Raytheon

Trusted Access: Mobile

Accessing critical, sensitive, and proprietary data and applications from mobile devices.

Benefits:

- Ideal for Bring Your Own Device (BYOD)
- Co-exists with existing MDM and MAM solutions
- Confident and cost effective collaboration
- Secure access to sensitive, confidential, or proprietary data
- Prevention of data loss and compromise
- Access to native, desktop and web apps

Key Differentiators:

- No modifications or added components required on the device
- Defense-grade security
- Highest level of information assurance and security for sensitive, confidential, or proprietary data
- No reliance on device specific containers and encryption solutions

Every organization has data that is considered mission critical or proprietary and numerous employees require access to that data to perform their jobs, even when away from their offices. Having sensitive data resident on mobile devices puts organizations at risk. For government or military users, sensitive data left unprotected and in the wrong hands can cost the ultimate price – human casualties. For commercial organizations, lost or stolen data can inflict a devastating blow to reputation and stock price, and immeasurable damage to the unsuspecting consumer. In healthcare, loss of patient records could lead to regulatory violations, expose patients' personal information and put lives at risk.

It is a challenge today to enable a mobile workforce. In addition to maintaining data security there are significant IT challenges. Mobile workers not only want access to sensitive, confidential, and even classified data from mobile devices, they also want to be able to use their personal devices to do so. This has ushered in the concept of Bring Your Own Device (BYOD) that is fraught with legal, security and management complexities.

Data resident on any end point device is inherently at risk. The only way to ensure that sensitive data is fully protected is to keep it off the device. But then how do employees who need that data securely gain access to it?

Raytheon, leveraging its long standing information assurance pedigree, delivers an unprecedented capability for securely and confidently accessing critical corporate and classified information from virtually any mobile devices. An ideal solution for security-minded commercial organizations and government.

Trusted Access: Mobile

Trusted Access: Mobile is a leading edge solution that enables secure access and interactions with data and applications from any mobile device. Unlike other solutions that attempt to secure data on the device using container and MDM-based protection/remediation technologies, Raytheon's mobile offering virtualizes native mobile applications in a secure virtual mobile infrastructure (VMI) and leverages secure redisplay technologies for user interactions alleviating concerns of data loss, theft or compromise and making it the ideal solution for BYOD deployments.

Trusted Access: Mobile protects sensitive data and mobile applications by hosting native mobile apps in a virtual mobile infrastructure (VMI) similar to a virtual desktop infrastructure (VDI) and by enforcing access policy within a gateway between the client and protected networks. Secure access on the remote mobile device is facilitated by a secure redisplay app that is provisioned onto the device with device and user identity credentials. The mobile gateway authenticates identity, manages resource access rights and maintains isolation of the discrete backend networks. The solution enables strict yet flexible policy enforcement at the device, gateway and VMI ends based on contextual information such as the user's role, device, location, time of day and many other variables.

The mobile gateway enforces access policy and routes communications between the secure redisplay client and the virtual mobile device instance hosted in the backend. Communications between the device and the gateway can be protected using VPN tunnels that terminate at the gateway border and then the domain border, offering defense-grade security. Mobile applications running on the protected backend are isolated from attack even if the client device becomes compromised. Data accessed by the protected mobile apps never leaves the protected network and is not vulnerable to attack on either the communications channel or the end user mobile device.

Key features of the solution include:

- No data at rest or in transit
- Software key store for device and user certificates
- Hardened mobile gateway using SE Linux foundation
- Identity and device context driven access policy
- Nested encrypted tunnels for secure transfer of redisplay stream
- Mobile gateway blocks all other traffic between device and enterprise
- Gateway isolates traffic between device and multiple protected networks
- PKI using internal or external Certificate Authorities (CAs)
- Revocation of certificates terminate access, device wipe unnecessary
- Remote provisioning of devices with out-of-band delivery of identity tokens
- Virtual mobile infrastructure hosted on protected network
- Virtualized apps are immune from attack by code running on the remote device
- VMI may be instrumented with insider threat detection capabilities

Trusted Access: Mobile Architecture Components

- **Redisplay Client**
  - Provides access to native virtual mobile apps and legacy virtual desktop infrastructure
  - Deployable on commodity or custom devices running Android 4.0 and above. iOS support will be available in Q4 2014.
- **Mobile Gateway**
  - Enforces the access policy for one or more sensitive or proprietary networks and virtual resources
  - Certificate-based identity management using internal certificate authorities or interoperate with existing agency PKI
  - Ensures that sensitive, confidential, or proprietary data never crosses the specified security level boundary
  - Deployable on commodity server platforms
- **Virtual Mobile Infrastructure (VMI)**
  - Ensures that redisplayed mobile apps are isolated from attacks against the physical mobile device
  - Deployable on commodity server platforms

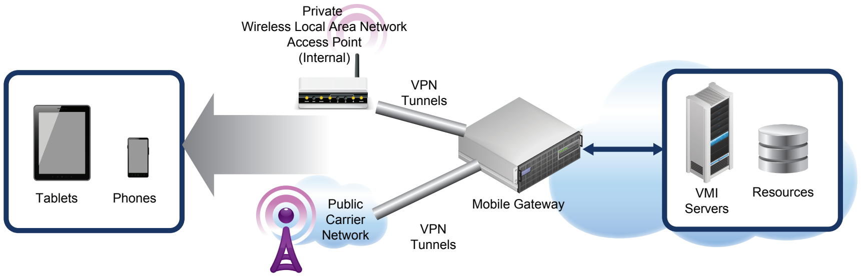
Administration

Trusted Access: Mobile is configured, managed and provisioned through a web-based administration interface that also allows for provisioning of deployed Android devices. The solution is not dependent on a specific MDM solution and integrates easily with any established mobility management ecosystem. Trusted Access: Mobile also enables a streamlined capability to publish and manage mobile applications with a central point of administration.

Robust auditing occurs at every service boundary within Trusted Access: Mobile, including the generation of log and audit entries for events of interest such as connections attempted, dropped, or failed.

Conclusion

Trusted Access: Mobile is the most secure mobile data access solution in the industry today. By employing Raytheon's proprietary VMI and secure redisplay technologies, sensitive, confidential, and proprietary data is accessible securely from mobile devices. It is the answer to BYOD because it is device agnostic and provides the highest degree of security by ensuring that no critical data or applications are resident on the device, yet completely accessible. Now remote workers, field agents, war fighters, or any employee working outside their office environment, can access their organization's sensitive, confidential, or proprietary data from their mobile device without putting that data at risk.



Trusted Access: Mobile Architecture

For further information contact:
Raytheon Cyber Products
12950 Worldgate Drive, Suite 600
Herndon, VA 20170
866.230.1307
www.Raytheon.com/cyberproducts

Raytheon

Customer Success Is Our Mission