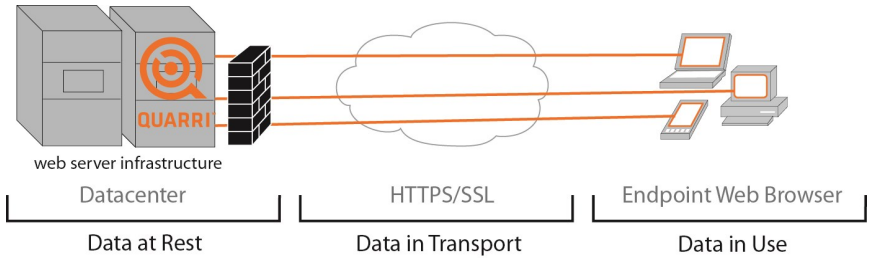
Quarri Protect On Q Mobile for iOS

Secure Your Sensitive Data on Apple iOS Devices

Quarri™ Protect On Q™ Mobile for iOS is the only web information security solution to enable IT professionals to control and protect users' browser sessions on iOS devices from theft or data leakage. By enabling IT administrators to enforce security policies that prevent unauthorized use and replication of confidential data, Protect On Q (POQ) Mobile for iOS enables web applications to place strict controls over the copying, saving and printing of browser-delivered information.



FEATURES

Browser Process Isolation

Blocks hostile code injection attacks such as Man-in-the-Browser as well as potentially hostile browser add-ons (i.e., plug-ins) from launching.

Browser Firewall

Controls allowed browser connections to only site-specified white list of destinations, mitigating session hijacking, XSS, and CSRF attacks.

Content Information Controls

Control file operations, such as copy, save and print within the browser to ensure delivered information is not leaked or replicated via user actions. Controls extend to child processes launched, including applications such as Adobe Acrobat, Microsoft Office and ZIP.

Screen Capture Detection

Detect screen shots captured via users pressing Home and Sleep/Wake buttons simultaneously. The user is notified the event contravenes policy and event is logged to POQ Manager.

Blocking of Apple Airplay

Block iOS display mirroring to PC devices via AirPlay when "Block Screen Capture" is enabled in the policy.

Jailbroken Device Control

Detects if iOS devices are jailbroken (rooted) and if true, enables site owner to block access to the protected web application from that device.

SSL Certificate Defenses

Mitigates MITM / hostile SSL proxying of secured connections by specifying a white list of allowed SSL certificates. To control social engineering of users certificate handling, sites can specify whether users can override certificate errors (expired, mismatched etc.).

Browser Session Data Privacy

Data files created during the protected session, including cache files, cookies, password store and history, are over-written and deleted at the end of session.

Toolbar Skinning

Enables site owners to brand toolbar color of their protected browser, providing visually distinct user interface that aids in reducing phishing risks.

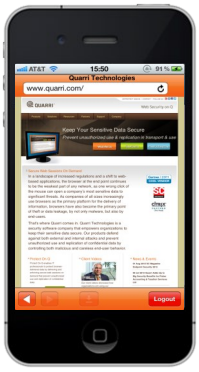
Session Timers

Allows sites to mitigate user mistakes by controlling both overall session length, as well as user inactivity.

SYSTEM REQUIREMENTS

Apple iOS devices

- iOS 5 or greater



Gartner | 2011 COOL VENDOR

SC MAGAZINE INNOVATOR

RSA CONFERENCE INNOVATION SANDBOX

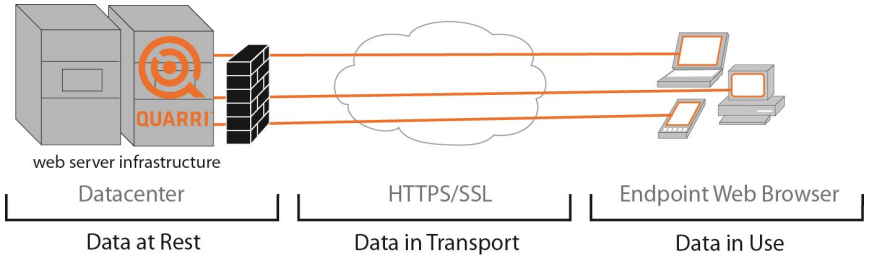
Phone: US: +1 866 416 9970
UK: +44 (7769) 710078
+1 512 590 7731
Fax: +1 512 777 5005
E-mail: info@quarri.com

Quarri Technologies, Inc.
7500 Rialto Blvd.
Building 2, Suite 210
Austin, TX 78735
www.quarri.com

Quarri Protect On Q Mobile for Android

Secure Your Sensitive Data on Android Devices

Quarri™ Protect On Q™ Mobile for Android is the only web information security solution to enable IT professionals to control and protect users' browser sessions from theft or data leakage. By enabling IT administrators to enforce security policies that prevent unauthorized use and replication of confidential data, Protect On Q (POQ) Mobile for Android enables web applications to place strict controls over the copying, saving, printing and screen-capturing of browser-delivered information.



FEATURES

Browser Process Isolation
Blocks hostile code injection attacks such as Man-in-the-Browser as well as potentially hostile browser add-ons (i.e., plug-ins) from launching

Browser Firewall
Controls allowed browser connections destinations with a site-specified white list, mitigating session hijacking, XSS, and CSRF attacks.

Content Information Controls
Control file operations, such as copy, save, print and screen-capture within the browser to ensure delivered information is not leaked or replicated via user actions. Controls extend to child processes launched, including applications such as Adobe Acrobat, Microsoft Office and ZIP.

Rooted Device Control
Detects if Android devices are rooted and if true, enables site owner to block access to the protected web application from that device.

SSL Certificate Defenses
Mitigates MITM / hostile SSL proxying of secured connections by specifying a white list of allowed SSL certificates. To control social engineering of users certificate handling, sites can specify whether users can override certificate errors (expired, mismatched etc.).

Browser Session Data Privacy
Data files created during the protected session, including cache files, cookies, password store and history, are over-written and deleted at the end of session.

Toolbar Skinning
Enables site owners to brand the toolbar color of their protected browser, providing a visually distinct user interface that aids in reducing phishing risks.

Session Timers
Allows sites to mitigate user mistakes by controlling both overall session length, as well as user inactivity.

SYSTEM REQUIREMENTS

Android Device

- Android 2.2+

Gartner | 2011 COOL VENDOR

SC MAGAZINE INNOVATOR

RSA CONFERENCE INNOVATION SANDBOX

Phone: US: +1 866 416 9970
UK: +44 (7769) 710078
+1 512 590 7731
Fax: +1 512 777 5005
E-mail: info@quarri.com

Quarri Technologies, Inc.
7500 Rialto Blvd.
Building 2, Suite 210
Austin, TX 78735
www.quarri.com