

## Protect Your Weakest Security Link: The Web Browser

Despite major investments in online security, companies and individuals still face significant risk to their data. In the battle for information security, cyber-criminals are moving faster and more aggressively than ever before. Lost data, stolen financial records, identity theft and public relations nightmares are in the news every day. And no one is completely safe: a recent study found that users visiting the most popular 1,000 web sites, including news and banking sites, are often *just two clicks away from malicious content*<sup>1</sup>.

The same study also found that the proportion of malicious links associated with top news sites, such as CNN, were higher than that of traditionally risky sites, such as online gambling or pornography. In fact, ninety percent of web threats come from trusted web sites, where malware has been embedded through dynamic or static links<sup>2</sup>.

In addition to being the focus of malware targeting valuable information, users – both careless and malicious - can be another method of browser-driven loss of sensitive content such as employee records, customer account data, and company intellectual property. The costs of security breaches are rising as companies deal with the theft of sensitive corporate and customer data, fines, legal costs and damage to their reputations. How do you protect your employees, patients and customers from data leaks that result in financial loss, medical fraud, identity theft and more?

### **HTTPS is no match for today's complex threats.**

Convenient “anytime, “anywhere” access has driven explosive growth in online services, from electronic banking and insurance to enterprise collaboration and healthcare portals. The volume of private and sensitive data delivered to browsers is higher than ever. Unfortunately, the browser has also become the primary vulnerability point for data leakage and malware attacks.

Applications are delivering sensitive data through an encrypted tunnel, but what happens upon delivery and decryption of that data at the endpoint? Web server security solutions and HTTPS offer little defense to data once it has been delivered to the endpoint, as today's most significant exposure is at the point of transaction – the end user's browser. Browser session content at the endpoint is increasingly at risk from theft or data leakage by malware or users.

**Data loss: an inside job?**

Threats to sensitive data don't just come from outside the company. With many of today's CRM databases, it's astonishingly easy to copy vast amounts of critical data, such as customer information, account numbers and other financial information onto an external drive. In fact, many companies have lost data to unscrupulous employees who have stolen competitive business information and either sold it or taken it with them to a new company. The consequences of data theft can be devastating — ranging from reputation damage to lawsuits and financial loss.

Data loss can also occur unintentionally by employees. With hosted enterprise applications like CRM systems and webmail, users have the flexibility to work anytime, anywhere from any browser-enabled PC. However, this web access model means you don't control the endpoint or its security. Every day you have to anticipate common scenarios, such as:

- An executive using an airport lounge computer to access corporate web-mail downloads some files and then departs on a flight, inadvertently leaving sensitive data on a public machine.
- A physician downloads patient records to a home computer. A key-logging application steals her ID and password and instantly gains access to thousands of names, insurance information, identification numbers and more.

To combat pervasive and fast-moving security risks both inside and outside of your company, you need a solution that's as flexible, seamless and easy-to-use as your web applications.

**Deliver instant protection wherever your users are.**

With Quarri, you can deliver a secure browsing experience anytime, anywhere, without having to deploy client software. Our key product, Protect On Q™, protects users and browser-delivered content from theft or data leakage by malware or users. Best of all, there's no software to install or need for system modifications. As a result, we can help you:

- Automatically protect and control browser operations and behavior to ensure that the web session and its content are protected.
- Ensure comprehensive information security by protecting all elements of browser-delivered content.

- Achieve significant deployment, support and usability cost savings with no user installation, system modification, software installation or residual software.
- Protect users on kiosk machines or those running with guest privileges.

Complement existing security products or browsers installed on client PCs.

**Quarri Protect On Q: *Make web information protection as easy as opening a browser.***

Quarri Protect On Q works by instantly and temporarily extending an automatic security agent from your web site to the browser, where it forms an armored barrier against keyloggers, session hijacking, cache miners, web malware and other attacks that may be introduced through a customer's web browser. Protect On Q protects your users against account takeover and data loss, even from malware embedded on compromised client computers.

The security features of Protect On Q include:

- Zero-hour malware defense protects against key logging, frame grabbing and MITB applications.
- Browser process isolation screens and filters potentially hostile browser add-ons.
- Browser firewall controls help minimize browser redirection attacks.
- Hostname resolution bypass fights malware that uses DNS or hostname tampering.
- Browser session data privacy encrypts all data files created within the armored browser session.
- HTTPS certificate defenses enable web sites to securely deliver a white list of certificates to be used for the session's HTTPS connections.

Protect On Q also prevents information loss by limiting the ability to copy, print or save browser-delivered information. There's no need to download, install or upgrade software, which reduces help-desk calls and IT workload. Everything to protect your data is delivered on the fly when customers log in. And no software or resident data is left behind when they log out. With Protect On Q, you get the security you need to protect your business, and users benefit from a simplified and automatically secured browser session.

**Quarri MyProtect™: Secure any browser session, anywhere.**

MyProtect is a simple, free service from Quarri that allows users to securely and privately surf the Internet. MyProtect is easily launched from any PC-based browser, and instantly provides a temporary security barrier to keep unauthorized users and applications from stealing information from your session.

After a one-time registration, MyProtect can be accessed anytime, anywhere because you never have to install or update any software. Simply sign on to the MyProtect site and use our secure browser for your web session. MyProtect can be launched from any PC, including your home computer, office laptop, a friend's PC or a kiosk at an airport flight lounge or hotel business center.

**Banking on security: A financial success story**

A top tier international investment bank discovered that users with access to customer data through a web application were copying this information and saving it to a local PC or USB drive. Once the data was extruded, the bank had no way of knowing where it went or how it was used — a major security breach. To prevent further data theft, the bank needed a way to allow authorized users to view the data they needed to do their job, but prevent them from copying or saving any information.

Protect On Q was exactly what they needed. By delivering their applications in an armored browser, users can no longer extrude or otherwise copy and save data to an external drive. As a result, the bank's financial and customer data is far more secure, and the company is looking to expand its security strategy with additional Quaresso applications.

**About Quarri**

Quarri is a leading provider of on demand web browser security solutions that secure information and content at the endpoint. Our products give enterprises the ability to extend security controls temporarily to web browser sessions, providing information protection and data leakage prevention wherever your users are. Quarri is a privately held, investor-backed corporation based in Austin, Texas. For more information, visit [www.quaresso.com](http://www.quaresso.com).

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

1.866.248.3990 US  
+1.512.590.7731  
+1.512.777.5005 Fax

info@quarri.com  
www.quarri.com

<sup>1</sup>Jackson Higgins, Kelly. "You're Always Just Two Clicks Away from Malware." Dark Reading, Sept. 28, 2010.

<sup>2</sup>Blue Coat Web Security Report, 2009.