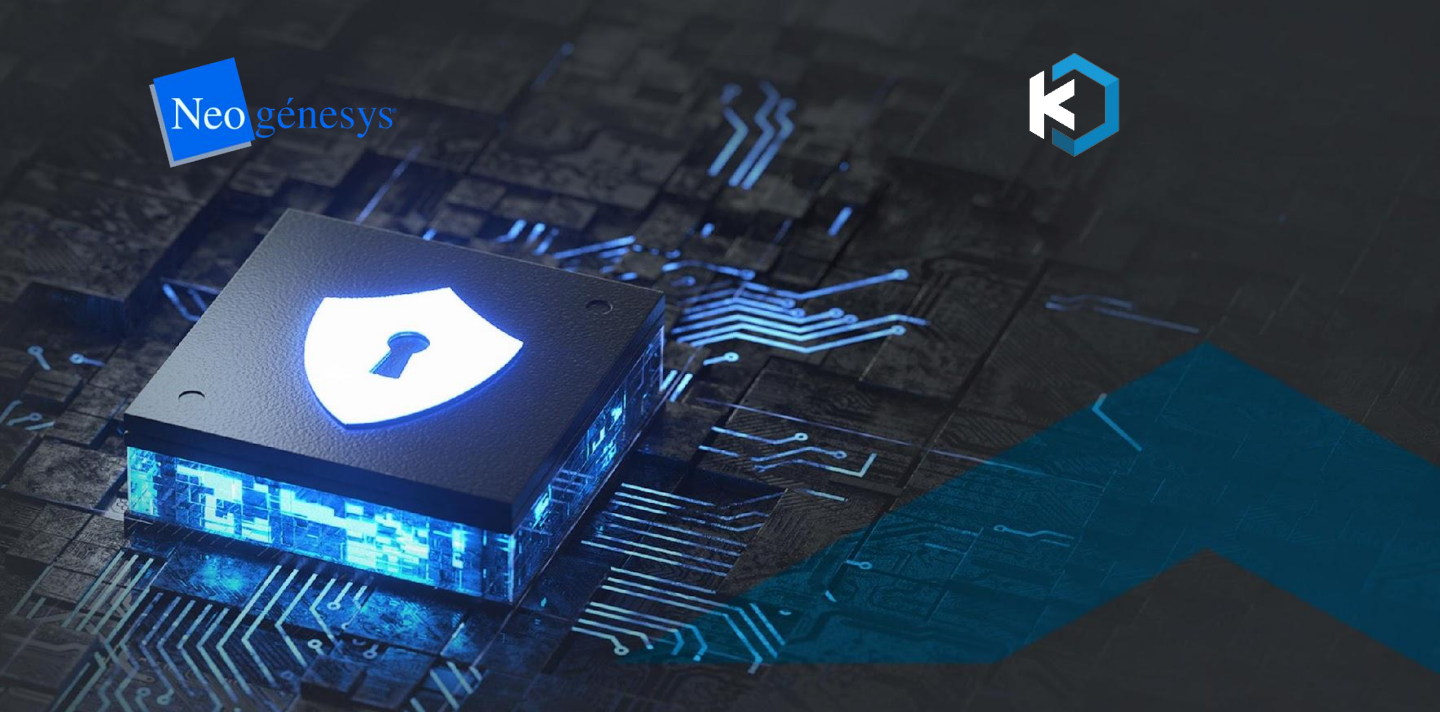
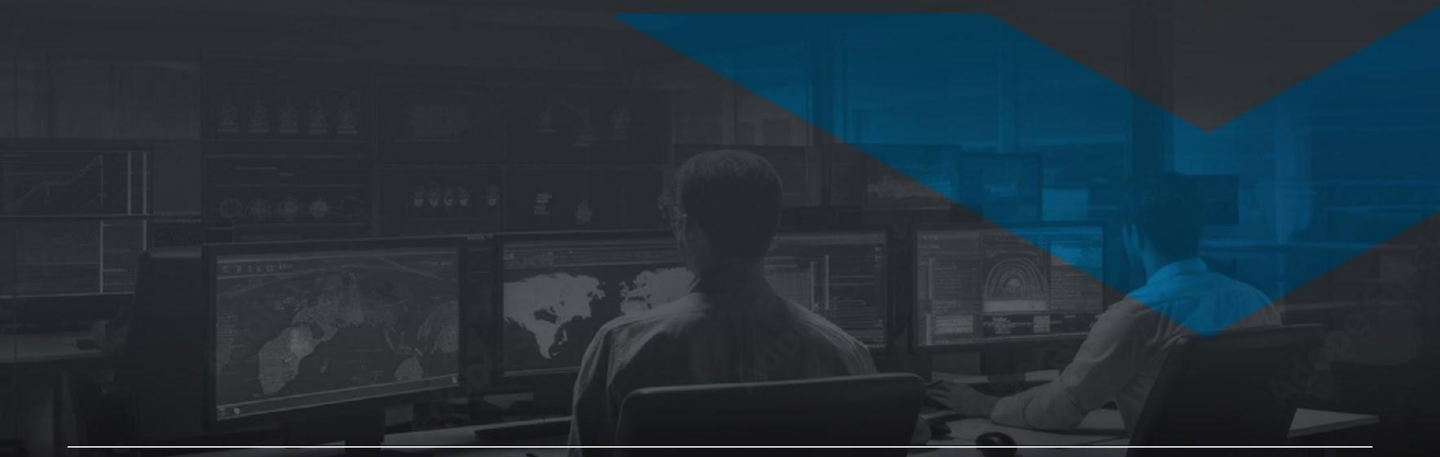
Neogénesys



ZERO-TRUST WEB ISOLATION

No confíe en mecanismos de detección obsoletos e ineficientes cuando se trata de proteger su empresa.



neogenesys.com.mx

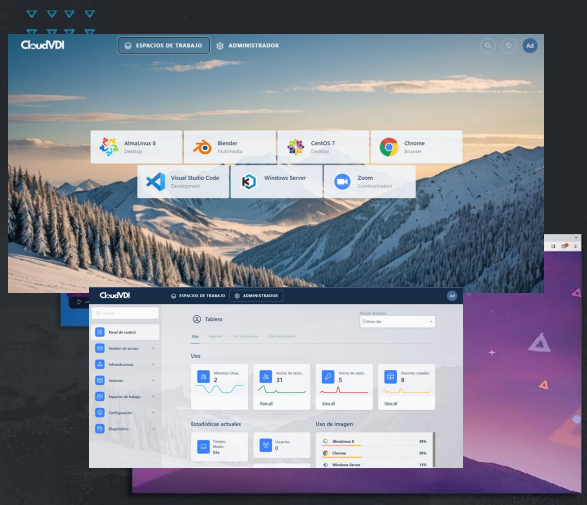
Boulevard Manuel Ávila Camacho 36,
Piso 10, Col. Lomas de Chapultepec,
México, 11000, CDMX

55 3155 6749

luis.perez@neogenesys.com

Organizaciones de todos los tamaños y sofisticación son víctimas de ataques de *malware*, *phishing* y *ransomware* a un ritmo alarmante. Incluso con una estrategia de seguridad robusta, está claro que la tecnología existente basada en firmas y heurística no es suficiente.

El equipo de expertos en ciberseguridad de Kasm ha dedicado los últimos 20 años defendiendo al Gobierno de los Estados Unidos contra las amenazas más avanzadas y persistentes. A través de esta experiencia, reconocimos que no hay *firewall*, *gateway* de correo, agente de prevención de pérdida de datos o herramienta de protección de *endpoints* que sea capaz de detener a un adversario decidido a explotar sus sistemas. Por eso creamos *Kasm Workspaces Zero-Trust Web Isolation*.



El aislamiento web elimina el riesgo de navegar por la web fuera del *endpoint* y de la empresa. Toda la actividad web se ejecuta en contenedores Docker que se ejecutan en un entorno aislado, enviando al navegador del usuario únicamente una interfaz de usuario renderizada sin fisuras.

Los usuarios se sentirán como si estuvieran experimentando la web de primera mano, sin embargo, como el contenido web nunca interactúa directamente con el *endpoint* local, su empresa está protegida contra el *malware* y sus datos permanecen seguros.

Extensión de navegador Open-in-isolation

La extensión para navegador **Kasm *Open-In Isolation*** proporciona una opción de menú contextual para abrir un enlace o texto seleccionado en web aislamiento. Navegue con seguridad por la web abriendo enlaces no fiables con la protección *antimalware* y la privacidad del Kasm *Zero-Trust Web Isolation*.

Beneficios de Kasm Workspaces Zero-Trust

Prevenir la infección por *malware*

Dado que la actividad de navegación tiene lugar en un contenedor separado y desechable, cualquier código malicioso que se encuentre está contenido y no afecta al dispositivo real del usuario, como *ransomware*, virus, troyanos u otros tipos de *malware*.

Protección contra el *phishing*

Los usuarios que accidentalmente hagan clic en un enlace de *phishing* no expondrán su dispositivo o red real al atacante. Cualquier actividad dañina se limita al contenedor

Protección de datos confidenciales

Dado que la actividad de navegación está aislada, es menos probable que los datos confidenciales utilizados en el navegador queden expuestos a programas espía o registradores de pulsaciones de teclas que puedan existir en el dispositivo del usuario.

Protección de la privacidad

Evite la divulgación de su identidad e información bloqueando rastreadores, anuncios y otros rastreadores web.

neogenesys.com.mx

Boulevard Manuel Ávila Camacho 36,
Piso 10, Col. Lomas de Chapultepec,
México, 11000, CDMX

55 3155 6749

luis.perez@neogenesys.com