KerioControl

KURZÜBERSICHT

Für Banken und Kreditgenossenschaften

Zero-Trust-Segmentierung und geprüfte Kontrolle an jedem Standort.

Next-Generation-Firewall und Unified Threat Management auf Ihrer eigenen Infrastruktur an der Peripherie jedes Standorts, ohne VPN-Kosten pro Standort.

Alles blockieren

standardmäßig

Jede Verbindung zwischen allen Standorten ist blockiert, sofern sie nicht ausdrücklich erlaubt und einer verifizierten Identität (AD/LDAP) zugeordnet ist. Ein kompromittiertes Gerät oder kompromittierte Zugangsdaten können nicht in andere Zonen vordringen.

Zero-Trust-Segmentierung, standardmäßig



So funktioniert es: Gateway-Mechanismus, dann KI

1 — On-Premises-Bereitstellung

Virtuelle Appliance, eigene Hardware oder eine dedizierte NG-Series-Appliance: Datenverkehr und Durchsetzung der Richtlinien laufen auf Infrastruktur, die Ihre Institution kontrolliert.

2 — Mehrstufige VPN-Zugangskontrolle

Zugangsdaten, dann Zwei-Faktor-Authentifizierung und anschließend die hardwaregebundene Prüfung des vertrauenswürdigen Geräts (7-Attribut-Fingerabdruck, Administrator: Freigabe/Widerruf, vollständiger Audit-Trail).

3 — Selbstüberwachte Verfügbarkeit

Der Watchdog überwacht kontinuierlich Netzwerk-, Firewall-, VPN- und IPS-Dienste und startet ausgefallene Dienste automatisch neu; dabei wird ein Crash-Dump zur Analyse protokolliert — ganz ohne Vor-Ort-Einsatz.

4 — KI-gestützte Bedrohungsabwehr (Shield Matrix)

Cloud-KI und globale Honeypot-Intelligenz blockieren bösartige IP-Adressen, bevor sie das Netzwerk erreichen; Bedrohungsinformationen werden alle 15 Minuten aktualisiert, ohne zusätzliche Last für die Appliance.

Compliance-tauglich: globaler Basisstandard

Basler Ausschuss für Bankenaufsicht: Grundsätze zu operationellem Risiko und Resilienz Aktives/passives Hochverfügbarkeits-Failover (eine Lizenz deckt beide Knoten ab) sowie Watchdog-Selbstwiederherstellung für zentrale Netzwerkdienste.	Unterstützt
Zugriffskontrolle und Aufgabentrennung (US GLBA/FFIEC; EU DORA; UK FCA/PRA; Singapur MAS TRM; Australien APRA CPS 234; Kanada OSFI B-13) Zero-Trust-'Deny-All'-Segmentierung mit identitätszugeordneten Regeln sowie vollständigem Admin-Audit-Trail für jede Gerätefreigabe, -ablehnung und -widerruf.	Funktion
Zentrale Aufsicht über alle Standorte GFI AppManager AI ermöglicht Ihnen, mehrere Appliances und zahlreiche Standorte von einer Konsole aus zu verwalten.	Funktion

Bereit loszulegen?

Fordern Sie eine kostenlose Testversion an unter gfi.ai oder kontaktieren Sie den Vertrieb: sales@gfi.com.

Copyright © GFI USA, LLC. Alle Rechte vorbehalten.