Menlo Security

BRIEF

Ensure That Endpoint Devices Are Protected—Even Before They're Patched

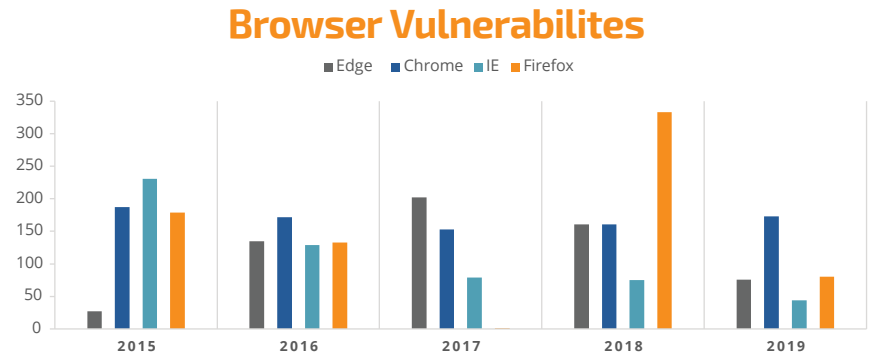
The Menlo Security Cloud Platform powered by an Isolation Core™ automatically patches popular browser vulnerabilities.

Benefits:

- 100% malware-free video streaming
- Browser vulnerabilities are plugged before they can be exploited
- Saves bandwidth and related IT costs
- Reduced IT overhead from patching distributed machines individually

It's a no-brainer: Consistent patching is critical for effective cybersecurity protection. Web browsers and their plug-ins need to be updated often and quickly before vulnerabilities are exploited by malicious actors looking to infiltrate the corporate network through the Internet. Browsers have evolved into complex applications that deliver rich functionality to their end users—adding complexity that has contributed to more vulnerabilities in both browsers and their plug-ins.

However, keeping up to date on patching is easier said than done—particularly when it comes to the logistics of updating browsers and plug-ins on thousands and even millions of devices in large organizations. It's clear that a new way is needed to ensure that malicious actors are not able to exploit browser vulnerabilities.

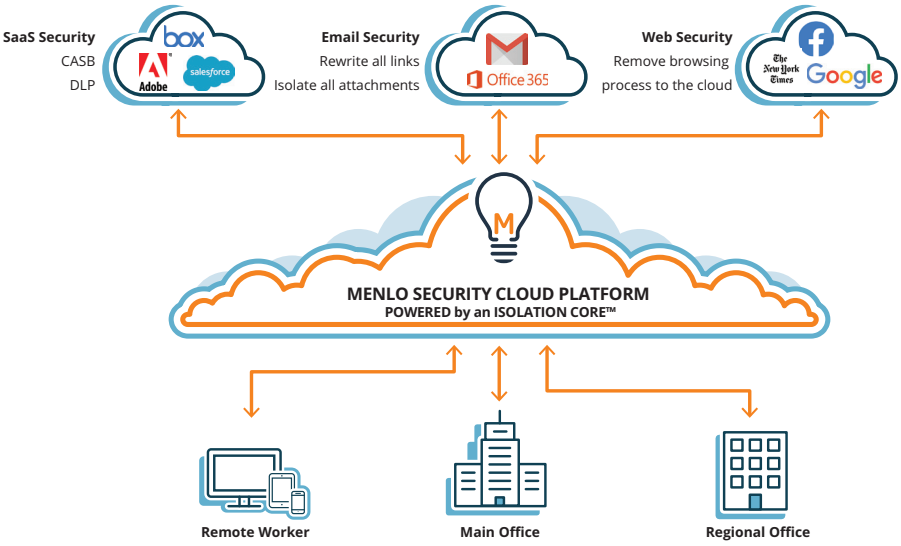


Source: https://cvedetails.com

No browser is immune from vulnerabilities. In fact, browsers are becoming less secure as they grow more sophisticated and advanced to support increasingly dynamic web content. Users are no longer content to view static websites. They want to interact with content, requiring complex functionality and plug-ins that remain vulnerable to cyberattacks. In addition, business today is much more reliant on powerful web apps and Software as a Service (SaaS) platforms that deliver core business functions.

Menlo updates its browsing engine as soon as possible—providing protection for endpoint devices even before they are patched individually.

Zero Trust Internet Architecture



Seamless, Centralized Patching in the Cloud

The Menlo Security Cloud Platform powered by an Isolation Core™ enables that new approach and updates its browsing engine as soon as possible—providing protection for endpoint devices even before they are patched individually.

Menlo begins testing the latest version of Chromium, for example, before it's made available to the public. New isolation nodes equipped with the latest Chromium release are deployed to the Menlo Security Cloud Platform upon completion of testing, so users are seamlessly transitioned to the latest version of the Chromium engine as soon as it is available publicly.

In this way, Menlo provides relief from the urgency of patching browsers and plug-ins. A core isolation strategy that doesn't have these capabilities degrades the entire security stack because of its inherent vulnerability before devices are individually patched. Seamless, centralized patching in the cloud, on the other hand, provides malware protection for endpoint devices even before they are patched.

To find out how Menlo Security can provide your company with protection against cyberattacks, visit menlosecurity.com or contact us at ask@menlosecurity.com.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The Menlo Security Cloud Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

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