalls, routers and where the solution fits in the DMZ, our customers can focus on what really matters—growing their business, providing unsurpassed customer service and improving the bottom line.

GUIDED BY THE CONCERNS OF OUR CUSTOMERS, WE HAVE CREATED AN INFRASTRUCTURE THAT PROVIDES THE HIGHEST LEVELS OF SECURITY AND UP-TIME, WHILE MAKING SURE THAT OUR CUSTOMERS' EXISTING PROCESSES ARE NOT COMPROMISED IN ANY WAY.

Data Center Connectivity

Airclic has chosen Level 3 Communications (<http://www.level3.com>) as our communication pipeline for essentially two reasons. First, they operate one of the largest communications and Internet backbones in the world, with a clientele that includes 18 of the world's top 20 telecom companies, 8 of the top 10 US ISP's, as well many of the largest US-based wireless providers. Second, Level 3 owns over 39,500 intercity route miles of telecom connectivity and, in total, opens up more than 77,000 intercity route miles for its customers. This ensures that, in the event of an interruption with one of the pathways, the data can simply be rerouted. And, in the event Level 3 were to experience a complete outage, Airclic has two other communication providers that can provide a backup channel for data movement. In addition, data is being continually replicated in real time to a secondary data location more than a thousand miles from the primary data location. This remote positioning offers protection from environmental issues that can affect certain regions of the United States. The secondary location remains dormant and in data collection mode, but if there is a problem, it can become primary within seconds.

Handset Security and Connectivity

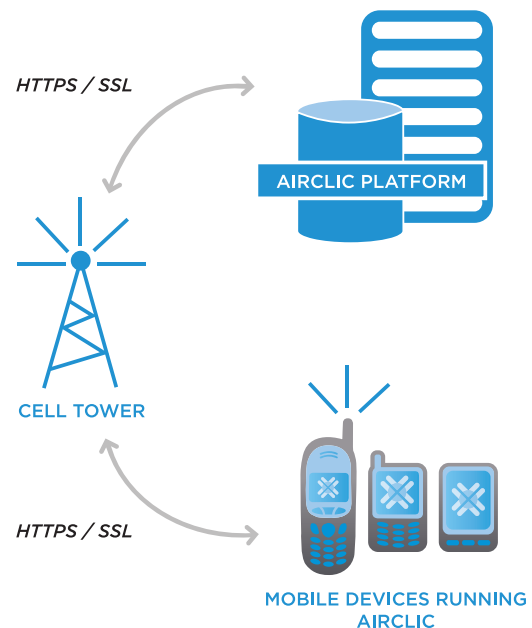
Airclic has chosen a handset security model similar to the one used by many corporate IT departments. Instead of requiring that each mobile handset has a static IP address that is directly accessible through the Internet, Airclic has chosen to communicate with the remote device in a much more secure manner. The Airclic solution allows the handset to have an IP address that changes on schedule or on demand and exists behind a private subnet. This alleviates the main concerns related to static IP provisioning because any party that is looking for a security breach through the mobile environment would have to find the handset. This is nearly impossible since the IP address is not published and dynamically changes. In fact, private IP addresses are not accessible from the Internet and potential hackers are unable to gain access to the device. Many competitors choose to use public IP addresses, which are not only static but are accessible to hackers who can exploit security holes within the device.

As users enter information into the handset, the data is stored locally in a file system. The mobile device then attempts to make a data connection to the nearest cellular tower in the data transfer format utilized by that carrier. Once a link has been established, the data is encrypted by the carrier and the mobile device uploads the data to Airclic using Hypertext Transfer Protocol (HTTP). By default, all Airclic data is encrypted at every stage of the transmission process. For example, just after a mobile device uploads data using secure Hypertext Transfer Protocol (HTTPS) with Secure Sockets Layer (SSL) to Airclic, it is re-encrypted with 128-bit encryption for final transfer to the customer's premise. Throughout the process, the transmitted data goes through an acknowledgement and sequence mechanism to ensure reliable transport even with poor network coverage. If a mobile worker is out of cell coverage but still needs to gather field information, the Airclic-enabled handset can store data until an appropriate communication channel is available. When the mobile phone is brought back into cellular coverage, it will download all information that has been collected since the last successful transmission. As a last precaution, in the event a mobile handset ever appears to be compromised—for any reason—an administrator can remotely lock the application, immediately preventing anyone from using it and ceasing all interaction between this device and other elements of the Airclic platform.

Airclic Mobile Application

Securely enables two-way data communication through a variety of networks including cellular carriers and Wi-Fi connections.

Figure 1: Airclic Mobile Application connectivity



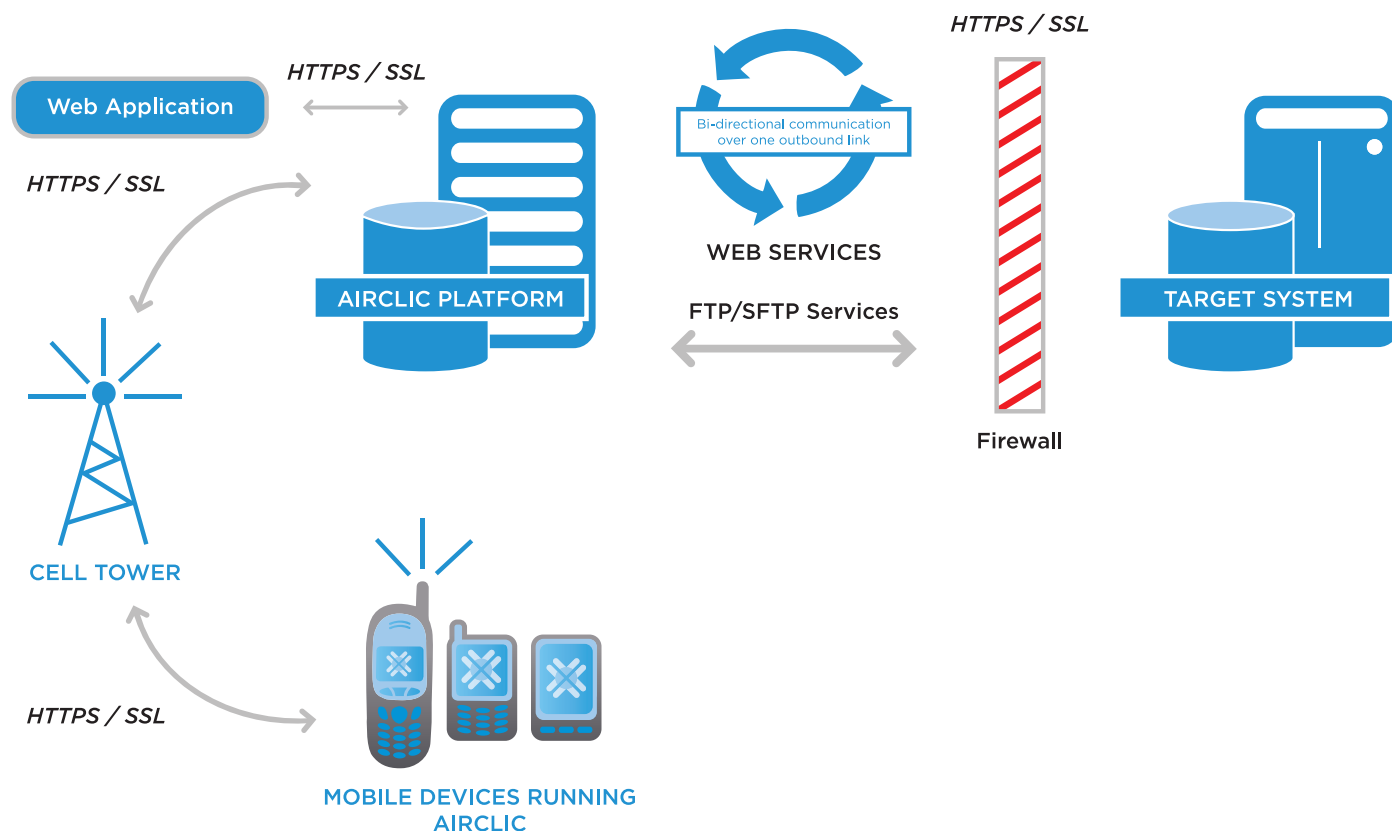
Data Movement

Aircltic offers customers multiple ways to access their data—through the password-protected Aircltic Performance View™ web application, secure FTP file transfers or via web services integration. The first option allows the customer to view, search and print the collected data via HTTPS/SSL. Only those individuals authorized by the customer are given the correct log-in credentials, ensuring the highest level of security.

The second option involves structured files transported directly between the Aircltic Mobile Performance Platform™ and a customer's back-end system via FTP or SFTP in real-time.

The third option leverages web services for direct integration. In this arrangement, the Aircltic Mobile Performance Platform™ serves as the integration point (figure 2). The primary advantage of this method is that all web service calls are made behind your firewall with no additional software or hardware required to be managed. We transport all web services calls securely in HTTP over SSL.

Figure 2: FTP and Web Services when used behind firewall



Aircllic Application Integration

The Aircllic strategy is to treat system integration security as an extension of its own mission-critical security methodology. When a customer purchases an Aircllic Perform™ product with integration to add real-time mobility to their organization, they are leveraging the robust security framework already imbedded in the Aircllic architecture.

Many technology providers take an approach to integration based on software that simply allows back-office systems to communicate with that vendor's application at the expense of overall security (figure 3).

This forces the customer to create a new security policy and rework the entire security element. This can also require a constant inbound connection through the firewall—virtually an open invitation to hackers interested in accessing their data. Aircllic takes a radically different approach, which closes down these openings wherever possible.

THE AIRCLIC STRATEGY IS TO TREAT SYSTEM INTEGRATION SECURITY AS AN EXTENSION OF ITS OWN MISSION-CRITICAL SECURITY METHODOLOGY.

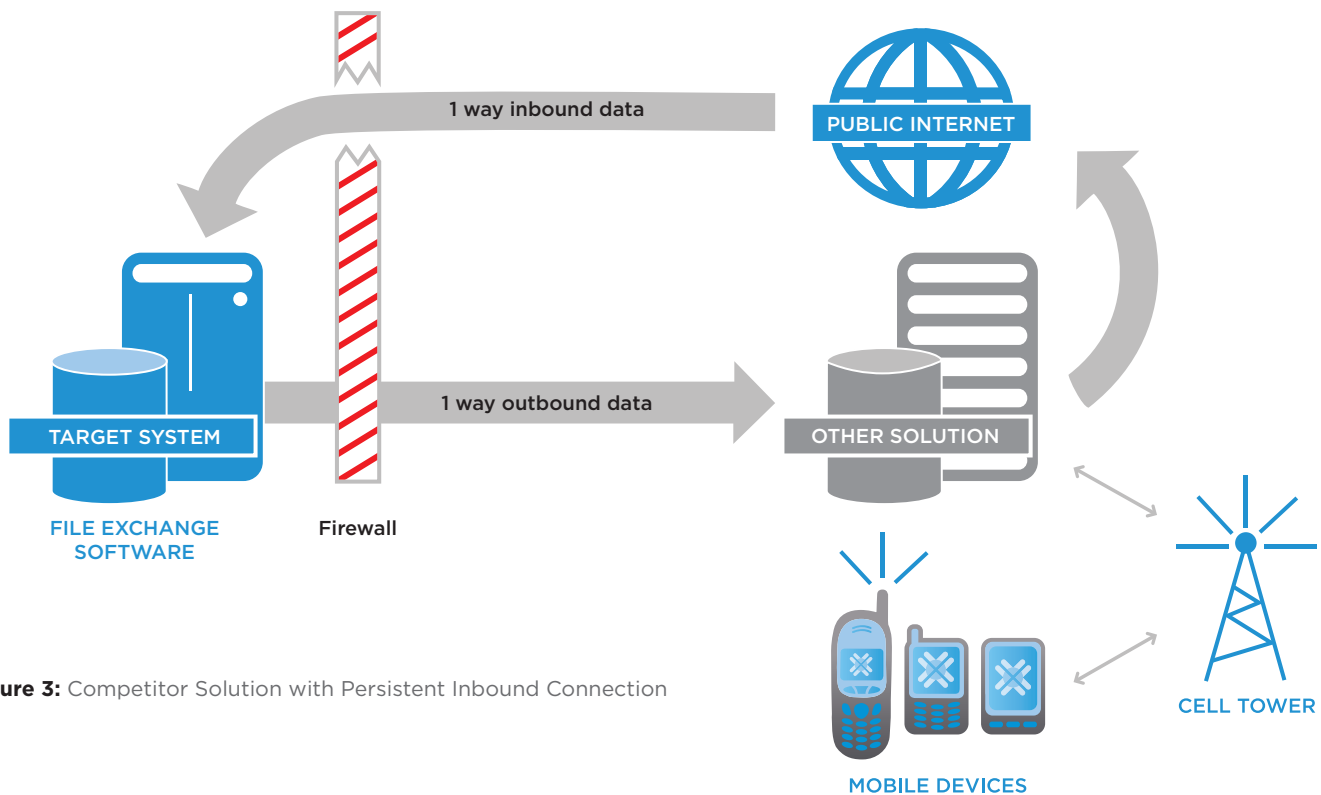


Figure 3: Competitor Solution with Persistent Inbound Connection

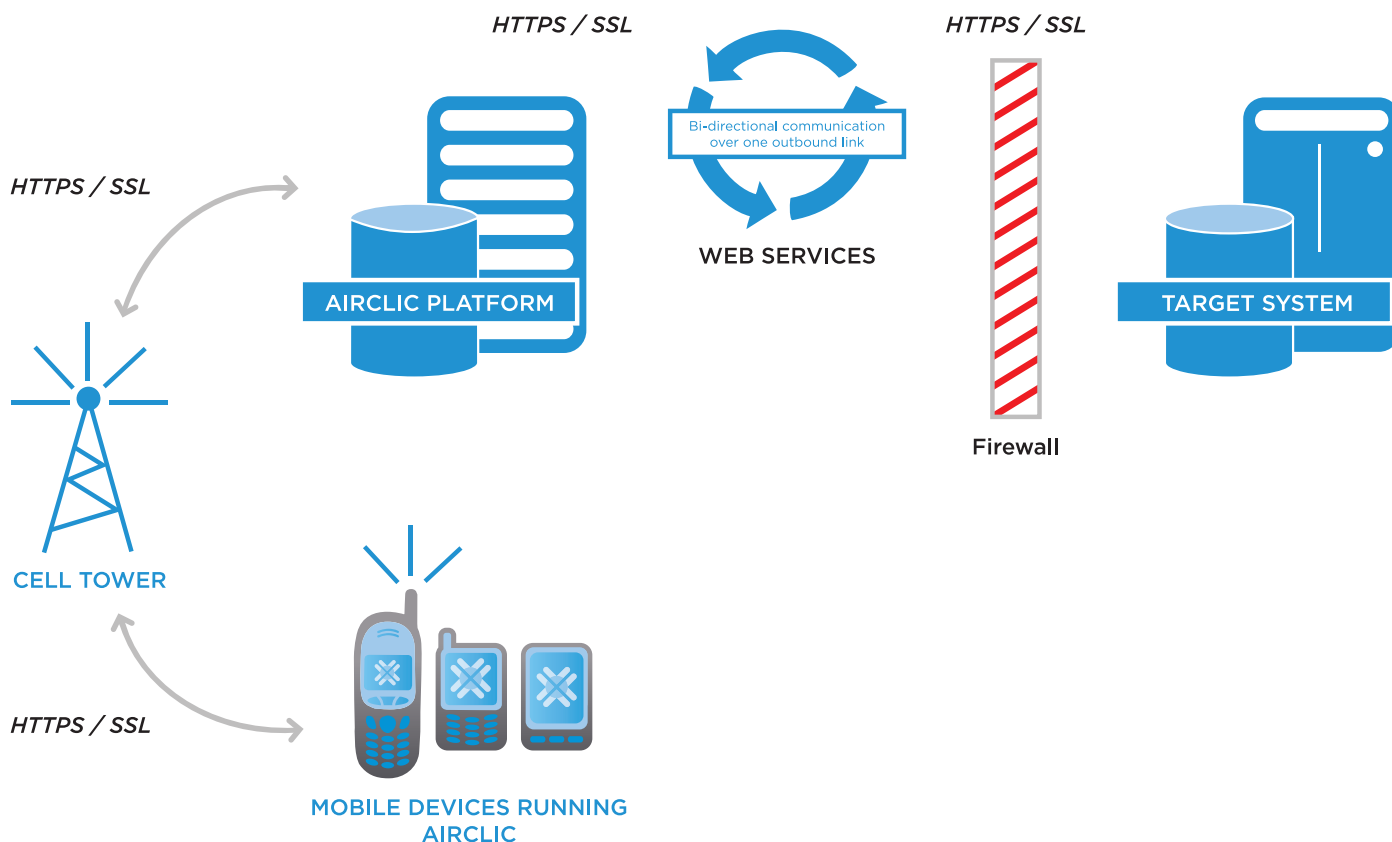
The Airclic Mobile Performance Platform™ acts as a VPN (Virtual Private Network), using only an outbound connection from the customer location. Although two-way traffic is traveling over the Internet, there is no risk because the Airclic integration model is inherently secure.

All data requests have to pass a series of tests to be allowed through. For the first test, the Airclic platform sifts through thousands of data packets and ensures that only correctly formatted data is processed. If the request does not ask for a very specific piece of information, it is rejected and never touches the customer's data. In the second test, the Airclic platform evaluates the remaining packets and ensures that they possess the correct security token.

Since all of this traffic can navigate via TCP port 443 with only an outbound connection, there is no need to open a new hole in the firewall. By default, all traffic to and from Airclic leverages port 443 as the primary option. With the included AES 256 encryption, there is an additional VPN-like security link from beginning to end.

From the moment of capture on the handset, the data is encrypted throughout the entire transmission until it reaches the customer's environment and system.

Figure 4: Airclic Security Architecture



Aircllic Physical Security

Aircllic stores its customer information at a state-of-the-art data center that offers protection against fire damage, water damage and unauthorized entry. The facility provides 24/7 security including photo and RFID access card verification and biometric sensors at all entry points. The server and networking hardware is located in a strictly environmentally-controlled area with heat sensors that can detect minute increases in temperature. If a problem arises, the Aircllic Operations Team communicates directly with select individuals who have access, so changes can be made immediately.

As discussed in the “Data Center Connectivity” section on page 2, if the primary facility fails to operate, all data is routed to a second location. There is little or no impact to the customer since data is continuously replicated and almost instantly distributed to the secondary location. The primary and secondary sites are positioned in two different geographic areas to further ensure the highest level of up-time. In addition, there are multiple lines going in and out of the data center so minor regional outages have minimal impact to the Aircllic Mobile Performance Platform™.

AIRCLIC STORES ITS CUSTOMER INFORMATION AT A STATE-OF-THE-ART DATA CENTER THAT OFFERS PROTECTION AGAINST FIRE DAMAGE, WATER DAMAGE AND UNAUTHORIZED ENTRY.

Conclusion

At Aircllic, we believe that our customers should never experience service interruptions or security breaches, so our architecture and software have been designed to anticipate any and every possible problem. We continuously monitor our systems and improve our methods - in essence, **we stay up at night so our customers don't have to.**

U.S.
HEADQUARTERS
900 NORTHBROOK DR.
SUITE #100
TREVOSE, PA 19053
TEL: +1 (215) 504-0560
information@aircllic.com

OFFICE
11460 CRONRIDGE DR.
SUITE #102
OWINGS MILLS, MD 21117
TOLL-FREE: +1 (800) 854-0473
information@aircllic.com

AIRCLIC MÉXICO
GRUPO AIRCLIC MÉXICO
RUBÉN DARÍO NO. 281
PISO 10, DESPACHO 1002
COL. BOSQUE DE CHAPULTEPEC
C.P. 11580 MÉXICO, D.F.
TEL: +55 3098 3360
informes@mx.aircllic.com

AIRCLIC EUROPE
KING'S LODGE,
194 KING'S ROAD
READING BERKSHIRE,
RG1 4NH
UK
TEL: +44 (0) 118 955 8500
info@aircllic.co.uk

AIRCLIC SPAIN
BALMES, 123 4º, 2ªA
08008 BARCELONA,
SPAIN
TEL: +34 93 452 2246
lgurgel@aircllic.com