KerioControl

RESUMEN

Para bancos y cooperativas de crédito

Segmentación Zero Trust y control auditado en cada ubicación.

Firewall de próxima generación y gestión unificada de amenazas desplegados en su propia infraestructura, en el perímetro de cada ubicación, sin coste de VPN por sitio.

Denegar todo
por defecto

Todas las conexiones en todas las ubicaciones quedan bloqueadas a menos que se permitan explícitamente y se asignen a una identidad verificada (AD/LDAP). Un dispositivo o credencial comprometidos no pueden avanzar lateralmente hacia otras zonas.

Segmentación Zero Trust, por defecto



Cómo funciona: mecanismo de puerta de enlace, luego IA

1 **Despliegue en las instalaciones**
Appliance virtual, su propio hardware o un appliance dedicado de la serie NG: el tráfico principal y la aplicación de políticas se ejecutan en la infraestructura que controla su institución.

2 **Control de acceso VPN en capas**
Credenciales, autenticación de dos factores y, a continuación, una comprobación de Trusted Device vinculada al hardware (huella de 7 atributos; aprobación y revocación por parte del administrador; registro completo de auditoría).

3 **Supervisión automática del tiempo de actividad**
Watchdog supervisa continuamente los servicios de red, firewall, VPN e IPS; reinicia automáticamente los que fallen y registra un volcado de memoria para su revisión, sin necesidad de una visita manual al sitio.

4 **Bloqueo de amenazas asistido por IA (Shield Matrix)**
La IA en la nube y la inteligencia global de honeypots bloquean direcciones IP maliciosas antes de que lleguen a la red; la inteligencia de amenazas se actualiza cada 15 minutos, sin carga adicional en el appliance.

Cumplimiento: línea base global

Comité de Basilea: principios de riesgo operativo y resiliencia Conmutación por error de alta disponibilidad activa/pasiva (una licencia cubre ambos nodos), además de la autorrecuperación Watchdog de los servicios de red centrales.	Compatible con
Control de acceso y segregación de funciones (EE. UU. GLBA/FFIEC; UE DORA; Reino Unido FCA/PRA; Singapur MAS TRM; Australia APRA CPS 234; Canadá OSFI B-13) Segmentación Zero Trust con política 'deny-all' y reglas mapeadas por identidad, además de un registro administrativo completo de auditoría de cada aprobación, denegación y revocación de dispositivos.	Capacidad
Supervisión centralizada en todas las ubicaciones GFI AppManager AI le permite administrar múltiples appliances y varios sitios desde una única consola.	Capacidad

¿Listo para empezar?

Solicite una prueba gratuita en gfi.ai o póngase en contacto con el departamento de ventas: sales@gfi.com.

Copyright © GFI USA, LLC. Todos los derechos reservados.