Air-Gapped Internet and Application Access: A Unique Zero Trust Approach

Current Security Solutions Are Not Preventing Cyberattacks. Why?

Today, no organization can avoid being targeted by cyberattacks. With costs of a breach estimated at over $4m, insurers have broadened exclusions and even insured companies are being left to cover most of the costs of clean-up and restoration, to say nothing of business disruption, reputational loss, legal fees and regulatory fines.

Despite heavy investment in security architectures that purport to be Zero Trust, cyberattacks are not being prevented. Web and email, which together account for almost 90% of ransomware delivered, are particularly problematic.

Business leaders who bear regulatory responsibility for data privacy and breach notifications need answers on how to deliver on the promise of Zero Trust protection for these most vulnerable attack vectors.

ericom security
by cradlepoint

Highlights

- Cloud-delivered Zero Trust security architecture
- Air-gapped isolation prevents web and email delivery of zero-day attacks
- Prevents confidential data loss in Zoom, MS Teams, and other virtual meetings
- Enables compliant use of GenAI systems like ChatGPT
- Removes users from the front lines of security defense
- Secures organizations from unmanaged device risk

How Cyberattacks Happen

Current security architectures and tools operate by detecting known malware by their signatures -- patterns in code or instructions that identify specific malware strains. To evade them, hackers have turned to zero-day exploits, newly developed malware whose signatures are unknown. Detection-based tools can't stop them.

These zero-day exploits are delivered to device browsers when a user clicks on a malicious URL, and from there to business networks. The URLs are dispatched via millions of phishing emails and social media posts designed to fool or pressure users into clicking.

Cyber awareness programs are most businesses' response to this issue. Training companies claim 95% improvement in phishing prevention, but even one click is enough to paralyze a business and place company secrets in criminals' hands.

Digital transformation is also increasing cyberattacks. To streamline processes and reduce costs, companies allow business partners, customers, contractors and remote workers to access corporate private and SaaS apps from their own unmanaged devices. Since BYODs are not controlled by corporate IT they are more likely to contain malware or spyware. Corporate apps and sensitive data are exposed to cyber risk when users connect from their unmanaged devices.

How True Zero Trust Security Addresses These Attacks

True Zero Trust security starts with the concept of DO NOT TRUST anything: Not the internet, not any inbound document and not any unmanaged device, regardless of whether a 3rd party device or a user BYOD. Even a company's own users should not be trusted to be security aware.

A Zero Trust web access architecture would prevent all web content (since none can be verified safe) from reaching user devices as they browse, attend virtual meetings, or engage with tools like Bard and ChatGPT. It must also provide a seamless, interactive internet and browsing experience.

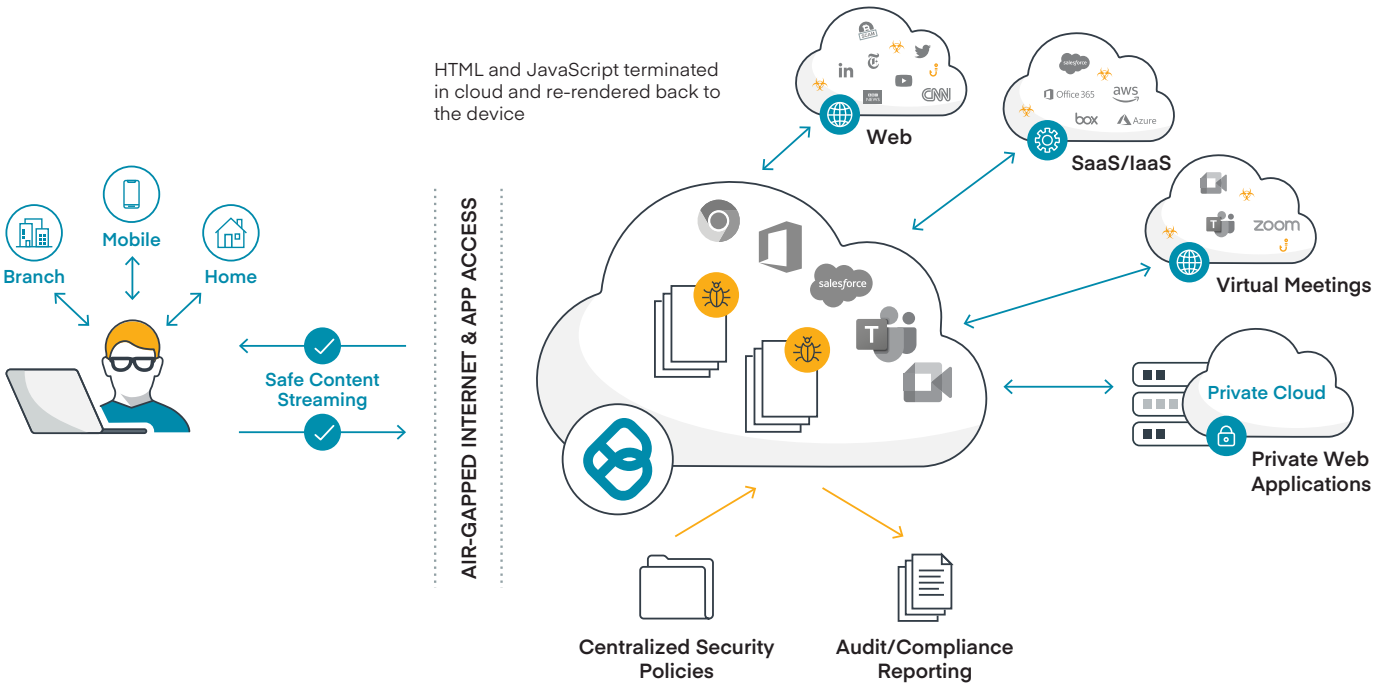
A Zero Trust application access architecture would clientlessly air-gap risky unmanaged 3rd party and BYOD devices away from corporate networks and private and SaaS applications; with further security controls in place to protect your data from being exposed; and limit user access to only the specific resources and functions each individual requires.

The Ericom Zero Trust Security Model

Ericom's Zero Trust security solution utilizes cloud-based isolation architecture to create an 'air-gapped' security layer that prevents zero-day exploits from moving from websites to your users' devices and your networks, and from unmanaged business partner, customer and contractor devices and user BYODs to your apps. Within the airgap, policy-based controls enforce least privilege access restrictions.

Our game-changing model delivers on the "never trust" principles that traditional security architecture and detection-based tools neglect.

Ericom Security



Zero Trust for Websites and Email

Flaw in standard approach: Detection-based solutions leave businesses at risk from unknown malware like zero days. To address this issue, businesses block large swaths of the web, frustrating users and burdening IT with access requests -- while still not achieving true Zero Trust. User anti-phishing training is flawed in its very premise and can never be fully effective.

Ericom Zero Trust approach: Ericom Web Security leverages remote browser isolation (RBI) to airgap user devices from the internet. Website code -- including sites opened from email links -- is executed in isolated virtual browsers in the cloud. Only safe rendering data is streamed to standard device browsers, where users interact just as they would with native web content.

Policy-based controls restrict which individuals or groups can access specific sites or site categories, and untrusted sites can be opened in read-only mode to prevent users from entering credentials. Content disarm and reconstruct (CDR) is applied in the cloud to documents prior to download to eliminate weaponized content and DLP ensures sensitive data is not leaked to web sites, cloud apps, GenAI sites, online translators and similar sites.

Zero Trust for Virtual Meetings

Flaw in standard approach: Risks associated with virtual meetings range from users disclosing PII in chats to uninvited "guests" joining meetings to sensitive data exposed in screenshares. No standard solutions address these threats, which is why many major organizations block these productivity-enhancing tools. Remember -- a compromised device has access to all video conference content.

Ericom Zero Trust approach: Ericom Virtual Meeting Isolation (VMI) isolates all meeting functions -- cameras, microphones, chats and screens. It preserves all meeting functionality, while enabling policy-based controls to restrict user access, feature usage and data sharing, and prevent exposure of sensitive data. Because the meeting are executed in isolated containers, endpoint IP addresses are not visible to hackers and meetings are secured from unauthorized or malware-enabled recordings. All standard isolation protections -- against zero days, weaponized content and more -- are available as well.

Zero Trust for Application Access from Unmanaged Devices

Flaw in standard approach: Unmanaged devices may have unresolved vulnerabilities and contain malware that can exfiltrate data or infiltrate and disable apps and systems. Uncontrolled privileges and inadequate data control for 3rd party contractors and customers creates data loss risk. A unmanaged device that is compromised will still have access to your network and apps.

Ericom Zero Trust approach: Ericom Web Application Isolation is a next generation clientless ZTNA solution that renders organizations' public and private web apps in isolated containers, where granular access and data usage policies are applied to users who log in on unmanaged devices. File uploads, downloads, print screen and clip boarding functions may be disabled to protect sensitive information. Alternatively, permitted uploads may be sanitized within the isolated environment to prevent injection of malware, and downloads scanned with DLP to prevent exfiltration. No data from apps reaches a device's caches, eliminating data loss risk if devices are lost.

Discover how Ericom Security Solutions can safeguard your organization from web-delivered threats.

Contact us today for a personalized demonstration or to learn more about our scalable cloud-delivered service at ericom.com/contact-us.