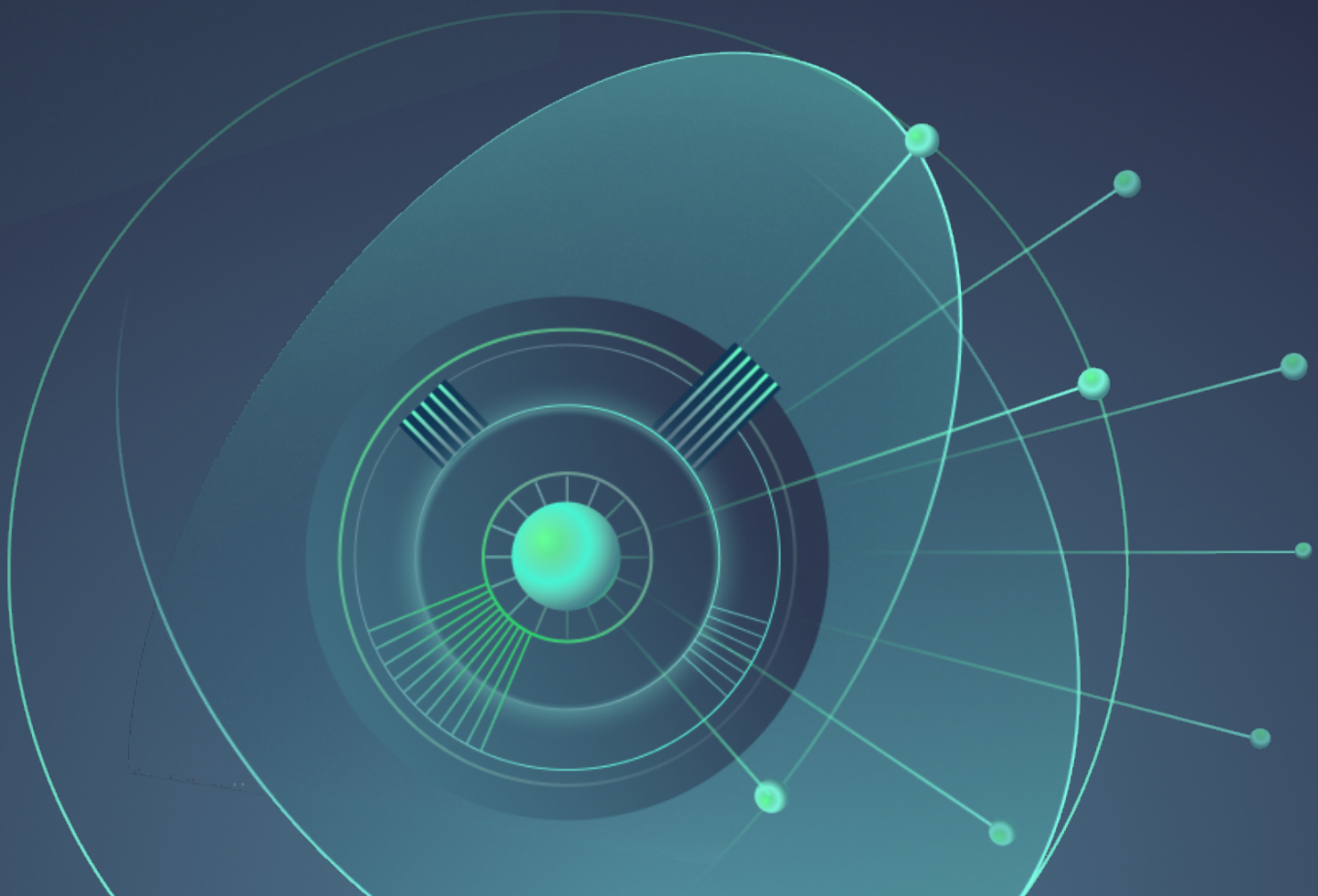
GARRISON

# Web Isolation Audit Guide

What you need to know about auditing the use of Web Isolation to secure users as they browse the web



If you're one of the growing number of IT Auditors reviewing the use of Web Isolation to protect an organization from threats like ransomware and phishing, you're far from alone. The specific Web Isolation technology being used and its configuration can have implications for the level of security achieved.

It's easy to see why Web Isolation (also known as Remote Browser Isolation) is such a critical technology. Threats on public web pages are growing and, while firewalls, proxies, user training, web filters, and other tools can help, there is always still a risk that malicious code can make its way onto your endpoints.

This guide tells you all you need to know about the different technologies used to deliver Web Isolation, and the questions to ask to assist you in performing an IT Audit of an enterprise that may or may not be using a Web Isolation solution.

# What is Web Isolation?

**Web Isolation (or Remote Browser Isolation) solutions protect users from ransomware, phishing and other web-based threats while they browse the web or click links in emails. It's often used to secure vulnerable or high-risk users, such as senior management, system administrators, or anyone whose job might involve visiting untrusted sites.**

**Web Isolation solutions effectively remove the browser from the user's device, isolating that user from any risks on the web. Different solutions then use different approaches to relay the browsing session back to the user.**

Applied correctly, Web Isolation can potentially remove a whole class of cyber threat – which is why so many organizations are using or exploring it, whether for high-risk users and sites or across the enterprise. However, not all Web Isolation tools use the same techniques and technologies.

Full isolation technologies use pixel-pushing techniques to offer robust security and high levels of compatibility. Partial isolation through transcoding uses different isolation techniques that traditionally offer lower costs and bandwidth requirements.

Moreover, new hardware-based pixel-pushing (such as Garrison ULTRA®) allows full isolation solutions to offer a powerful mix of security and usability alongside lower costs and management overheads.

This guide explores the differences between these competing Web Isolation technologies and gives you the information you need to perform an IT Audit of the use or non-use of Web Isolation in your organization.

# Why are organizations adopting Web Isolation?

Web browsing poses a significant risk to any security-conscious enterprise. And as phishing scams and ransomware become increasingly sophisticated, the threat to users only grows.

For instance, Verizon's latest Data Breach Investigations Report found that 36% of cyber security breaches involve phishing attacks; 11% more than the previous year[1]. And today, Google Safe Browsing lists just under 2.1 million websites as dangerous[2]. Crucially, Google's list only includes the dangerous websites we know about. The unknown threats could be far greater in number.

Protecting users from the growing ranks of malicious pages is notoriously difficult, as user behavior always includes elements of unpredictable human error. Trying to train users not to click on malicious links or visit dangerous web sites will not be effective in stopping today's sophisticated attacks. It only takes one user to make a mistake and the enterprise could become compromised. You cannot realistically expect all your users to never make a mistake.

There are only a handful of ways to truly secure a user that browses the public internet. You can use a carousel of separate sacrificial devices (and deal with the costs and administrative burden of constantly replacing malware-infested hardware). Alternatively, you can adopt a Web Isolation solution. Any other method, whether it be firewalls, secure web gateways, web filter lists, endpoint protection, or training to educate users, still involves your users directly accessing web pages with their devices – which could present a risk.

Web Isolation avoids these issues entirely by ensuring your users' endpoints never connect to the web page at all. Instead, a remote machine accesses web pages on your users' behalf and delivers a separate, clean version of the web page.

1 https://www.verizon.com/business/en-gb/resources/reports/dbir/
2 https://transparencyreport.google.com/safe-browsing/overview?hl=en_GB&unsafe=dataset:1;series:malwareDetected,phishingDetected;start:1148194800000;end:1612080000000&lu=unsafe

# Full or partial isolation: similar names, very different results

There are two general schools of thought around how to isolate users' web browsing:

**Partial Web Isolation** strips the website code down to a smaller subset of information to remove malicious code or other parts of a website that could be compromised. That data is then reconstructed to better resemble the original website before being sent to the user. This type of process is enabled by transcoding technologies such as DOM remodelling and network vector rendering.

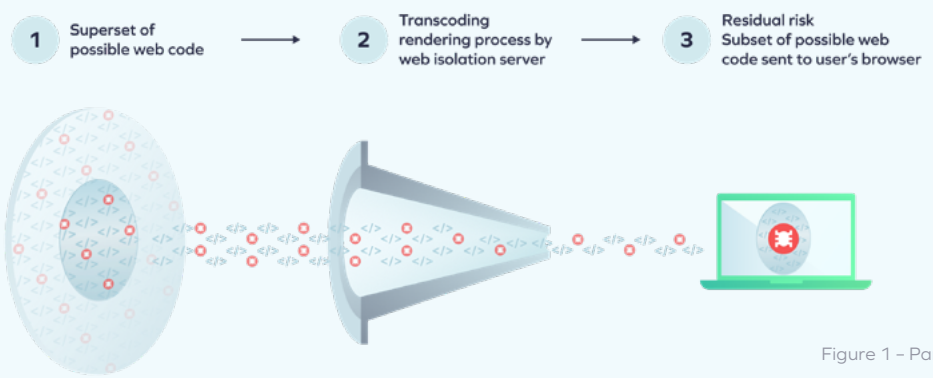



Figure 1 – Partial Web Isolation

**Full Web Isolation** involves completely separating users from the websites they browse. The Web Isolation solution handles the browsing in its entirety and delivers the information to users as a video stream that includes none of the website's original code. This is enabled by a technology called pixel-pushing. Traditionally, video streams are encoded and delivered via software, but more modern solutions use dedicated hardware to improve the user experience and reduce the cost.

Of course, both approaches have the same end goal: delivering a secure web browsing experience. But they offer different results in terms of the web experience users receive, IT management and costs, and – most critically – the level of security provided.

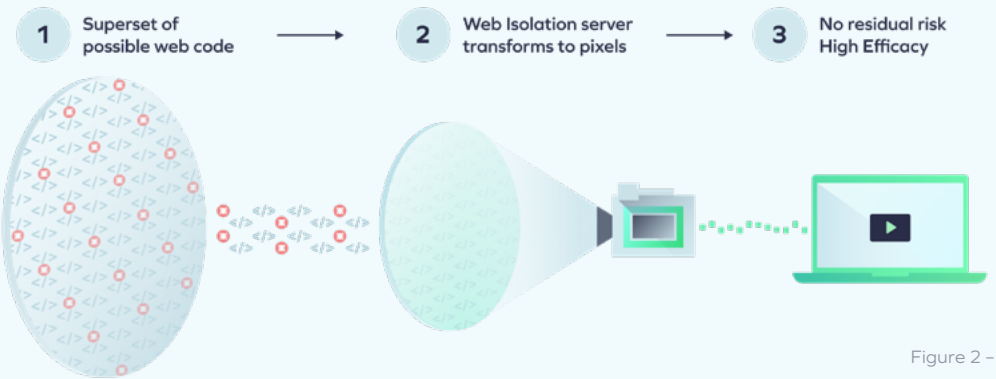



Figure 2 – Full Web Isolation

# How do full and partial Web Isolation compare?

There are four main criteria for judging the quality of a security solution:

- Security
- Usability
- Cost-effectiveness
- IT simplicity

How do full and partial Web Isolation compare across these four points? As IT Auditor you will naturally focus primarily on security. Nevertheless, you will still find it helpful to understand the other criteria.

## Security

Nobody considers Web Isolation technology unless they're serious about securing their key users. The first criteria, then, is what protection the solution offers.

Web Isolation solutions work by keeping the user away from potentially harmful website code. So, when you're considering how effective they are, the main question is what code – if any – still makes it through to the user's device.

### Partial Web Isolation

Because transcoding presents a subset of the original code to users, it's inherently porous. The effectiveness of the security depends on which parts reach the user, and what gets stripped out. You're likely to have questions about these decisions, as they determine the potential for malicious code to slip through the net or for attackers to exploit the site in a new way.

Unfortunately, transcoding is generally a black box: solution providers rarely explain exactly what subset of website code gets used. Security then becomes a matter of trusting the vendor without being able to verify how it works.

### Full Web Isolation

Full isolation technologies like pixel-pushing are inherently non-porous because they prevent users from interacting directly with any website code. All web content is transformed into a harmless video stream of pixels. These Web Isolation technologies therefore offer far more comprehensive security.

### What to look out for:

- Security-conscious enterprises will want to look for the improved protection and transparency that full Web Isolation offers.
- When auditing the use of a partial isolation solution, make sure the provider can offer transparency around how their transcoding works and what website code it lets through to users. Otherwise, the enterprise is incurring an unknown level of risk despite the use of a Web Isolation solution.

# Usability

Web Isolation can have two main impacts on usability:

1. **Incompatibility with websites can break the user experience.**
2. **Sending traffic between the client and the Remote Browser Isolation solution can add latency.**

These are both key issues. If your users don't enjoy their browsing experience, they may try to find a way around your Web Isolation solution – creating new security risks.

## Partial Web Isolation

In some cases, partial isolation technologies offer acceptable latency levels. But this is situation-specific: in many cases latency can be poor and variable, particularly where technologies use protocols that aren't optimized for real-time communication. Transcoding can also create significant compatibility issues. Some kinds of content – like video playback, for example – may not work at all, or only function with a limited set of features.

And as website and plugin developers constantly update their code, transcoding solution providers must continually update their systems to keep pace. When they fall behind, website features (and even entire websites) can stop working, significantly degrading the user experience. Some vendors will be tempted to fix such incompatibilities by allowing the unsupported code to simply pass through—increasing the security risk.

Finally, for some websites, transcoding solutions can be bandwidth-intensive, meaning they don't work well under poor network conditions. This is particularly noticeable on sites where transcoding tricks don't work well. In these cases, providers have to fall back to pixel-pushing – for which their technology is typically not optimized, unlike true pixel-pushing solutions.

## Full Web Isolation

Pixel-pushing technologies avoid compatibility issues as they don't interact with website code – they instead turn the content into a video stream that's sent to the user in real time.

Historically, these streams demanded high bandwidth resulting in significant latency and a degraded browsing experience. This remains true of many software-based pixel-pushing solutions, but new, hardware-based solutions mitigate much of these bandwidth requirements.

Such solutions use specialized hardware to compress and stream video feeds more efficiently to help reduce latency and deliver a seamless browsing experience. And by hosting the solution in the cloud (as in the case of Garrison ULTRA®), enterprises can get the security and usability benefits of modern pixel-pushing without worrying about deploying and maintaining hardware.

## What to look out for:

- Hardware-based pixel-pushing solutions can offer the best balance between latency and compatibility – and the most consistent user experience.
- Many vendors will lock you to pre-set web addresses for their trial period – limiting your ability to test the service in normal browsing conditions. So, when assessing solutions for usability, make sure any demos or trials let you test the service on all websites.
- Ultimately, usability is subjective. The only way to decide which experience your users will enjoy is by testing different solutions.

# Cost-effectiveness

Cost will always be a vital concern when assessing security solutions. If a Web Isolation solution's upfront or ongoing costs are too high, it could limit your ability to scale. And if licensing models are inflexible, it can affect how you decide to roll out and deploy solutions across different user groups. And between the technology license itself, the computing resources, and the bandwidth connectivity costs, there can be a lot to consider here.

## Partial Web Isolation

Different partial isolation solutions will use different transcoding approaches to protect users, so ongoing costs can vary between vendors. While some partial isolation solutions may keep bandwidth requirements down, many rely on transcoding approaches that can be compute-intensive – leading to significant infrastructure requirements and costs.

Vendors will also approach licensing and scalability differently, so it's worth calculating the potential costs if you decide to roll the service out to more users than you initially planned.

## Full Web Isolation

Traditional, software-based pixel-pushing isolation moves significant data volumes, which can be compute and bandwidth-intensive and lead to high operating costs.

But new, hardware-based full isolation solutions significantly reduce those ongoing costs. And cloud solutions running on purpose-built hardware can offer the same benefits without the need to pay for isolation devices upfront.

## What to look out for:

- Hardware-based pixel-pushing solutions can offer lower ongoing costs compared to software-based alternatives or partial Web Isolation.
- Where possible, use a vendor that will offer licensing based on concurrent active sessions instead of per user. This allows more flexibility in how the solution is deployed (for example, the enterprise could have a large group using the solution less frequently or a smaller group of intensive users for a similar cost).

# IT simplicity

Whether it's through initial deployment requirements, or ongoing manageability and integration issues, enterprises want to be sure the Web Isolation tool keeps things simple for technical teams – and doesn't divert IT resources from other essential work.

## Partial Web Isolation

The key issue with transcoding solutions is that many aren't designed to work alongside existing proxies and secure web gateways. And those that claim interoperability with such security tools may still need extensive configuration to ensure everything integrates and works together correctly.

Even when a solution is properly configured and integrated, the low compatibility of transcoding-based solutions can put pressure on IT to answer a greater volume of support tickets, as users encounter websites that don't work. This may put pressure on IT to bypass the Web Isolation solution causing security risks.

## Full Web Isolation

Unlike transcoding approaches, full Web Isolation doesn't need to modify entire chunks of website code to deliver pages to users. While there's still a risk of incompatibility, there's a much lower chance of new updates to websites breaking the underlying method of Web Isolation. And that means there's less need to constantly install update patches.

And depending on the solution vendor, the upfront deployment requirements can also be easier than with partial isolation solutions.

Hardware-based alternatives vary in IT complexity, but on-premises options require upfront installation and deployment. By comparison, hardware-based solutions hosted in the cloud don't have this need – although, like any solution, some configuration is still required to ensure interoperability with proxies and other security tools.

## What to look out for:

- In general, full isolation solutions are more consistently compatible with websites and more readily designed to integrate with other security tools – so they demand less of the IT department.
- Some organizations will want the additional control of deploying their Web Isolation tools on premises.
- Those that don't have such stringent requirements can further reduce IT management burden by opting for a hardware solution hosted in the cloud.
- But think carefully about how the Web Isolation solution will integrate with other security solutions, such as the proxy and secure web gateway.

# Full Web Isolation and full security – without the drawbacks

While partial and full Web Isolation technologies each have their pros and cons, there's no doubt that organizations that put security first are likely to consider the latter.

Some firms may be willing to explore a less secure solution if they believe it will offer other usability, cost and management overhead benefits.

However, for most security-conscious enterprises, hardware-accelerated, full isolation – delivered through the cloud – offers the best combination of security, user experience, IT management, and cost.

# Questions for IT Auditors to ask

After reading the previous sections, you should now have a good understanding of the different Web Isolation methodologies and their pros and cons. The questions and considerations in the table below can assist you in performing an IT Audit of an enterprise that is or is not using a Web Isolation solution. These should assist you as you develop your overall IT Audit plan.

| Question | Consideration |
|---|---|
| **Are you using a full or partial Web Isolation solution? Or no such solution?** | Go to the appropriate section depending on the answers. |

## If no Web Isolation solution is in place

| | |
|---|---|
| **Have you identified high risk users?** | High risk users should include those who are administrators or have access to sensitive systems or data. |
| **Have you determined the risk to the enterprise if any user's endpoint is compromised?** | Attackers may be able to escalate their privileges or spread malware once they get access to a single endpoint in your network. |
| **Is the enterprise heavily relying on user training to stop phishing attacks?** | If so, the enterprise is likely incurring an unacceptable risk. Phishing remains a top vector for successful attacks, including ransomware. |
| **Is the enterprise relying on endpoint protection and browser security to protect against phishing and browsing dangerous websites?** | If so, the enterprise is likely incurring an unacceptable risk. Attackers regularly test their malicious code against the endpoint protection systems and browsers on the market. |
| **How are you ensuring that users don't browse dangerous websites?** | If you overly restrict users from browsing, they may not be able to do their jobs. Allowing users to browse potentially dangerous sites opens the enterprise up to the risk of attack, including ransomware. |

## If you are using a Partial Web Isolation Solution (Transcoding or Rendering method)

| | |
|---|---|
| **Do you understand exactly how the solution transcodes website code into a subset of website code?** | Many vendors will not share this information. |
| **Do you have a list of the subset of website code?** | Many vendors will not share this information. If you don't have this, you have no way to verify how secure the solution is. |
| **Have you, a pentester, or a trusted 3rd party expert verified the subset of website code to ensure that no malicious code could leak through?** | Validating this will require skill, time and an understanding of how malicious code could be transmitted via a website. |
| **What assurance do you have the subset of website code will never allow potentially dangerous code to be transmitted?** | Need to understand how the vendor keeps the solution updated and compatible. What assurances do you have that no shortcuts will be taken in the future that could compromise security? |

## If you are using a Full Web Isolation Solution (Pixel-pushing method)

| | |
|---|---|
| **Is the solution available either on-premise or in the cloud?** | Allows the enterprise more flexibility if both deployment models are available. |
| **Does the solution use specialized Web Isolation Hardware?** | Adds additional security and performance advantages. See hardware section. |
| **If a software-only architecture, does it ensure that only a video stream of pixels will be transmitted to the user's endpoint?** | Even the most sophisticated attacker should not have a way to send code through the Web Isolation solution to the endpoint. |

## Specialized Web Isolation hardware

| | |
|---|---|
| **Does the specialized hardware use Hardsec?** | Provides additional trust in the security of the hardware architecture and implementation. |
| **Do you have an easy-to-understand description of the hardware architecture?** | Reliable vendors will describe in sufficient detail how the hardware architecture works. |
| **Does the hardware architecture ensure that only a video stream of pixels will be transmitted to the user's endpoint?** | Even the most sophisticated attacker should not have a way to send code through the Web Isolation solution to the endpoint. |
| **Have any government security experts reviewed the architecture?** | Robust security solutions should be able to withstand the scrutiny and challenges of demanding security environments. |

## Cloud-based Web Isolation solutions

| | |
|---|---|
| **What is the control plane architecture of the solution?** | The cloud architecture of the solution should readily demonstrate robust security. |
| **Does the solution have strong multi-tenant architecture and controls?** | A tenant must never be able to see another tenant's data or even the presence of another tenant. Moreover, a tenant must not be able to leverage the architecture as a pivot point to attack another tenant. |
| **Does the vendor have or plan to have the appropriate SOC2 certification?** | Just piggy backing on the cloud provider's SOC2 certification is not good enough. The vendor needs their own. |

## Web Isolation policy

| | |
|---|---|
| **What is the policy for what is pushed through the Web Isolation solution?** | |
| **Which users does the solution apply to?** | Should at least ensure that all high-risk users go through the Web Isolation solution. |
| **Which websites does the solution apply to?** | Some organizations may allow listed sites to not go through Web Isolation. This can save bandwidth and processing. |
| **What risk is incurred by any users or websites not using the solution?** | Are you comfortable with this remaining risk? |
| **How are policy decisions made and maintained?** | Determine if the way that the policy is determined and kept up to date incurs any additional risk. |
| **Are all policy and configuration changes logged in an audit trail?** | Standard security requirement. |
| **Review some of the audit trail see if the security policy has been followed** | Performing a spot check on the audit trail provides additional assurance that the solution has been operated according to policy. |
| **Does the audit trail indicate that the solution was frequently turned on and off either entirely or for certain users or websites?** | This indicates that the solution may be having compatibility or performance issues periodically requiring it to be turned off. The result is increased security risk. |

## General Security Questions

| | |
|---|---|
| **How are the Web Isolation administration accounts managed and secured?** | Look for use of multi-factor authentication, no shared admin accounts, etc. |
| **Does the Web Isolation server start new clean sessions?** | New browsing sessions should not have artifacts or potentially malicious code left over from previous sessions. |
| **Does the solution allow the user to download files and store them in an isolated location and display them through the Web Isolation solution?** | Allows a user to securely read and interact with downloaded files such as PDFs without posing a risk to the user's endpoint. |
| **Does the free trial of the solution have a restricted set of websites that can be browsed?** | If so, this indicates that the solution vendor is nervous about potential customers or even attackers testing their solution against malicious websites—a sign that the underlying architecture has known security drawbacks. |
| **Is there any aspect of the Web Isolation solution architecture and methodology that is treated as a black box with no explanation?** | If so, this indicates that the solution vendor is likely relying on security by obscurity and that the architecture and methodology will not withstand scrutiny. The result is that the enterprise is likely incurring risk it doesn't know about. |

**Email** info@garrison.com
**UK Telephone** +44 (0) 203 890 4504
**US Telephone** +1 (646) 690-8824



**www.garrison.com**

© Garrison Technology Ltd 2022

CD00000652 - April 2022