GARRISON

Garrison ULTRA®

## Where Enablement Meets Security

The Internet is a Necessary Risk

The continued proliferation of malware and phishing attacks, compounded by an increasingly uncertain geopolitical cybersecurity climate and AI/ML algorithms that will make signature detection increasingly difficult, makes the Internet a scary place. But the need for constant innovation and workforce enablement makes Internet access a requirement for competitive intelligence, commerce, threat research, and enabling the workforce to keep an eye on their personal lives.

That's why Garrison has spent 9 years developing the hardware-based technologies that will protect your workforce from online threats while enabling them to access unknown or even known malicious web content to continue pushing the envelope in innovation and competition.

Software and Code are Easy to Hack
Hardware and Pixels Aren't

Garrison secures your employees' Internet access by eliminating the reliance on detection-based algorithms from endpoints to the network edge and instead applying four hardware security (hardsec) guarantees to your company's use of the Internet:
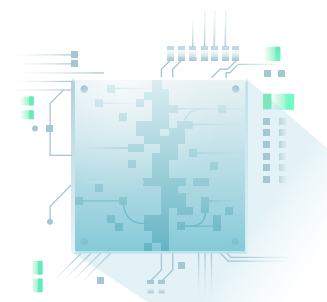
Present pixels and waveforms, not code
Advanced exploits can bypass risk reduction algorithms. Instead of taking chances reducing risk via code, our pixel-pushing technology ensures that only an audio/video stream of web browsing is presented.

Isolate processing on a separate system
Containerisation and virtualisation can be compromised. We provision each active user with two physically separate systems for browsing – one to execute risky code, and one to receive the pixels and waveforms before compressing them for streaming to the end user. Our Secure Reboot technology ensures that no malware can persist between sessions.

Transform content with fixed-function hardware
Adversaries can develop exploits to subvert software. Instead of engaging in a patch race, we host fixed-function hardware in our data centers to ensure that adversaries can't subvert our software to compromise your web browsing.

Render 100% of presented content
A URL that's safe one day may contain malicious content the next. Instead of relying on lists of known-good or known-bad URLs, we render safe all traffic sent to our ULTRA cloud servers.

Tested and Trusted by the
World's Most Secure Networks

Don't take our word for it: the technology underpinning ULTRA has been deployed across the US and UK's most secure networks and is in use by more than 75,000 users as the Lloyd's Banking Group's secure browsing solution – and now we're bringing it to the cloud with a flexible licensing model. With our concurrent session licensing, you only pay for the capacity you need, rather than users who will only be browsing part of the time.

Click here to read the **Lloyds Banking Group Case Study**

The only real way to evaluate us, however, is to try it for yourself – contact us to set up a consultation with a hardsec expert and learn more about our ULTRA solution: info@garrison.com