Mobile Security Solutions

Secure Communications with Confidence

Mobile endpoints enhance productivity but add risk to infrastructure and intellectual property.

PROFESSIONAL SERVICES

- Cloud Computing
- Data Center
- Data Storage
- Desktop Management
- Messaging
- Microsoft Consulting
- **+ MOBILE SECURITY**
- Networking
- Security
- Unified Communications
- Virtualization
- Wireless

MANAGED SERVICES

- Systems Monitoring
- 24/7 Fully Managed Services
- After Hours Support Services
- Custom Tools/Regular Tools

Mobile Security Solutions Overview

Most enterprises today are comfortable with securing and managing computing endpoints such as desktop and laptops, but may not have the same processes for what is likely the fastest-growing computing platform: mobile endpoints. Like a PC, a mobile endpoint is susceptible to malware, spyware, and other threats. Some examples of mobile endpoint devices are:

- BlackBerries
- Androids
- iPhones
- iPads
- HP TouchPads
- Cisco Cius

Not only are these devices capable of enhancing productivity, but they also open pathways to your corporate systems and data. If managed incorrectly, these devices inadvertently open up security holes and increase unauthorized access to your confidential data, systems and infrastructure.

Continental Resources (Conres) eases your concerns of mobile consumerization including security, liability and manageability issues.

To provide a productive and secure environment, all mobile endpoints must be reviewed. Remote access and data backup processes must be evaluated, and mechanisms put in place to manage stolen or lost devices (i.e. encryption and/or remote device disable). Through experience, ConRes understands how mobile devices work with enterprise environments.

ConRes works with you to evaluate/create security processes to ensure your mobile devices are seamlessly integrated without excessive cost and risk.

Major Concerns in Mobile Endpoint Security

There are several significant technial challenges to overcome when addressing mobile security on your corporate and personal mobile devices. Your IT staff will wrestle with balancing the needs of your employee with the need to secure your corporate data.

Challenges Associated with Mobile Endpoint Security

- The user's expectation for full-use (business and personal) of the device.
- The prevalence of compromised data devices and applications.
- The balance between privacy and security.
- Consumerization of IT: Mobile devices are designed, sold and used as consumer devices, while security and manageability become secondary concerns.
- Mobility: Data reaches easily across multiple trusted and untrusted networks exposing the devices to high risks.
- Social networks (high traffic, real-time networks) can be exploited for attacks on enterprise infrastructure and data anywhere...instantly.
- Mobile, cloud, and virtualization technologies connect enterprises to the world, and transmit information well beyond corporate firewalls.

"They [ConRes] have some of the best engineers I've ever worked with. They've been very flexible and very helpful. At heart, they're still people. At the end of the day, they're able to work with you as a company, they're able to work with the individuals. They'll do whatever has to be done. That is, at the end of the day, of utmost importance. If this project needs to work, they'll find a way to make it work for you."

~ Director, Network Operations, Internet and IT of a provider of healthcare information

If some of these challenges match your current environment, leverage the expertise of ConRes to take the burden off your team. Engage ConRes to review your challenges, propose a solution...and propose a course of action aligned with your acceptable risk threshold. We ensure secure mobile device access in relation to your corporate data.

Mobile Device Management is Key

"A well-managed device is a secure device."

Each device has unique functional capabilities as well as an identifiable signature. Along with its core functional components, devices feature entire layers of enhancements, add-ons, hot-fixes, software and firmware updates. The sheer number of device types, combined with disparate features, functions and applications, serves to magnify risk and increase administration costs. The key is to configure and implement mobile/endpoint security solutions consistently with acceptable risk and security parameters.

As mobile devices become smarter, they provide greater corporate access and store more data, thereby increasing the urgency of greater control and management. ConRes shares your concern and works with you to protect corporate information while promoting sustained productivity.

What is Endpoint Security?
Endpoint security is an approach to network protection that requires each computing device (endpoint) associated with a corporate network to comply with certain standards before network access is granted.

What is a Mobile Endpoint?
A mobile endpoint is a wireless handheld device capable of roaming from cell to cell with the ability to gain access to data that does not reside locally on the device. These devices also have the capability to store information locally on the device.

Identifying the Threat

Several mobile devices, like smartphones, have many potential entry points for a compromise. A compromised mobile device can provide a wealth of information to an attacker. Due to their ultra portability, short-range devices such as Bluetooth, Infra-red and Wi-fi are more viable avenues of exploitation.

Potential Threats from Compromised Mobile Devices

- SMS messages give an attacker the ability to search for your passwords and/or perform unauthorized financial transactions.
- Emails give an attacker the opportunity to access your private corporate information such as credentials and password reset links.
- Phones: Low-level access to your hardware allows an attacker to record or listen to your voice conversations.
- Social Networking: Attackers pose as you, allowing the retrieval of your personal information and your social contacts.
- Operating system vulnerabilities.
- Physical access to lost, stolen and/or unattended devices.
- Video/Photo: Low-level access to your hardware provides an attacker with the ability to retrieve video and/or photos from your phone to provide details of its surroundings.
- Built-in GPS or GSM antennas allow attackers to identify the location of your mobile device.
- Attackers are able to access documents stored on your device, including email attachments such as PDF files, Microsoft® Office files, credentials, encryption certificates, internal videos and e-books.

"As enterprises start considering how they will build their mobile security strategy, they must be prepared to invest in cross-platform solutions that can provide protection for the data on the device as well as the enterprise network." *~Senior Research Analyst, IDC's Mobile Enterprise*

Considerations for Mobile Security

Mobile devices work across several different environments, in virtualized infrastructures and with removable media. So when determining your corporate or personal needs for mobile security, take the following questions into account:

- What kinds of data are stored on your mobile devices?
- What kinds of risk do you face and what financial impact do these risks pose?
- What security measures are you currently employing on your devices?
- Do you have any mobile applications that your customers and/or partners can access?
- Does your business need to comply with any regulation that governs loss of specific types of data?
- Do you know if your mobile applications have been created and deployed securely?
- Did you utilize third parties in the development of your mobile applications?

Addressing Mobile Security Now

ConRes recommends addressing the security concerns of your mobile devices as soon as possible. Attention to security while a technology is developing is the key to ensuring the technology grows into a reliable resource. ConRes recommends you:

1. Address the security aspects of cell phones and smartphones used by employees and/or contractors.
2. Ensure your mobile devices are configured, deployed, and managed to meet your security requirements.
3. Employ the appropriate security management.
4. Ensure an ongoing process of maintaining the security of your mobile devices throughout their lives.

9 Recommended Mobile Security Practices

ConRes recommends the following mobile security practices (at a minimum):

- Forcing encryption of data at rest on your mobile devices.
- Forcing secure connectivity on unsecured public networks.
- Confirming unauthorized mobile devices do not have access to your corporate LAN.
- Confirming mobile user spending aligns with the mobile policy.
- Authentication: Setting your device to auto-lock and limits for unauthorized login attempts.
- Having a clear policy on remote data deletion.
- Classifying data according to its sensitivity.
- Allowing only digitally signed applications.
- Being aware and able to adapt to the ever-changing mobile landscape.

Statistically Speaking...

- By 2017, there will be close to 9 billion mobile subscriptions and 85% of the world's population will have Internet coverage via 3G.

  ~Traffic and Market Report, 2012

- The worldwide mobile messaging market was worth USD 202 billion in 2011. This number is forecast to rise to USD 310.2 billion by end-2016.

  ~Mobile Factbook, April 2012

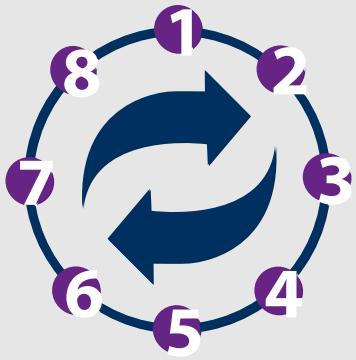
- At the end of 2011, there were 6 billion mobile subscriptions. That is equivalent to 87% of the world population. And is a huge increase from 5.4 billion in 2010 and 4.7 billion mobile subscriptions in 2009.

  ~The International Telecommunication Union, 2011

MOBILE SECURITY SOLUTIONS

PROVEN ENABLING METHODOLOGY®

To provide the most secure and useful solutions, ConRes follows a Proven Enabling Methodology, a structured approach and framework to plan, design, implement and optimize unique solutions.



1. BUSINESS DISCOVERY
2. ASSESS CURRENT STATE
3. GAP ANALYSIS
4. SOLUTION DESIGN
5. PLAN & TEST
6. IMPLEMENT
7. SUPPORT/TRANSITION
8. MONITOR

Benefits of Working with ConRes

The Professional Services team at ConRes consists of solution architects, solution engineers and project management professionals who average over eight years of experience.

Protecting your corporate systems and data is the main focus of our mobile security practice. Supporting this initiative requires distinct policy conformance, encryption and/or disabling methods and unique data backup policies. Having secure data requires paying attention to the smallest detail...how are thumb drives used? What other methods of data transport are used?

ConRes works with you to provide the necessary solutions and support to ensure proper security measures are in place.

Mobile Security Services Provided
To complement these solutions, ConRes provides evaluation, analysis and implementation and management services.

- Software Distribution for Endpoint Devices
- Endpoint Security
- Corporate Data Security
- Remote Access
- Custom Inventory Solutions
- Custom Software Distribution
- Security Policy Management
- Custom Package Building
- Custom Data
- Collection/Customized Reporting
- Software License Compliance
- Data Backup/Recovery
- Configuration & Implementation
- Security Audit & Risk Assessment
- Policy Review & Recommendation
- SLA Review & Mediation

About ConRes

Build a better IT infrastructure and data center, maximize your choice of IT products and services, and strengthen your ROI – with the friendly professionals at ConRes, the hybrid VAR™. As a hybrid, ConRes brings you a broad range of products, combined with the services and support you'd expect from a traditional VAR.

Whether you're an IT professional in business, academia or government, you can rely on ConRes for enterprise-class solutions ranging from virtualization, disaster recovery, unified communications, unified computing, cloud computing, security, and networking to UNIX®, Linux®, and Windows®.

- 50 years of experience and financial stability
- 96% customer satisfaction rating (3rd party survey)
- Ranked annually in the top third on the VAR500 (currently #63)
- Elected to the CRN Tech Elite 250, best-of-breed solution providers

Experience, stability and third party credentials make ConRes a reliable and trustworthy resource for your IT infrastructure and data center solutions.

Links to related online content:

- Full Resource Library
- Partnerships & Solutions Overview
- Professional Services Overview
- Security Solutions Overview

Continental Resources, Inc. | 800.937.4688
Local Contacts: Boston | Chicago | Connecticut | New Jersey | New York
Philadelphia | Washington D.C.
Headquarters: 175 Middlesex Turnpike, Ste 1 | Bedford, MA 01730-9137
ITsolutions.conres.com

ConRes 10035-1209 (Replaces 10035-1110)

ConRes IT SOLUTIONS 50 YEARS