AN INTERVIEW WITH HENRY HARRISON
CTO, GARRISON

ISOLATION AS A POWERFUL WEB CONTROL

ISOLATION is one of the most powerful primitives in cyber security. That is, by separating assets from threats, the likelihood of an attack successfully occurring is greatly diminished. Assurance is another powerful concept in cyber. It is driven by the observation that trust in the implementation of a control is directly related to how well it protects assets. As one would expect, combining isolation with assurance creates a desirable environment for reducing cyber risk.

Garrison is a UK-based cyber security company that builds an isolation platform with high levels of trust and assurance. Specifically, the platform sits between the content stream from browser to website, making certain that any dangerous malware is detonated away from live assets. By implementing this in high assurance hardware, Garrison offers a valuable and trustworthy platform. We met with Henry Harrison of Garrison to better understand this architecture and how it can be used in enterprise.

EA Henry, can you explain how isolation provides risk reduction for the enterprise? What specific threats are mitigated by secure remote browsing?

HH Isolation is a core principle of computing, recognizing that within a single endpoint, the user will work with both extremely sensitive data and with extremely risky data, and that these need to be kept apart. With secure remote browsing, our team at Garrison focuses on the World Wide Web, which is the number one source of extremely risky data – and how to keep that isolated from the sensitive work that people do on their endpoints. We aim to make it possible for people to click on dangerous links without the risk of introducing malware onto their endpoints.

EA What is the role of hardware in the provision of your security solution?

HH Isolation is already a key feature of the user's operating system and of their browser, and for many people that's enough. But, for some customers, the risk is still too high, and that means they need a level of isolation that is over and above that level. We don't believe that step-up can be achieved using the same software approaches that are already used in the OS and browser. Instead, we believe the isolation needs to be delivered at the hardware layer.

EA How is it possible that users would experience the same behavior with Garrison providing security-in-the-middle versus a direct connection to the Internet?

HH Our hardware turns risky content from the Web into pixels, and delivers just those pixels to the user's endpoint. In the reverse direction, the user can click and type just like they normally do to support a regular web browsing experience. The hardware isolation technologies that we use – namely, our own Garrison SAVI technology, and the hardsec approach described at www.hardsec.org – mean that customers can have a very high degree of confidence that it's just safe pixels that reach the user's endpoint. The result is that the endpoint is protected against sophisticated attacks.

EA Do you see secure remote browsing becoming a greater regulatory and compliance requirement for enterprise?

HH For some parts of some countries' governments, the requirement for isolation and secure remote browsing is already a regulatory and compliance requirement. So, the good news is that compliance governing bodies do recognize the benefit of this control. As ever, these requirements tend to end up flowing down into the Critical Infrastructure and Financial Services sectors.

EA Any near or long-term predictions about isolation and secure remote browsing?

HH Leading financial services firms in particular are beginning to recognize two things: First, they have come to see that secure remote browsing can make a massive difference to their risk exposure. And second, they've learned that regardless of the isolation vendor they choose, it's not going to be a trivial project. That means that there's an increased focus on ensuring they really get an attractive return on investment (ROI) to justify the effort they're going to expend deploying it. This is done by providing significant risk reduction in the areas that really matter.