



Threat Isolation

Integrating with Symantec Secure Web and Mail Gateways

At A Glance

Problem:

Protect users from threats delivered by uncategorized websites without over-blocking access to the web.

Solution:

Fireglass Threat Isolation with Symantec Secure Web & Mail Gateways – ProxySG, ASG, VSWG, SMG.

Benefits:

- Allow safe access to uncategorized or risky sites safely and without risk, increasing business productivity
- Enable access to documents through isolation instead of being downloaded
- Inspect and remove exploitable content from files before download
- Prevent submission of corporate credentials to malicious websites
- Block malware such as Ransomware, Remote Access Trojans, and Command & Control traffic

The Uncategorized Web – A Critical Attack Vector

IT security teams experience a constant barrage of attacks trying to penetrate their defenses and steal their data. Over 90% of these cyber-attacks originate from the web and they are becoming more sophisticated by the day. Cybercriminals leverage a variety of malware and social engineering tactics to dupe employees into infecting their devices and your network with malware, and an important one is the creation of malicious internet sites.

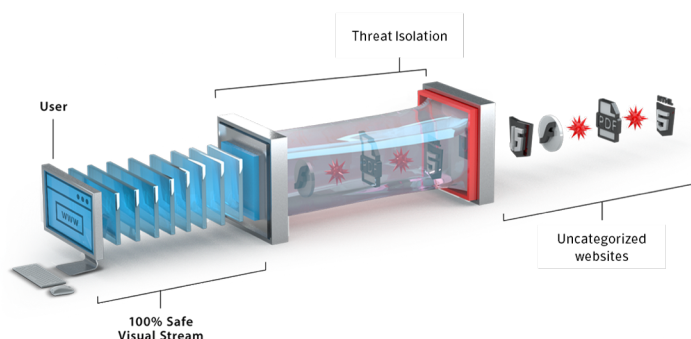
Millions of new internet hosts – domains, sub-domains, IP addresses – are born every day. The vast majority of these exist for 24-hours, popping up and coming down quickly. Analysis has revealed that while the majority of these host locations have valid business purposes, many of them are tools for hackers, who use various techniques to lure employees to them in order to infect visiting machines with malware. All of these sites, valid and malicious, are not categorized effectively by web filtering and threat intelligence services because they have no meaningful history.

Some enterprises set policies that completely block sites that cannot be categorized. This typically results in over-blocking their employee's web use since valid sites get caught up in this type of policy rule. Others may choose to roll the dice and permit access to uncategorized sites to allow their employees to perform their business activities, but this opens the organization up to undo risk.

Threat Isolation Conquers the Uncategorized Web

Threat isolation is the most effective way to solve the uncategorized web challenge and Symantec's acquisition of Fireglass brings the market's leading threat isolation product into Symantec's enterprise security portfolio. Combining threat isolation with Symantec ProxySG and Web Security Service secure web gateways and content and malware analysis products adds an isolation layer that protects users in real-time from threats targeting users from vectors such as uncategorized web sites.

By creating a secure execution environment between users and the web, and sending only a safe visual stream to users' devices, isolation eliminates web-borne threats from these locations.



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

Fireglass's technology handles all resources remotely, eliminating the need to send malware-prone rendering elements such as DOM, CSS files and custom fonts to the browser. Offered as a managed cloud service, on-premise virtual appliance, or as a hybrid model, Fireglass **easily integrates with existing Symantec ProxySG and Web Security Service deployments**. Policies can be configured in your Symantec proxies to send all traffic from uncategorized sites down a Threat Isolation path, allowing your users access to these sites while ensuring your organization is protected from any threats these sites pose to your organization.

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

