



# Garrison Trust Qualified Browsing

## Simplifying Hardware-Enforced, Cloud-Hosted Browser Security



### Browser Security Today: Heavy on Simplicity, Light on Security

The Internet is no longer just the world's largest source of information. As cloud-first and cloud-native architectures become more common, the Internet and the web browser have also become places to run applications that were once the purview of dedicated software and store sensitive data that was once kept in on-premise servers.

It should come as no surprise that adversaries have seen the increasing versatility of the browser and sensitivity of the data that it accesses as an opportunity. In 2023 alone, **8 high or critical severity CVEs** were identified in the backbone of two of the three major web browsers. **Phishing attacks** and resulting credential theft and **malware** – including debilitating ransomware and IP-stealing spyware – have become commonplace.

But securing the browser has become increasingly difficult:

- Proxy and SWG categorization databases can be **outdated or tricked**
- “Known good” website security can be circumvented by **targeted attacks**
- Deny-by-default configurations are nearly impossible due to a spiderweb of **dependent web resources**
- Endpoint and network detection technologies often miss nation-state and sophisticated cyber criminals’ **zero day attacks**
- Phishing simulations are becoming ineffective, demoralizing, and time-consuming with advances in **AI-powered spearphishing**

## Simplify and Secure with Garrison Trust Qualified Browsing

Enter Garrison **Trust Qualified Browsing**, the newest solution from a company known for innovation in cybersecurity isolation solutions that are trusted by the most security-minded organizations in government and the private sector. With Trust Qualified Browsing, Garrison provides organizations with a suite of tools designed to ensure that only your company's **most trusted web apps** can run the system-level code that makes web browsers so risky. At the same time, Trust Qualified Browsing provides your employees access to the wealth of information on the open Internet – information they need to do business – while using our patented and trusted cloud-hosted, hardware-enforced technology to **remove the risk of malicious webcode** from your systems. Finally, we provide your administrators the tools they need to **optimize the level of risk** they're taking with the sites and webapps that are allowed to run natively.

## The Garrison Trust Qualified Browsing Suite

Garrison's Trust Qualified Browsing suite builds upon the security of Garrison's best-in-class, hardware-enforced ULTRA® remote browsing cloud service. We've added Garrison's new Citadel Browser and extension to provide your security teams with browsing telemetry and ensure that your employees have access to browse enterprise-approved sites natively, and our first of its kind Garrison Trust Boundary Engine, a data-driven SaaS application that allows your team to analyze enterprise browsing habits and modify your Trust List accordingly – both by learning the sites employees use, assessing them, and adding them to the list, and by highlighting trusted sites that are no longer being visited so you can reduce your risk profile accordingly.



### **Enable your Enterprise** *with the Garrison Citadel Browser or Extension*

- Automatically redirects non-trusted browsing to a codeless browsing session
- Empowers your browser to understand and render all dependencies necessary for trusted domains
- Continuously syncs telemetry and Trust List to comply with enterprise risk decisions



### **Secure your Network** *with the Garrison ULTRA Cloud Service*

- Secure open Internet browsing with technology trusted by US and UK governments
- Renders all sites outside the trust list into codeless, interactive video streams, removing malware risk
- Provides a near-native browsing experience with the help of cloud-hosted video compression



### **Optimize your Boundary** *with the Garrison Trust Boundary Engine*

- Learns your organization's browsing patterns and enables easy Trust List creation
- Centralizes enforcement of the Trust List on Citadel-powered endpoints
- Manage requests for additions to the Trust List or remove sites that are no longer in use

## Learn More about Trust Qualified Browsing Today

If you're excited about the prospect of dramatically limiting your browser attack surface while empowering your workforce with the wealth of information available on the open Internet, visit us for more information and our full [Trust Qualified Browsing white paper](#) – or sign up now for access to our [Trust Qualified Browsing early access program](#), where you can participate in our beta and have the opportunity to shape the development of this powerful tool.