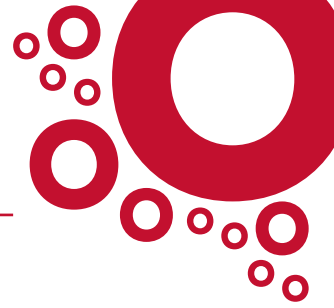


Simple and Secure: PoQ (Protect on Q)



Managed or in the Cloud

LET'S FACE IT:

Creating a safe browsing environment is a fundamental challenge in today's business. With the proliferation of readily available hacking utilities, port scanners and knowledgeable global hackers, attacks typically reserved for servers and data centers have now become a target for the desktop. In fact, billions of dollars are lost every year due to data loss and the expensive cleanup required after an attack spreads cross-company.

That's where PoQ comes in. Protect on Q protects your web resources and provides critical IT services and key components to support simple and secure access to your web-enabled enterprise.

Secure Online Banking

Typically banks offer their customers online financial services to process their transactions 'securely' over the Internet. The bank, however, does not have any way to protect the security status of the remote user, which is heavily dependent upon the user's technical abilities and knowledge. With PoQ, the user can connect to his or her bank's website in an entirely secure session, which is immediately purged upon exiting the browser.

Secure Email & Collaboration

Secure webmail is another service frequently used by employees or contractors in the field. Even if communication over the webmail server is secure, the browser used to send/receive the mail is the easiest point of attack for hacking or a man-in-the-middle attack.

Data Leakage Protection

PoQ enforces the internal security of clients through the prevention of actively copying sensitive data (customer information, employee information, contracts, etc.) over the Internet.

PoQ is an armored browser, featuring a security layer around the conventional browser, which provides an extra level of protection. The armored browser is opened on-the-fly for each individual browser session and leaves no discernable trace on the computer. Neither admin rights nor client installation is required as the software is downloaded on demand each time a secured session is launched.



wizlynx group

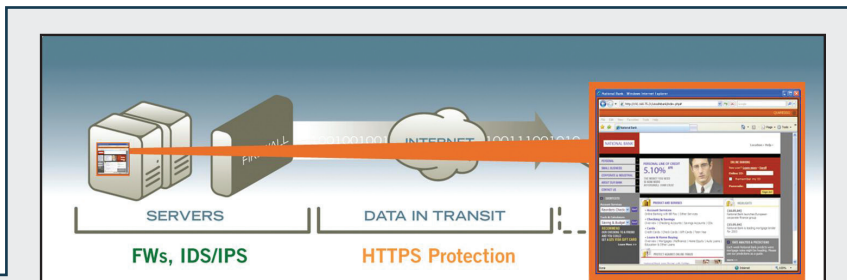
Wizlynx, Inc.
1 McCain Court
Flanders, NJ 07836
USA

Tel +1 973 927 3524
Fax +1 775 997 0720

www.wizlynxgroup.com

OVERVIEW

Quaresso Protect on Q is the only ondemand web security solution to enable web sites to control and protect users' browser sessions - without client software management.



KEY FEATURES

- ▶ Armored browser delivered on-the-fly by website
- ▶ Site-specific security policy
- ▶ Broad array of heuristics and whitelist-based malware defenses
- ▶ Browser data leakage prevention and auditing
- ▶ On-demand, zero impact, dissolvable security agent

PRODUCT BENEFITS

- ▶ Extends websites' security to browsers, without the hassle of managing client software
- ▶ Provides zero-hour protection from malware compromising credentials and session data
- ▶ Mitigates cross-site scripting and other browser redirection attacks
- ▶ Prevents data leakage by encrypting files and restricting local save/print/copy/forward operations
- ▶ Zero installation, update or software maintenance

Your Security Challenge

Convenient, "anytime, anywhere" access has driven explosive growth in online services, from electronic banking and enterprise collaboration to insurance 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 malware attacks and data leakage, targeted by a **multi-billion dollar** professional malware industry. Even worse, the browser is a vector for many attacks on web sites themselves.

Compounding the problem, the web access model means that web sites typically don't own or manage connecting PCs. Sensitive data must be delivered blindly to desktops that site owners can't control, or even validate. User behavior is unpredictable, and any variety of security tools may be present. Regardless of the investment in server-side security and SSL encryption, data is increasingly vulnerable - and increasingly compromised - at the endpoint. But how can you secure the browser without costly, cumbersome endpoint software deployments that ruin the access model?

The Protect on Q Solution

Fortunately, there's now a solution which allows web site owners to extend customized, site-specific protection of sensitive data out to the endpoint. With no user effort or software installation, Quaresso's revolutionary Protect on Q defends user credentials and web session data from theft or data leakage. Protect on Q's "armored browser" shields sensitive data from key loggers, session hijacking, cache miners, and other malware, while blocking inbound attacks as well. To prevent data leakage, Protect on Q enables web applications 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 it is completely cleaned up at the end of a browser session. There are never any signature downloads, software updates, client maintenance costs or administration headaches.

wizlynx group

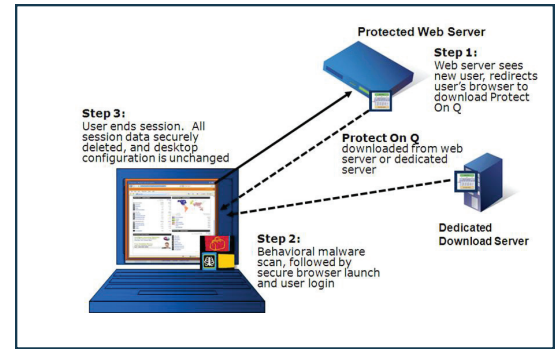
Wizlynx, Inc.
1 McCain Court
Flanders, NJ 07836
USA

Tel +1 973 927 3524
Fax +1 775 997 0720

www.wizlynxgroup.com

How Protect on Q Works

Protect on Q is a software solution which delivers an on-demand security agent, the Protect on Q Enforcer, to the user desktop and protects the browser. Using the Protect on Q management console, an administrator defines granular, application-specific policy settings. These settings are packaged with the binary Enforcer components and placed on a provisioning server for subsequent download. The provisioning server can be the web application server or a remote standalone server. Via simple modifications to the application login page, a check is made to ensure that users are running Protect on Q before they log in. If they are not, a web services call triggers an automatic download of the Enforcer from the provisioning server to the user's desktop and a new, secured, visually distinct browser instance is launched. 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 Enforcer exits and cleans itself up, leaving behind no remnants or modifications to the user's desktop - unlike competitive solutions which leave behind software packages, browser toolbars and system changes which can interfere with normal browser behavior.



Protect on Q's Enforcer

Protect on Q's Enforcer launches a visually distinct, hardened instance of Internet Explorer. Enforcer code runs within this armored browser to control and enforce the Protect on Q policy that is defined by the website's administrator. Based on proven, patent-pending technologies that enable wide-ranging security controls, and combined with "anytime, anywhere" access, the Enforcer has a small footprint and is delivered on the fly using standard web technologies like HTTPS, Java or ActiveX. The Enforcer lasts only as long as the web application session. Once the user closes the session, the Enforcer exits with no permanent desktop modifications, thus providing client-side security without the overhead and expense of managing client software.

The User Experience

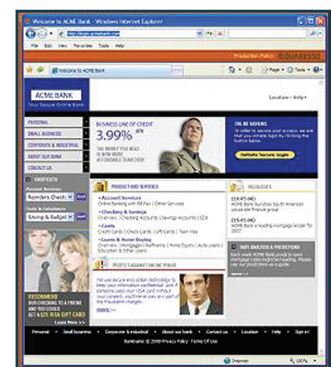
Despite the advanced security features being applied, the user experience is very straightforward and friendly. The user does not have to learn anything new or go through any extra steps such as software installation or updating. After a few seconds for initial download and launch, there is no degradation in performance or adverse user impact. The armored browser's visual elements such as the border, toolbar, logo and messaging are also customizable via the Protect on Q security policy.

Managing Protect on Q

A web-based interface is used to manage Protect on Q. In addition to building the security policies and pushing them to the provisioning servers, the management console offers an embedded test mode, which allows sites to evaluate the Enforcer policy behavior prior to deployment on production systems. Protect on Q provides centralized logging from the armored browsers to enterprise log servers, using standard W3C log formats and HTTPS POSTs.

Zero-Hour Malware Defense

Throughout the session, Protect on Q scans running processes, using patented run-time behavioral analytics to identify key logging and framegrabbing applications. Once identified, policy-defined actions can be taken to block availability of keyboard inputs and screen captures to the Protect on Q controlled applications.



wizlynx group

Wizlynx, Inc.
1 McCain Court
Flanders, NJ 07836
USA

Tel +1 973 927 3524
Fax +1 775 997 0720

www.wizlynxgroup.com

Browser Process Integrity

As Protect on Q's Enforcer launches the armored browser, it screens and filters potentially hostile browser add-ons (e.g., toolbars and plug-ins). Website owners can also specify which, if any, add-ons are required by its web applications; All other add-ons are blocked in the armored browser session.

Browser Networking Controls

Protect on Q enables websites to restrict the armored browser's network connections to specific destinations, including hosts or domains. Sites can use this feature to minimize browser redirection attacks and XSS attacks.

Hostname Resolution Bypass

To defeat malware that utilizes DNS or hostname tampering as part of its attack on a web session, Protect on Q enables websites to deliver a host table with the armored browser. This enables the protected session to bypass this attack vector. Additionally, the armored browser can bypass local hostname file resolution to prevent poisoning attacks.

Browser Session Data Privacy

All data files created within the armored browser session are encrypted in real time using 256-bit RC4. Browser cache files, cookies, password store and history are encrypted to protect from access and compromise by other applications. When the session is over, all session data is overwritten and then deleted.

HTTPS Certificate Defenses

To defeat poisoning a browser's certificate store, Protect on Q enables websites to securely deliver a white list of certificates to be used for the session's HTTPS connections. To control social engineering of users by hostile HTTPS proxies, Protect on Q enables websites to specify whether users can override certificate errors (e.g., expired or mismatched certs).

Content Information Controls

Websites, such as web mail servers, deliver content as rendered HTML as well as common file formats such as Adobe Acrobat and Microsoft Office. Protect on Q's information controls enable websites to control whether content delivered can be "extracted" out of the browser and onto the desktop via such operations as print, copy, save, clip boarding and print-screens. These controls extend beyond the browser to applications such as Adobe Acrobat and Microsoft Office.

ENFORCER AGENT SYSTEM REQUIREMENTS

- ▶ 32-bit versions of Windows XP, Vista, or 7
- ▶ IE6, IE7, or IE8 installed
- ▶ JavaScript enabled
- ▶ Sun JRE 1.4.2+ or
- ▶ ActiveX enabled
- ▶ 10MB disk space
- ▶ 256MB RAM

MANAGEMENT TOOLS

- ▶ **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

WIZLYNX GROUP, IN PARTNERSHIP WITH
QUARESSO, OFFERS PoQ (PROTECT ON Q) AS A
FIRST IN BROWSER AND APPLICATION SECURITY.

ON THE MARKET FOR ONLY 12 MONTHS, PoQ
HAS BEEN DEPLOYED IN SEVERAL LARGE
MULTINATIONAL AND ACADEMIC INSTITUTIONS
REQUIRING A COST EFFECTIVE AND SECURE
SOLUTION THAT COULD BE IMPLEMENTED
GLOBALLY TO PROTECT THE INTELLECTUAL ASSETS
AND PRIVACY OF THE COMPANY.



wizlynx group

Wizlynx, Inc.
1 McCain Court
Flanders, NJ 07836
USA

Tel +1 973 927 3524
Fax +1 775 997 0720

www.wizlynxgroup.com



wizlynx group

Wizlynx, Inc.
1 McCain Court
Flanders, NJ 07836
USA

Tel +1 973 927 3524
Fax +1 775 997 0720

www.wizlynxgroup.com