




ZERO-TRUST WEB ISOLATION



Don't rely on outdated and ineffective detection mechanisms to protect your enterprise.



 kasmweb.com

 1765 Greensboro Station Pl McLean,
Virginia 22102

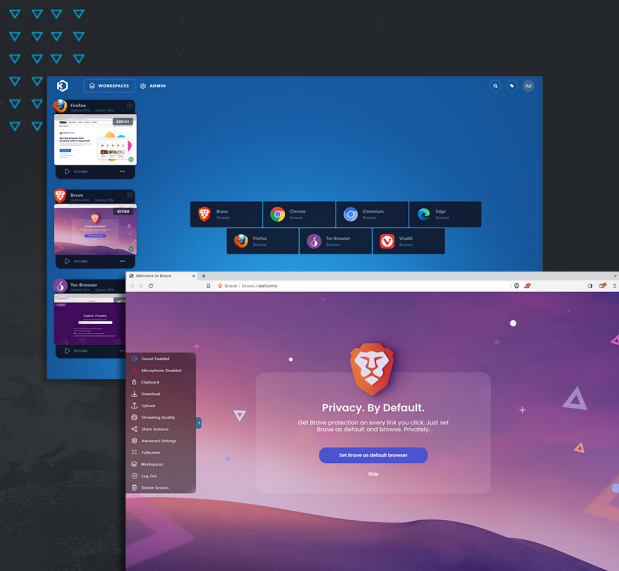
 571-444-5276

 info@kasmweb.com

Organizations of all sizes and sophistication fall victim to malware, phishing and ransomware attacks at an alarming rate. Even with a robust security strategy, it's clear that existing technology based on signatures and heuristics are not enough.



The Kasm Team of cybersecurity experts has spent the last 20 years defending the US Government against the most advanced and persistent threats. It is through this experience that we recognized that there is no firewall, mail gateway, data loss prevention agent or endpoint protection tool that is capable of stopping a determined adversary from exploiting your systems. That is why we created Kasm Workspaces Zero-Trust Web Isolation.



Web isolation moves the risk of browsing the web off the endpoint and outside of the enterprise. All web interactivity is executed in docker containers running in an isolated environment with only a seamless rendering user interface being sent to the user's browser. Users will feel as if they are experiencing the web firsthand, however, since web content never directly interacts with the local endpoint, your enterprise is protected against malware and your data remains safe

Open-in-isolation Browser Extension

The Kasm Open-In Isolation browser extension provides a browser context-menu option for opening a link or selected text in web isolation. Securely navigate the web by opening untrusted links with the malware protection and privacy of Kasm zero-trust web isolation.

Kasm Workspaces Zero-Trust Isolation Benefits



Prevent Malware Infection

Since the browsing activity is taking place in a separate, disposable container, any malicious code encountered is contained and does not affect the user's actual device. This could include ransomware, viruses, Trojans, or other types of malware.



Secure Sensitive Data

Because the browsing activity is isolated, sensitive data used within the browser is less likely to be exposed to spyware or keyloggers that may exist on the user's device.



Protect Against Phishing

Users who accidentally click on a phishing link will not expose their actual device or network to the attacker. Any harmful activity is confined to the container.



Provide Privacy

Prevent the disclosure of your identity and information by blocking trackers, ads, and other web-based trackers.

