Menlo Security

BRIEF

The Risky Web

Unrestricted access to the internet and a secure enterprise are not mutually exclusive.

Today's Threat Landscape:

- New webpages are sprung up and down every day and are constantly updated—creating a dynamic web that is difficult to categorize..
- Threat intelligence also has trouble keeping up as web pages are constantly updated and enriched with third-party content.
- Whether delivered as a link in an email or as an attachment, weaponized documents download malicious malware on an unwitting user's device.

The Enterprise Dilemma: Unrestricted or Controlled Access to the Web

The threat of contracting malware from the web is very real. There are more than 500 million variants in existence, and even trusted sites can harbor malicious content hidden in plain site. It's extremely easy to propagate and, for this reason, malware has played a critical role in many high-profile breaches recently. The costs of these breaches reaches millions—even billions—of dollars, forcing enterprises to adopt increasingly-strict web security policies.

The risky web is forcing security administrators into a no-win situation. They are constantly being asked to walk the fine line between protecting the enterprise from malicious content and giving users unfettered access to the web-based tools and information they need to do their jobs when any restriction hinders productivity and adds complexity for administrators.

Existing Tools Rely on Allow or Block Approach

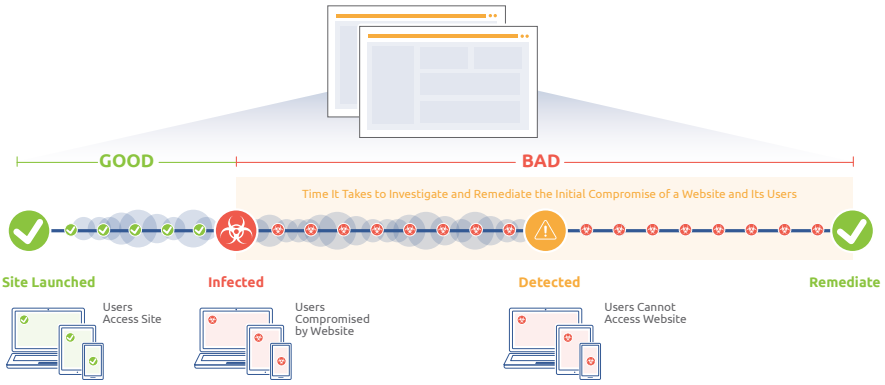
Traditional Secure Web Gateway (SWG) solutions rely on website categorization to determine whether to allow or block access to a site. However, not all legitimate websites can be categorized. The nature of today's internet is that new webpages are sprung up and down every day, creating a dynamic web that is difficult to categorize in real time. Users may need access to a new customer site or a site that doesn't fit into an existing category. This forces enterprises to set security policies that are too strict and impede productivity or are too lenient and increase malware risk.

A New Approach: Internet Isolation

Isolation eliminates the possibility of malware reaching users' devices via compromised or malicious websites, email attachments or documents. Rather than rely on an allow or block approach based on detection and classification, web isolation treats all web content as risky and conducts the fetch and execute commands in a cloud-based isolation platform. Only safe, malware-free content is mirrored to the user's device, resulting in a completely safe web experience without having to block any websites, documents or other legitimate content in the interest of security.

20%

Menlo Labs research states that at least 20% of URL's Isolated by the Menlo Internet Isolation platform turn from Good to Bad!



Integrating web isolation capabilities within a traditional SWG allows administrators to open up more of the internet to users while eliminating the risk of attacks.

Uncategorized Websites	Weaponized Documents
How They Work: URLs may be categorized because they are unknown, new or just don't fall neatly into any existing category.	**How They Work:** Threat actors have perfected the art of coercing users into downloading malware-infested documents on their device.
Why Existing Solutions are Inefficient: Dealing with uncategorized websites requires an extremely labor-intensive process. Security experts need to constantly categorize websites and respond to user requests to unblock false positives--costing millions of dollars per year in management costs.	**Why Existing Solutions are Inefficient:** A recent tactic is to disguise an infected XML file as a Word document that prompts the user the enable malicious macros that download malware--effectively allowing them to avoid sandboxes and AV solutions.
The Solution: Web isolation allows users to access any website without posing a risk to the organization. This eliminates the expense of categorizing websites and of responding to trouble tickets.	**The Solution:** Web isolation executes all active content in the cloud--far away from users' devices. Users also have the option to download safe and cleaned or original versions of documents based on policies.

About Menlo Security

Menlo Security protects organizations from cyberattacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com