GARRISON

Let them click links

Would you click this link?

Web links can be dangerous. A carefully crafted malicious web page could take complete control of the visitor's endpoint machine. From there, they could wreak havoc in the corporate network – stealing data, or even more worryingly, making changes to critical systems or information.

What about www.app1e-support.x.com?

Malicious links are part of our everyday life. Everyone who has an email address receives phishing emails purporting to be from Apple, or their bank, or Amazon. We all need the everyday skills to differentiate between valid emails and phishing emails. Training can help us to spot giveaway signals that an email or a web address is not what it first seems. But in practice, even the most well-trained people tend to make a mistake once in a while.

How about www.excession-reports.com?

For criminals targeting individuals, the payoff is usually small-to-medium sized. It justifies a certain amount of effort – but the best strategy is to find the most gullible individuals. As a result, many phishing emails are deliberately misspelt or ungrammatical: if the recipient fails to spot the flaws, the chances are they will fail to get wise to the rest of the process before it is too late.

In the corporate world, the situation is quite different. The potential payoff can be huge – financially, or in the case of nation state actors, strategically. Rather than seeking out the most gullible individuals, attackers seek out the most valuable individuals – and then expend real effort crafting phishing emails that appeal directly to them, include detailed personal information, and contain highly plausible links.

And increasingly, those links are not to "bad" sites that have been set up by the attacker. Rather, they are to valid sites with valid content – but sites which have weak security and which have been compromised by the attacker.

Even the most sophisticated cyber security professionals can easily be tricked by this sort of sophisticated spear-phishing. Training is not a strong enough response.

Technology to the rescue?

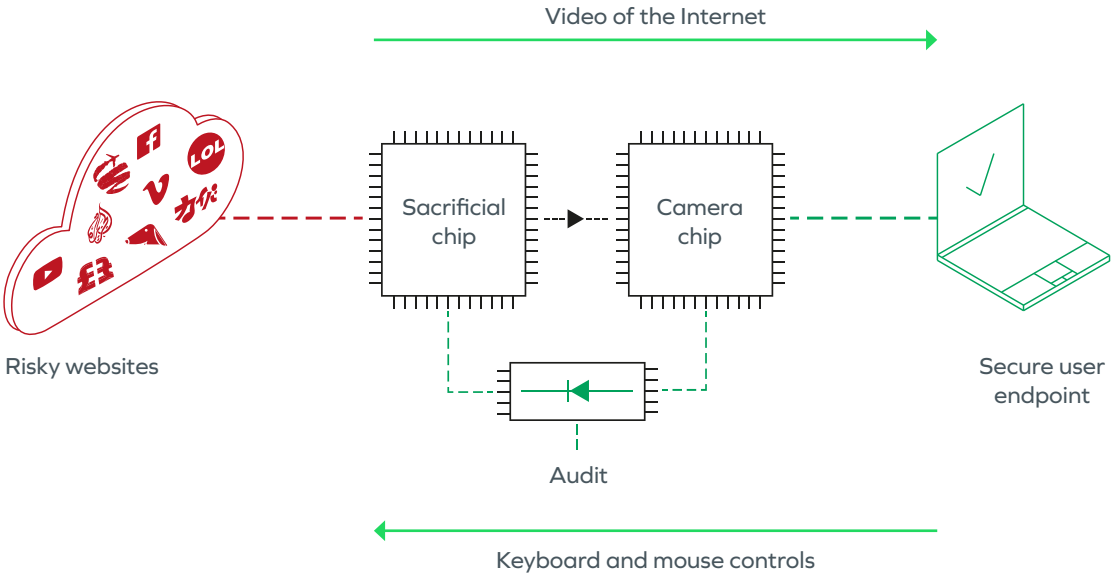
Professionals need to click on links. If we ask our employees to act as knowledge workers, we must provide them with safe access to the knowledge that is available. If the technology that we have cannot protect them when the link turns out to be bad, we need to invest in technology. But clearly, given the existing levels of investment in cybersecurity technology that is failing to protect from bad links, we need something dramatically stronger.

Garrison's Silicon Assured Video Isolation technology (Garrison SAVI®) provides that next level of protection. Sufficiently strong that it is being adopted by national governments to protect users of highly sensitive systems, Garrison SAVI® allows personnel to click on even the most dangerous links without putting their employer's systems and data at risk while delivering a frictionless experience to the end user.

How does it work?

Garrison SAVI® works by reimagining web browsing right down at the hardware level. The Garrison SAVI® Isolation Appliance is a data center unit containing hundreds of SAVI Nodes – each node containing two physically separate silicon chip devices like those typically found in a mobile phone.

One of those chips does the browsing – exposing itself to the inevitable risks. The other chip simply watches what the first chip does, sending just a video of the results to be displayed to the user. And in the other direction, keyboard and mouse commands are sent from the user to the first, sacrificial chip – allowing the user to browse in the same way they are used to.

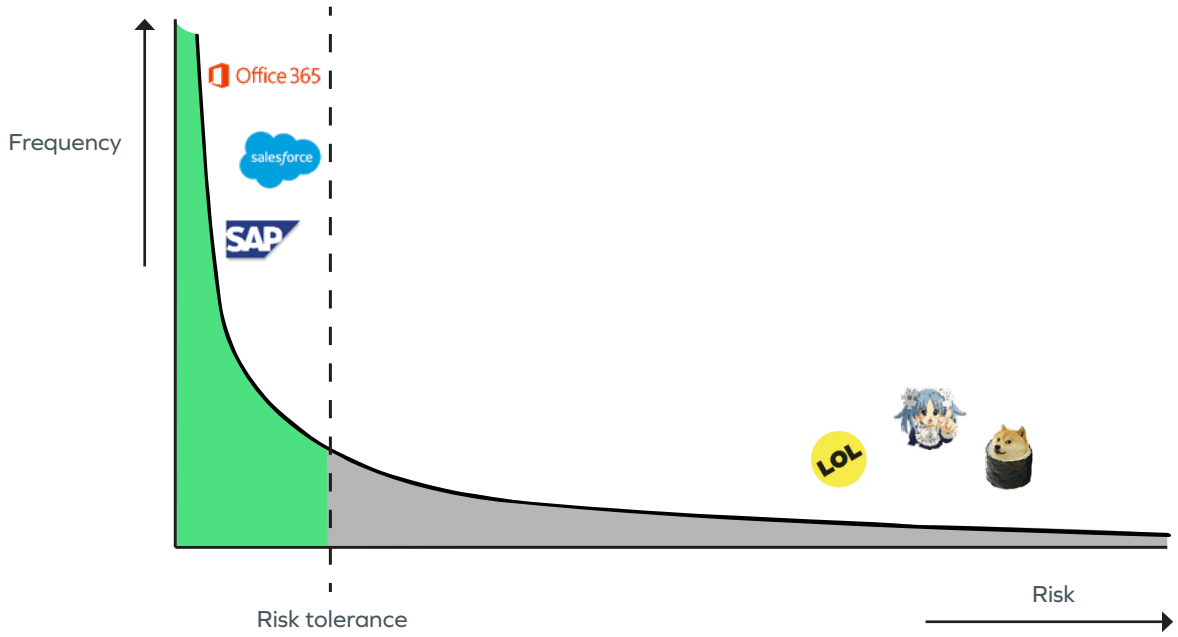


The result isolates the risky web at a fundamental, physical level: even if the first, sacrificial chip is thoroughly compromised by web-based malware, the user's endpoint machine remains safe.

How is Garrison SAVI® used?

Some organisations use Garrison SAVI® for all their staff's web browsing needs. But other organisations use Garrison SAVI® only for the riskiest types of browsing – links in emails from unknown sources, web pages with low reputation scores, or inherently dangerous website categories such as filesharing or social media.

In a corporate context, the most frequently visited sites tend to be relatively low risk. By setting their risk tolerance accordingly, organisations can push either a higher or a lower proportion of their web browsing traffic through Garrison SAVI®, balancing risk with cost and user impact. Many organisations start with only a very small proportion of web traffic or for only high-risk users, thus requiring a very low investment.



Over time as their risks grow or their risk tolerance falls, they can start to direct more traffic through Garrison – eliminating whole classes of risk while maintaining the productivity of their knowledge workers.

GARRISON

Email info@garrison.com

UK telephone +44 (0) 203 890 4504

US telephone +1 (646) 690-8824

www.garrison.com

CD00000217v1.1 - UK - October 2018