IRONCHIP

Comparativa Técnica

ITDR IRONCHIP VS CISCO DUO

COMPARATIVA TÉCNICA DETALLADA

	Ironchip ITDR	Cisco Duo
Modelo de seguridad	✓ Identidad + Dispositivo único + Localización RF + Contexto (tiempo/actividad) + ITDR	✗ Identidad + Dispositivo/OS/estado + IP/país/red + RBA (riesgo en login)
Señales de localización	✓ Radiofrecuencia (no GPS/IP), Zonas seguras personalizadas por usuario; detecta viajes imposibles y ocultación por GPS/IP falsos	✗ Geolocalización basada en IP/país/red; políticas por ubicación/redes; detección de redes anónimas en planes altos
Análisis de SIM / SIM-swap	✓ Sí: analiza SIM (origen/destino/portabilidad) y detecta SIM-swap y fraudes asociados	✗ No nativo (usa app/push, FIDO2, OTP; recomienda evitar SMS por SIM-swap).
Detección vishing	✓ Sí: señal “usuario en llamada” durante autenticación (posible vishing).	✗ No público; foco en factores/políticas y RBA en el momento del login.

	Ironchip ITDR	Cisco Duo
Detección de tampering	✓ Sí: dispositivos emulados, apps depuradas, root/jailbreak, señales de malware.	✗ Postura de dispositivo: root/jailbreak móviles, salud del endpoint (firewall, cifrado, AV, versión); Trusted Endpoints.
ITDR (detección y respuesta)	✓ Sí: alerta y bloqueo en tiempo real ante amenazas de identidad (fraude, suplantación, viajes imposibles, señales anómalas).	✗ Detección de anomalías (Trust Monitor / RBA) con enfoque en login; visibilidad/alerta; bloqueo condicionado por políticas.
Resiliencia a evasión por red	✓ Alta: no depende de IP/GPS; resistente a CGNAT, VPN, proxys, Private Relay.	✗ Dependencia de IP/red para parte de las decisiones; puede requerir bloquear anonymizers y ajustar políticas por país/red.
Passwordless	✓ Sí (sin móvil opcional). USB estándar, smartcards NFC, OTP in-app, push, email sin agente, etc.	✗ Sí: Passkeys/FIDO2/WebAuthn, push, OTP, tokens.
Hardware	✓ USB estándar (no FIDO2), smartcards NFC; sin móvil si se requiere.	✗ FIDO2/WebAuthn keys (YubiKey, etc.), tokens; smartcard/PIV en ciertos escenarios.

	Ironchip ITDR	Cisco Duo
Cobertura de plataformas	✓ Autenticador en cualquier OS móvil y ordenador; protege web, SSO, apps propias, y logon físico y remoto (Win/Linux/macOS).	✗ Amplio: web/SSO/VPNs y logon en Windows, macOS y Linux (Unix/PAM).
Políticas adaptativas	✓ Granularidad total: usuario, grupo, app, dispositivo, postura, zona segura, horario, señales RF/SIM/vishing, riesgo dinámico.	✗ Políticas por usuario/grupo/app, ubicación/IP/red, OS/versión, salud endpoint; RBA (riesgo en login) y Verified Push.
Respuesta automática	✓ Bloqueo/step-up inmediato por riesgo y brechas; orquestación con ITDR.	✗ Step-up/deny en login según políticas y RBA; anomalías visibles para actuación.
Integraciones	✓ Microsoft y no-Microsoft: apps externas, apps in-house, máquinas Windows/Linux/macOS (físico y remoto).	✗ Amplias integraciones (Microsoft 365, VPNs, SSO, RDP/macOS/Unix, SaaS).
Operación sin móvil	✓ Nativa (USB/Smartcard/OTP/Email)	✗ Sí (FIDO2 keys, tokens), pero orientado a móvil/push.

	Ironchip ITDR	Cisco Duo
Coste/TCO	✓ Menor fraude + menor dependencia de MDM + USB estándar más económico + menos “fatiga MFA” = TCO inferior.	✗ Licenciamiento por niveles; posible necesidad de tier alto para capacidades avanzadas + coste de FIDO2/MDM.

LA DIFERENCIA ESTRATÉGICA QUE CISCO DUO NO PUEDE REPLICAR

Ironchip cambia el paradigma de protección de identidad al combinar autenticación sin fricciones con inteligencia de localización por radiofrecuencia y detección y respuesta a amenazas de identidad (ITDR) en tiempo real. Esto permite detectar y bloquear ataques que MFA tradicional no ve (ingeniería social, SIM-swap, ocultación por VPN/Proxy, GPS/IP falsos, viajes imposibles, dispositivos emulados o rooteados/jailbreakeados), reduciendo fraude, coste y esfuerzo operativo.

1. **Señales únicas y anti-evasión** (RF + SIM + **zonas seguras** + huella de dispositivo + señales de vishing).

2. I**TDR en tiempo real** (alerta y **bloqueo automático**).

3. **Cobertura sin móvil (USB estándar y smartcards NFC**; accesos web, apps propias y logon físico/remoto en **Windows, Linux y macOS**).

4. **Políticas adaptativas 100% granulares con contexto de riesgo real** (persona-dispositivo-lugar-momento).

5. **TCO inferior**: menos fraudes y menos mantenimiento (sin **MDM obligatorio**, **USB estándar**, reducción de helpdesk y fatiga MFA).