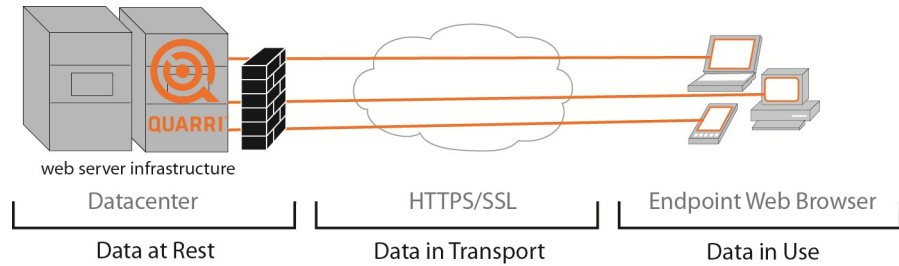


## Secure Your Sensitive Data

Quarri™ Protect On Q™ is the only on demand web information security solution to enable IT professionals to control and protect users' browser sessions



from theft or data leakage. Protect On Q's hardened browser shields sensitive data from key loggers, session hijacking, cache miners, and other malware, while blocking inbound attacks as well. Protect On Q also enables IT administrators to place strict controls over the saving, forwarding, or printing of browser-delivered information. Protect On Q is downloaded automatically and transparently to the user's browser, and completely cleaned up at the end of a browser session – there are never any signature downloads, software updates, client maintenance costs, or administration headaches.

### FEATURES

#### Zero-hour Malware Defense

Scan running processes throughout session using patented run time behavioral analytics to identify key logging and frame grabbing applications. Policy-defined actions block availability of keyboard inputs and screen capture.

#### 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) launching; allows white listing required add-ons; all others are blocked

#### Browser firewall

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

#### Hostname Resolution Bypass

Provides site-specified hostname resolution, enabling the bypass of local host file or DNS resolution, mitigating name resolution-based attack.

#### Content Information Controls

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

#### Browser Session Data Privacy

Real-time encryption using 256-bit RC4 for data files created during the protected session, including cache files, cookies, password store and history. All session data is overwritten and deleted at end of session.

#### 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.).

#### Virtual Machine / RDP Block

Enables sites to control whether its users can access from virtual OS or

terminal services connections, which can create data leakage bypasses.

#### Browser Skinning

Enables sites to brand their protected browser, while 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.

#### Filter Module Enforcement

Enables web applications to enforce the use of the protected browser. Sites can use Quarri's .NET pipeline modules, Java request filter modules or web services APIs.

#### Citrix NetScaler Integration

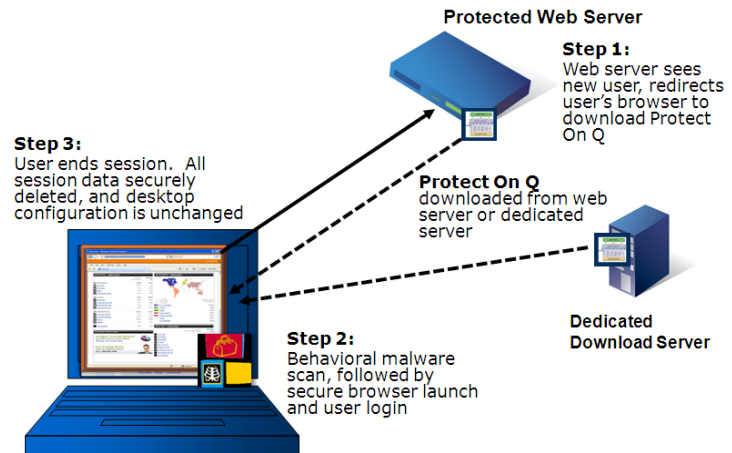
Enables easy product integration with Citrix market leading web front end.

#### Syslog Support

Utilize syslog servers to receive log information from POQ Servers.

## HOW PROTECT ON Q WORKS

Protect On Q is a software solution which delivers an on demand security agent to the user's Windows PC endpoint that protects that single browser session from data compromise via malware, as well as careless or malicious end users. Using the Protect On Q management console, an administrator defines granular, application-specific policy settings. These settings are packaged with the agent components and placed on a provisioning server for subsequent download. The provisioning server can run on the web application server or a remote standalone server.



As users connect to a web site, a check is made to ensure that users are running Protect On Q before they log in, through simple changes to the web server. If they are not, a web services call triggers an automatic download of the agent from the provisioning server to the user's desktop and a new, secured, visually distinct browser instance is launched. The web application can be integrated with Protect On Q to make use of the protected browser mandatory. Protect On Q enforces security in only the secured browser; no other browser instances or applications are affected. When the user logs out of the protected web application, the agent exits and cleans itself up, leaving behind no remnants or modifications to the user's desktop.

## SYSTEM REQUIREMENTS

### Windows Agent

- 32-bit Windows XP, Vista or 7 and 64-bit versions of Vista or Windows 7 and applications
- IE6 to IE9 installed, JavaScript enabled
- Sun JRE 1.4.2+ or ActiveX enabled
- 10MB disk space, 256MB RAM
- No admin rights required

### Management Console

- Manager: installs into Tomcat 6 or other servlet engines with Java 6
- Server: installs into Tomcat 6 or other servlet engines with Java 6
- 100MB disk space
- 512 MB RAM

### Cool Vendors in User and Data Security, 2011

Ray Wagner, Avivah Litan, John Girard, Peter Firstbrook, Eric Ouellet, Joseph Feiman, April 21, 2011

Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Phone: US: +1 866-248-3990  
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