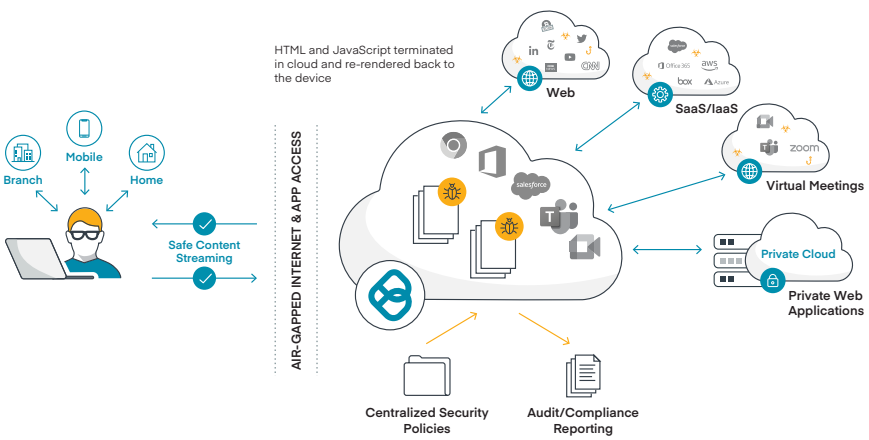
Why is Your Business Still Experiencing Cyberattacks?

Your security stack has secure web gateways, new generation firewalls and WAFs. Yet malware is still getting in. How can that be? As detection-based solutions have grown more effective, savvy threat actors are increasingly using two sure-fire paths to evade them: Zero-day exploits, since unknown signatures raise no alarms, and targeting users, who are easily fooled by phishing and other social engineering techniques.

Web use is the gaping hole at the center of organizations' Zero Trust security programs. It is where cybercriminals lure your users in – and where users, inadvertently or not, expose sensitive data with dire results for businesses, customers, and the users themselves.

Ericom Security for Financial Institutions



ericom security
by cradlepoint

- **Zero-Day Web Security**
  Stops zero-day exploits, provides web access controls, blocks data exposure in virtual meetings and chats.
- **Phishing Prevention**
  Blocks malware delivery even if users click. Stops users from entering credentials on even expertly spoofed sites and forms.
- **Protect Data in Generative AI**
  Keep sensitive data from being exposed to LLMs. Block malware in AI responses from infecting devices or networks.
- **Unmanaged Device Web/Cloud App Access**
  Clientless least privilege access to resources contractors need. Prevents data loss and protects apps from unmanaged device risk.

Prevention-Based Security that Stops Breaches and Zero Days

Ericom's cloud security solutions apply innovative prevention-based Zero Trust security controls to protect critical resources from web-delivered cyber threats – even zero-day exploits. They prevent user actions that too often result in breaches or worse, without limitations on web use that frustrate users and burden IT. With Ericom solutions, your users can access popular web apps like virtual meetings, instant messaging, online translators and GenAI sites without risk of sensitive data or PII being exposed.

Unlike traditional security tools, Ericom's isolation-based security solutions protect your organization's users, apps, and data from even undetectable threats.

Zero-Day Web Security

Ericom Web Isolation security works on the principle that since no web content can be verified as safe, all content should be prevented from reaching user devices. Ericom's next-gen solution renders websites in the cloud and streams only safe data to endpoint browsers, where users interact with it as they would directly with the site.

Policies can be applied to control which users can access each kind of site, and to what extent. For virtual meetings, that means controlling which users can share screens or use chat, and what they can share. Content disarm and reconstruct (CDR) technology sanitizes downloads in isolation to prevent malware infection via weaponized attachments.

Phishing Prevention

Despite email filters, phishing emails continue to flood into corporate inboxes. Even anti-phishing training providers concede that 5-7% of users continue to click despite regular training. And even one click is enough to launch a cyberattack.

Ericom Web Security opens potentially malicious links in isolated cloud containers to keep malware off user devices. Websites from suspicious link appears in "read-only" mode so users can't be misled into providing credentials.

Protect Data in Generative AI

GenAI websites record and store all conversations for use in model-training datasets. That means that if your users enter sensitive data, it could be revealed in responses to other users' queries.

Ericom Generative AI Isolation restricts use of GenAI platforms to approved users. It protects PII and other sensitive data from exposure; enforces granular controls on upload, downloads and clipboarding functions; and blocks malware in responses from reaching user devices and networks.

Secure Web/Cloud App Access from Unmanaged Contractor Devices and User BYODs

3rd party contractors and partners often need to access corporate data and apps. But their unmanaged devices are apt to introduce risk and are often associated with cyberattacks. User BYODs can present similar risks.

Clientless Ericom Web Application Isolation manages access via the cloud. It applies isolation-based clipboarding controls to protect SaaS, cloud and web apps and data from user and device risk, and applies DLP to prevent loss of sensitive data and PII.

Discover how Ericom cloud-based cybersecurity solutions can protect your organization from cyberattacks and data loss.

Contact us today to learn more about our cloud-delivered Zero Trust security solutions or for a demonstration.