KerioControl

SCHEDA SINTETICA

Per banche e cooperative di credito

Segmentazione Zero Trust e controlli verificati in ogni sede.

Firewall di nuova generazione e gestione unificata delle minacce (UTM) distribuiti sulla tua infrastruttura, al perimetro di ogni sede, senza costi VPN per sito.

Nega tutto
per impostazione predefinita

Ogni connessione tra tutte le sedi è bloccata, salvo esplicita autorizzazione e associazione a un'identità verificata (AD/LDAP). Un dispositivo o una credenziale compromessi non possono spostarsi lateralmente verso altre zone.

Segmentazione Zero Trust, per impostazione predefinita



Come funziona: meccanismo del gateway, poi l'IA

1 — Distribuzione on-premise
Appliance virtuale, hardware proprio o un'appliance dedicata della serie NG: il traffico principale e l'applicazione delle policy vengono eseguiti su un'infrastruttura controllata dalla tua istituzione.

2 — Controllo degli accessi VPN multilivello
Credenziali, poi autenticazione a due fattori, quindi verifica del Trusted Device vincolata all'hardware (impronta a 7 attributi, approvazione/revoca da parte dell'amministratore, audit trail completo).

3 — Disponibilità monitorata automaticamente
Watchdog controlla continuamente la rete, il firewall, la VPN e i servizi IPS e riavvia automaticamente quelli che si arrestano, registrando un dump di crash per la revisione, senza interventi in loco.

4 — Blocco delle minacce assistito dall'IA (Shield Matrix)
L'IA cloud e l'intelligence globale dei honeypot bloccano gli IP malevoli prima che raggiungano la rete; l'intelligence sulle minacce si aggiorna ogni 15 minuti, senza carico aggiuntivo sull'appliance.

Conformità: baseline globale

Comitato di Basilea: principi relativi al rischio operativo e alla resilienza Failover attivo/passivo ad alta disponibilità (una licenza copre entrambi i nodi) più il recupero automatico dei servizi di rete core tramite Watchdog.	Supporta
Controllo degli accessi e segregazione dei compiti (US GLBA/FFIEC; EU DORA; UK FCA/PRA; Singapore MAS TRM; Australia APRA CPS 234; Canada OSFI B-13) Segmentazione Zero Trust «Nega tutto» con regole associate all'identità, oltre a un audit trail amministrativo completo per ogni approvazione, diniego e revoca dei dispositivi.	Funzionalità
Supervisione centralizzata in tutte le sedi GFI AppManager AI ti permette di gestire più appliance e numerose sedi da un'unica console.	Funzionalità

Pronto per iniziare?

Richiedi una prova gratuita su gfi.ai oppure contatta l'ufficio commerciale: sales@gfi.com.

Copyright © GFI USA, LLC. Tutti i diritti riservati.