Solution Brief

Symantec Web Isolation:

An Essential Part of Your SASE Strategy

Challenge

The web is a dangerous place. Without intending to, users can get into all kinds of trouble, whether they inadvertently browse to a dangerous web page or click a malicious link that was emailed to them. Just a few clicks can expose your organization to a devastating breach. Of course, you can protect your users and your organization by severely limiting web access, but such a draconian approach could severely constrain users from doing their jobs. The fact is, just about everyone needs access to the web throughout the workday, and it is not possible to allow or block every site.

Opportunity

At Symantec, a division of Broadcom (NASDAQ: AVGO), we believe you can go far toward that goal of protecting your users and your organization by implementing web isolation technology. By separating out questionable sites and placing them in secure, disposable containers, web isolation executes web sessions away from endpoints. Sending only safe rendering information to users' browsers enables users to visit potentially dangerous websites without the risk of infection. A similar approach can also protect email attachments that have passed through other security filters but are still deemed to have potential risk.

How to Enable Safe Browsing at Your Organization

Symantec Web Isolation connects each active browser tab to a secure browser running in a container either on-premises or in the cloud. This secure browser interacts with the Internet for the user, ensuring that attacks stay away from the local machine, while preserving the user experience. Information from the secure browser is rendered back to the end user, and unless visually indicated, users may not even know they are being isolated. To ensure high system availability, Symantec dual mode isolation automatically selects the right method for each class of web page, while providing an operational failsafe.

This type of security does not require detection-based technologies and eliminates entire classes of attacks. In addition, because Web Isolation controls both ends of the communications, it can apply controls like read-only for suspicious sites (to prevent phishing), DLP on all outgoing data, and other sophisticated controls, very easily with minimal configuration or administrative challenges.

Web Isolation fits well into Gartner's Secure Access Service Edge (SASE)[1]* architecture as a central way to provide absolute security and visibility on end user web browsing.

We understand the nature of website risk, spanning critical data security, and protecting against sophisticated phishing and water hole attacks. To this end, Symantec web intelligence considers websites in terms of risk, recognizing that risk to be dynamic.

For example, a website that was safe a few minutes ago can quickly become the source of malware or a phishing attack, enticing users to give up their usernames, passwords, or sensitive data. Comprehensive web security analytics are used to quantify risk by evaluating the age of the web site, the owner, the content it is hosting, and whether similar sites or IP addresses have a history of delivering malware.

Using comprehensive web security analytics allows every website to be allocated a risk score, Web Isolation can be applied either selectively (to certain higher risk websites only) or in full.

Without this analysis, there will inevitably be trade-offs between over-blocking web access, which angers and frustrates end users and overwhelms IT support teams, or being open to attack, which can jeopardize your business.

1 Gartner "The Future of Network Security Is in the Cloud," Neil MacDonald, Lawrence Orans, Joe Skorupa, 30 August 2019

Benefits

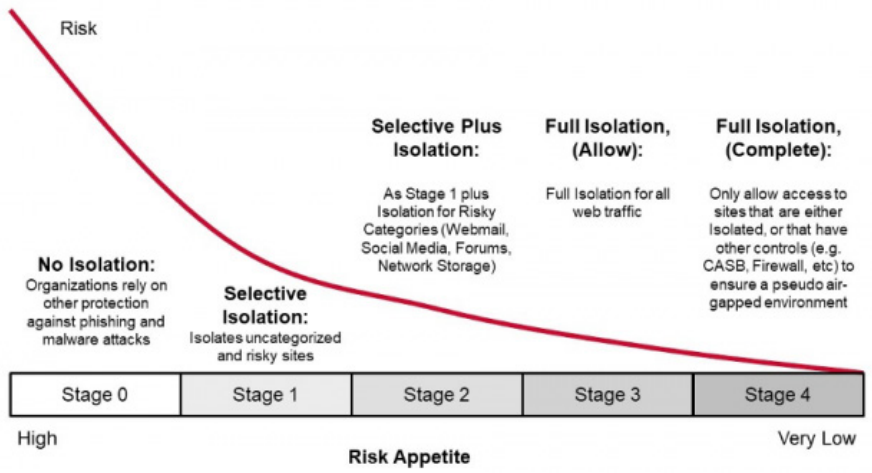
Symantec Web Isolation works in concert with other cyber security technologies. For example, when combined with Symantec Secure Web Gateways, rich policies can replace standard, inefficient "allow or deny" policies by isolating traffic from uncategorized sites or URLs with suspicious or potentially unsafe risk profiles.

By integrating with Symantec messaging solutions, Email Threat isolation quarantines links in email to prevent phishing threats and credential attacks, and ensures attachments that do not trigger existing anti-malware screens, but are considered risky, are presented in an isolated form to reduce attacks.

On a practical note, maintaining a high level of protection for an organization's entire endpoint estate can create operational challenges and may prove impossible even in the most sophisticated organizations.

Ensuring that all operating systems, software, browsers, and security controls are all up to date and patched for all critical vulnerabilities (at all times) is challenging to say the least. Web isolation can act as a buffer and give an organization flexibility to implement the patching and updating regimen that works best for them, striking a balance between operational and security concerns.

By preventing threats from entering at all, web isolation can significantly reduce the volume of attacks to endpoints in an organization, which means fewer infected systems, less chasing of detection alerts, a lower risk profile for web browsing, and more time to focus on real threats.



How to Enable Safe Browsing (cont.)

By isolating websites according to risk level, it is possible to hit the sweet spot between over-permitting and over-blocking access. As you can see in the chart above, implementing Stage 1 isolation delivers dramatic benefits.

Additional risk reductions are more gradual, but can be vital, depending on the user and web content being accessed.

Applying maximum isolation in conjunction with other protection technologies, such as Stage 4, might be necessary for organizations where the risk tolerance for a website attack or breach is very low. Some organizations also decide to deploy isolation in a hybrid format, where the majority of users are protected with selective isolation, and other higher value users experience full isolation.

Using Symantec Web Isolation

Symantec Web Isolation works in concert with other cyber security technologies. For example, when Symantec Web Isolation is combined with Symantec Secure Web Gateways, rich policies can replace standard, inefficient *allow or deny* policies by isolating traffic from uncategorized sites or URLs with suspicious or potentially unsafe risk profiles.

By integrating with Symantec messaging solutions, Email Threat isolation quarantines links in email to prevent phishing threats and credential attacks, and ensures that attachments that do not trigger existing anti-malware screens, but that are considered risky, are presented in an isolated form to reduce attacks.

Web Isolation Changes the Equation Completely

You might ask why Web Isolation is needed if you already have existing web protections in place like proxies, next generation firewall, or endpoint protection. Web Isolation is meant to work in conjunction with those kinds of security technologies to eliminate common types of risks. Consider that for all of those security controls to work, they must be enabled and running, have up to date signatures, visibility on the traffic or payload and so on. If any of these things is lacking, then the endpoint is vulnerable to an attack. Web Isolation changes the equation completely.

The bottom line: Web access is an essential part of work. Safe browsing must be, too. As you implement a SASE architecture at your organization, be sure to include web isolation.

*Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties,expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

SED-WI-SASE-SB100 October 5, 2020