REPORT REPRINT

Garrison draws a hard[ware] line in the sand for securing web activity

APRIL 9 2019

By Fernando Montenegro

In the never-ending trade-off between security and usability, techniques for providing secure browsing via isolation have become more popular. In many cases, the potentially malicious content is rendered in a separate environment and only 'good' content makes its way to the user. Garrison offers an interesting browsing isolation approach that uses not only remote browsing, but hardware-enforced isolation between components.

Introduction

Modern security teams understand well that protecting their users' browsing activities is essential. This includes protection against malicious downloads, phishing attempts and more. Browser isolation is one of the many techniques used in this context. There are different approaches to isolation, from on-device virtualization to remote execution, each with their benefits and drawbacks. Invariably, however, it's a trade-off between usability and security.

UK-based Garrison has designed a combined hardware-and-software approach to isolation that places a significant premium on achieving high levels of isolation while maintaining usability. This approach is usually favored with high-security customers and the company is looking to expand further.

451 TAKE

Organizations often point to user behavior as a key security concern and it is in accessing external resources via browsing that this is most evident. We have seen interest in different approaches to handling the issue, and browser isolation is one of those approaches.

Garrison is one of the vendors in this space, coming to market with a hardware-based approach that places a premium on security. Garrison seems well attuned to how its current customers need secure browsing as part of a broader security architecture. The company's message about focusing on secure browsing specifically and tying to other components such as policy definition, file transfer and DLP is clear and welcome.

As the company pursues a broader set of commercial clients, however, it will have to contend with two key challenges: can Garrison simplify the integration and use of its platform (the upcoming cloud service may help here) and, importantly, can it clearly demonstrate the benefits of its approach to a wide enough set of prospects?

Context

Garrison Technology is a UK-based company founded by David Garfield and Henry Harrison in 2014. The company currently employs roughly 70 people, with a strong presence in the UK and field sales in North America. Both Garfield, now CEO, and Harrison, CTO, have had previous executive experience at Detica, which was then acquired by BAE Systems.

Garrison has raised about £34.9m ($50m) across two funding rounds. The company raised a series B round of £22.9m in October 2018, with European investor Dawn Capital leading the round and participation from NM Capital, IP Group and Business Growth Fund. Post-money valuation is estimated at £123m.

451 Research estimates current revenue to be in the £8-10m range.

Strategy

Garrison has approached isolation by navigating the balance between security and functionality but with a very clear message of when in doubt, security is the key differentiator. This principle permeates several follow-up business and technology choices.

The company is diligent about identifying the right type of customer that may be receptive to its message. At present, it focuses on large enterprises (usually more than 50,000 endpoints) and government customers that place a premium on security.

Being UK-based, the company has a strong European presence but also pursues opportunities elsewhere, notably North America.

Garrison understands that its target customers already have well-defined components such as sandboxes, web proxies and data leakage prevention (DLP) tools in their security stacks, so the company chooses to offer integrations. Garrison indicated it can integrate with over 10 different proxy vendors and many other security products.

While Garrison's offering has been centered on providing on-premises appliances, the company is now in the process of adding a cloud-delivered version of its offering. This will entail running Garrison in multi-tenant mode at multiple points of presence, which is something the company aims to achieve in the near term.

Product

The main objective of isolation offerings is to handle potentially malicious content in a safe way. Some do it by virtualizing key components of the endpoint while some do it by rendering the content away from the endpoint and showing back a neutralized stream, usually video. Garrison takes this latter approach, but it uses hardware-assisted technology to both better segment the traffic and obtain the necessary performance for supporting multiple users.

The key use case for Garrison's approach to isolation is to balance the benefits of typical web browsing with the risk appetite of security-conscious organizations that often have deeply resourceful attackers as part of their threat models.

Garrison's isolation approach works by providing browsing functionality through a dedicated endpoint application – not a traditional browser – that interacts with hardware appliances that are responsible for fetching content and securing the sessions. Content is then presented to the user as a video stream over a UDP-based protocol. The endpoint application is supported on Windows, Linux and soon, mobile operating systems.

The company considers its product architecture a key differentiator. Garrison uses a set of rackable appliances, each loaded with customized hardware: hundreds of cell-phone-based processors that are paired dynamically to support a browsing session, coupled with FPGA-assisted hardware paths for support functions. The company makes distinct appliances for the browsing process itself and for support functions such as file transfers. Both types of appliances can then integrate into a customer's existing architecture and identity management systems.

Garrison works by dynamically pairing two processor chips to support a user session: one chip is used to obtain remote content via a Mozilla-based browser engine or a PDF viewer then render that via its HDMI output; the second chip captures that output as a video stream and sends it to the internal user after performing compression. Keyboard and mouse input from the user are processed by a hardware-enforced security fabric based on FPGAs. After the session is terminated, each processor chip is released back to a general pool.

The product supports typical browsing to external sites but makes no policy decisions of its own. All policies regarding which sites should be browsed through Garrison are made by the customer's existing proxy/gateway infrastructure. Some customers choose to send all traffic through Garrison, while others segment specific sites/categories or specific departments.

Browsing often includes supporting functionality such as copy & paste, file transfers and printing. Garrison provides mechanisms for sanitizing content via allowing only specific data types or converting files to inert formats. Any file transfers of specific binary formats can be made by integrating Garrison appliances with third-party file transfer capabilities, which can then perform additional content screening.

Garrison made a few design decisions that favor security over usability, such as disabling support for mechanisms that could result in covert data exfiltration from the customer site. This means that in-browser support for video camera, for example, is not supported.

Competition

Garrison seems to be approaching competition with the perspective that it'll find commercial success when pursuing larger organizations that place particularly high value on isolation security, so its efforts are focused on proper opportunity qualification.

Still, as the company competes in a broader commercial market, there is ample competition on the basic functionality for browser isolation.

Many browsing isolation vendors have offerings in this space, including but not limited to specialist vendors Menlo Security, Ericom, Cyberinc, Light Point Security, WebGap, Authentic8 and Randed. Larger vendors such as Symantec and Proofpoint also have isolation offerings.

Isolation is also a key feature of endpoint virtualization-based approaches such as Bromium and Hysolate. At the other end of the spectrum, virtual desktop infrastructure (VDI) offerings such as Citrix Secure Browser and VMware Browser also offer isolation capabilities.

To some extent, browser isolation is adjacent to or can be seen as a special case of the broader area of content disarm and reconstruction (CDR), though most vendors in that space focus more on asynchronous traffic flows. Votiro and Sasa Software have CDR offerings for browsing.

Last, there is significant work in terms of isolation within the browsers themselves. Microsoft Application Guard provides an isolated version of Edge and extensions for Google Chrome and Firefox. Google also engineered the Chrome browser with site isolation, and Firefox recently announced similar support.

SWOT Analysis

STRENGTHS

Garrison's choice of using video streams not only between user and remote viewer but also between remote viewer and browser rendering engine points to an architecture with very strict security controls.

WEAKNESSES

As the company pursues opportunities in broader commercial accounts, the potential efforts needed to integrate Garrison into an environment and the usability trade-offs may be a hindrance to some.

OPPORTUNITIES

Using browser isolation to sidestep potentially malicious content is an efficient mitigation technique and can complement other security architecture components. It can work particularly well in scenarios of more restricted web usage.

THREATS

The increased sophistication of the browsing experience, in combination with improved protection within the browsers themselves, may make isolation less appealing as a technique.