Symantec. A Division of Broadcom

Product Brief

Symantec Web Isolation

Advanced Threat Prevention Capabilities for Secure Web Gateways

At A Glance

Problem

Protect users from malware and phishing threats often delivered by uncategorized and potentially risky websites without over-blocking access to the web

Solution

Symantec Web Isolation with Secure Web Gateways

Benefits

- Allow protected access to uncategorized or potentially risky sites
- Increase business productivity by giving employees access to a broader set of websites
- Secure web browsing for executives and privileged users whose access to sensitive documents and systems makes them highly prized targets for cybercriminals
- Prevent users from disclosing corporate credentials to malicious websites
- Avoid patient zero by blocking advanced malware and targeted phishing attacks, minimizing alerts, investigations and remediation efforts
- Simplify web access policies and minimize support tickets requesting access to blocked sites

The Uncategorized and Risky Web: Critical Attack Vectors

IT security teams experience a constant barrage of attacks attempting to penetrate defenses and steal data. According to Symantec's Internet Security Threat Report, the vast majority of these cyber attacks originate from the web and email. Cybercriminals leverage a variety of malware and social engineering tactics to dupe employees into infecting devices and networks with malware, often by luring them to malicious websites.

Millions of new internet hosts (domains and sub-domains) are born every day. The vast majority of these exist for less than 24 hours, coming up and down quickly. Analysis reveals that while the majority of these hosts have valid business purposes, many of them are tools for hackers. These sites, both valid and malicious, are not categorized and analyzed for risk effectively by web filtering and threat intelligence services because they have no meaningful reputational history. Add to this websites that are categorized and have a potentially unsafe risk profile, and security professionals have a real challenge on their hands.

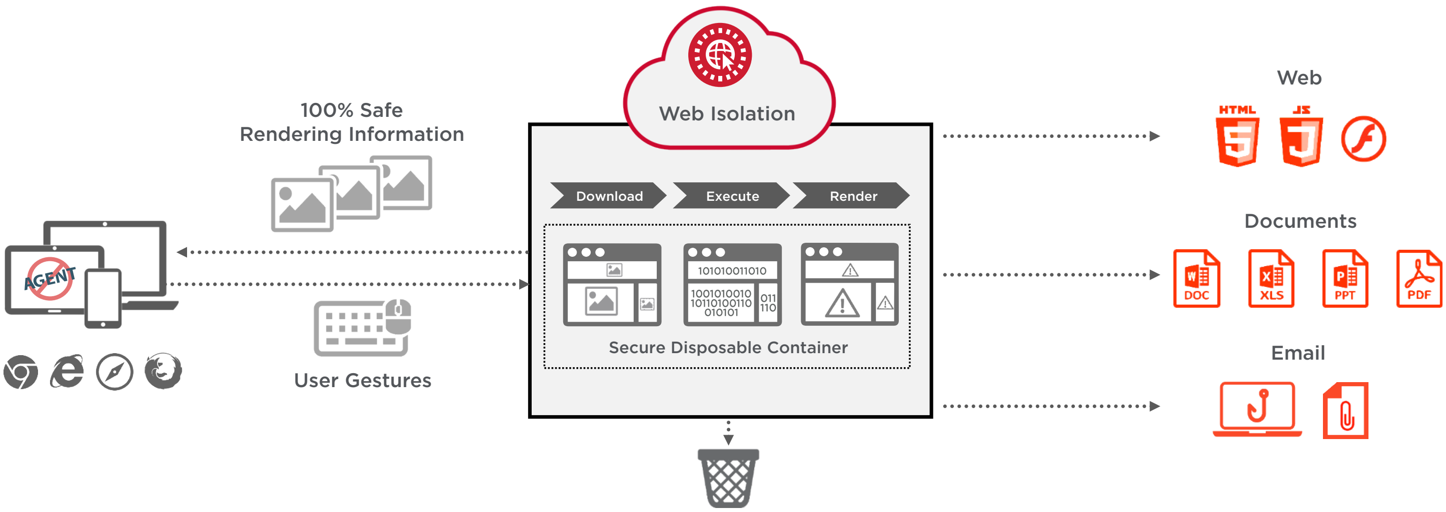
Some enterprises set policies that completely block sites that cannot be categorized or are assessed to have a potentially unsafe risk level. This typically results in overblocking employee web use as valid sites get caught in these types of policy rules. Others may choose to roll the dice and permit access to these types of sites in order to not impede employee ability to perform business activities, but this opens up the organization to undo risk. This risk is magnified in the case of privileged users, who are prized targets for cybercriminals because of the significant access rights and sensitive data typically found on their machines.

Web Isolation: Expand Web Access, Protect Privileged Users, and Combat Phishing Attacks

Web isolation eliminates web threats and solves the challenge of providing secured access to the uncategorized and potentially risky web. Symantec Web Isolation creates a secure execution environment between users and the web. By executing web sessions remotely and only sending safe rendering information to users' browsers, Web Isolation eliminates any web-borne threats from reaching users' devices.

Combining web isolation with Symantec ProxySG, ASG, and VSWG products provides an isolation layer to protect users in real-time from threats targeting them from uncategorized sites or URLs with potentially unsafe risk profiles.

Figure 1: Symantec Web Isolation Inputs and Outputs



Enterprises can also use isolation to provide enhanced security for privileged users who have unique access to sensitive data and critical systems. Policies can be configured to send all web traffic from these users through an isolation path, which can protect them from web-based threats.

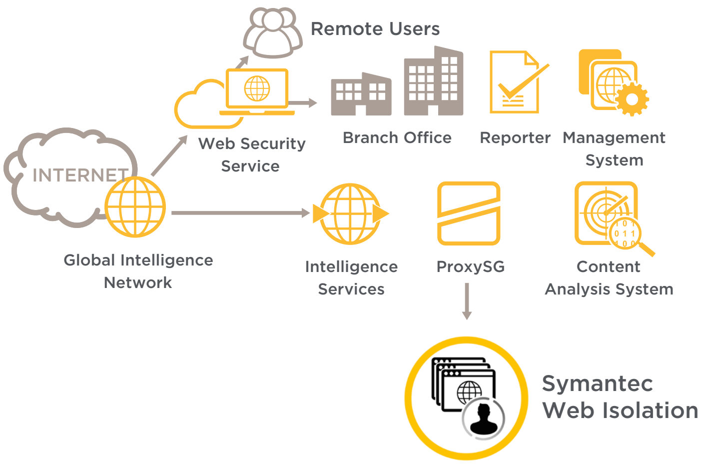
Additionally, Symantec Web Isolation can combat phishing attacks by making email links to malicious websites harmless. These sites, when isolated, cannot deliver their malware, ransomware, and other advanced threats to the email recipient's machines. Symantec Web Isolation can also prevent users from submitting corporate credentials and other sensitive information to these sites by rendering them in read-only mode.

Symantec's patented Transparent Clientless Rendering (TCR) technology provides a seamless user experience through the native browser, indistinguishable from browsing directly to the web. Symantec Web Isolation does not require any endpoint or plug-in installation and supports any OS, device, and browser, which allows for enterprise-scale deployments.

Symantec technology can handle web resources remotely, eliminating the need to send exploitable web content to the browser. Offered as a managed cloud service, on-premise virtual appliance, or as a hybrid model, Web Isolation easily integrates with existing Symantec ProxySG, ASG, and VSWG deployments. Policies can be configured in Symantec proxies to send traffic from uncategorized sites and sites with potentially unsafe risk profiles down a Web Isolation path, allowing users access to these sites while helping to ensure the enterprise is protected from any threats these sites pose to the business.

The addition of Web Isolation to Symantec's Secure Web Gateways maximizes business and user productivity with secure, unrestricted web access to uncategorized and potentially risky websites while minimizing operational overhead and complexity related to managing web access policies, support tickets, security alerts, and forensic investigations.

Figure 2: Symantec Secure Web Gateway



Symantec
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-webIsol-PB100 September 18, 2020