GARRISON

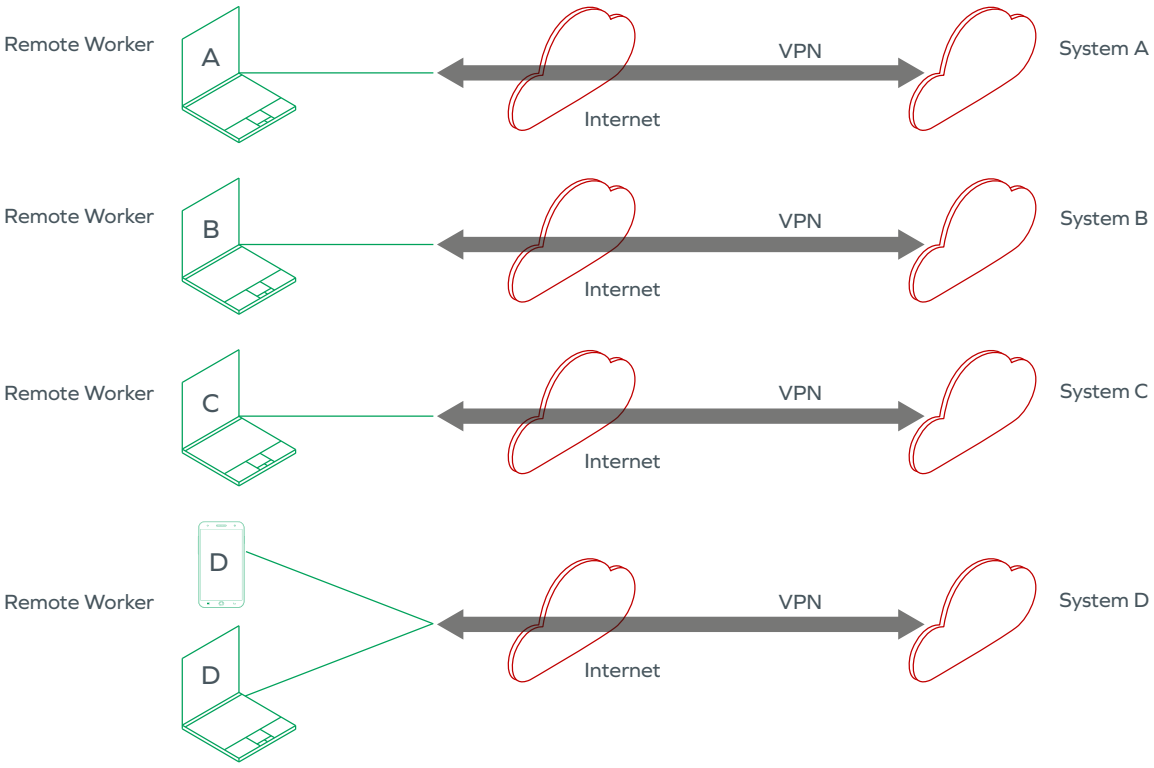
Remote working with classified systems

How Garrison can help

Traditionally, access to classified data has been limited to secure facilities. But today, remote working is a critical requirement. How can government organizations mitigate the risks to sensitive data that remote working threatens to introduce?

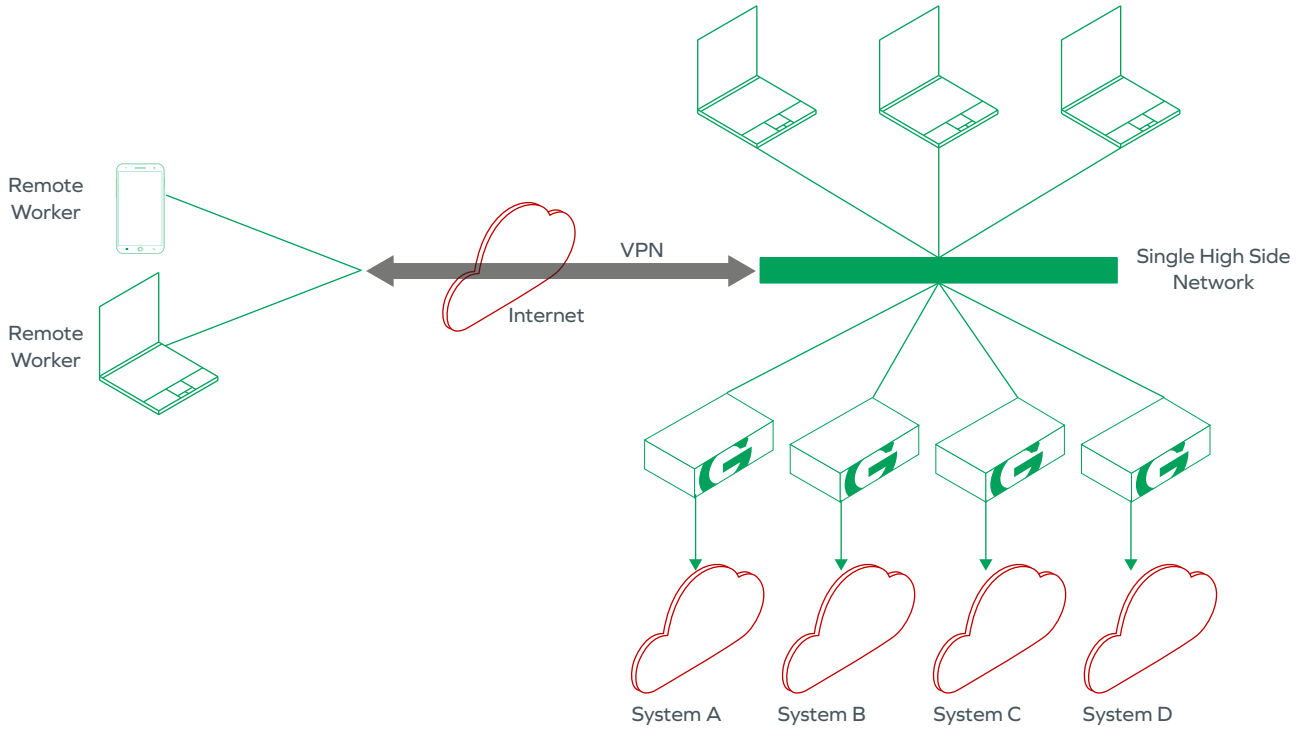
A single pane of glass for secure remote devices

Remote workers can be provided with a locked-down secure workstation or mobile device that connects to classified systems via VPN – using a high-assurance hardware crypto device or using suitably assured commercial cryptography[1].



But in the secure facility, workers will often have access to multiple workstations, each used to access different sensitive systems. This can be operationally painful in an office environment, but in a remote working environment it is wholly impractical. Garrison can allow a remote device to act as a single pane of glass – providing access via a "browse down" model to multiple sensitive systems while maintaining hardware-level isolation between those systems.

1 In the context of the NSA's Commercial Solutions for Classified Program (CSfC) note that Garrison provides application-level cryptography between the remote device and the core. In most circumstances it should therefore only be necessary to provide one layer of 3rd party VPN, with Garrison providing the required second layer of independent cryptography.



Avoiding persistent data on remote devices

A remote device will always be riskier than one in a secure facility: even if the device is heavily locked down with excellent cryptography and strong access controls, the risk of physical theft is inherently higher. If a device is taken, access rights to secure systems can be revoked, but any data that has persisted on the device is at risk.

With a "browse across" model, Garrison can enable locked-down workstations or mobile devices to act as the ultimate thin clients: devices that users can use to interact with classified data and systems, but without introducing the risks of persistence. By ensuring that all classified data is converted to a transient video stream, Garrison minimises the risks that even inadvertently cached data finds its way into the hands of adversaries.

Preventing download and upload

An attacker may seek to use a compromised remote device to force the download of quantities of data or files from the secure systems. Adopting a "full stack protocol break" between the remote device and the secure systems eliminates such a risk.

As with the non-persistent data model above, Garrison prevents downloads from the secure systems and the protective monitoring already in place can alert operators to unusual sequences of requests to view lots of records.

Such a protocol break also prevents malicious data or code from being uploaded to the secure systems. Implementing technology that rigorously enforces and audits key presses and mouse movements will strongly mitigate the risk of an attacker "keying" such content into the secure systems.

Minimising the risks of BYOD

It will always be safest to restrict access to classified data to locked-down government-supplied devices, but that may not always be practical. When it is necessary to provide access from third party devices (as with BYOD) it becomes critical to ensure both that data does not persist on those devices, and to mitigate the risk that if compromised, the remote devices might attack the classified core.

With a "browse up" model, Garrison not only minimises the risks of data persistence but also massively constrains the attack surface for the classified core. Devices can interact with the core using only keyboard presses and mouse movements, each of which can be logged for analytics and forensics.

About Garrison

Garrison provides hardware-level isolation that is in use today to provide access from classified devices to the Internet, and to provide access from higher-classification devices to lower-classification systems. Garrison ensures – at the hardware level – that all lower-classification data is converted to a stream of raw bitmap data to prevent attacks on the device, and allows interaction via keyboard and mouse (or touch, for mobile devices) only.

In some cases, Garrison provides cross-domain access to web content – for example, allowing users of classified devices to browse the World Wide Web over the Internet. But in many other cases, Garrison is used to provide access to VDI platforms – allowing users of high-classification workstations to work interactively on lower-classification Windows or Linux desktops.

Devices can operate multiple Garrison sessions in parallel, allowing true single pane of glass operation for those whose work requires interaction with a complex set of classified systems each of which must be kept isolated from each other.

If you'd like to learn more about how Garrison can help to enable secure remote working, get in touch.

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

www.garrison.com

CD00000404v1.0-US - Sept 2020