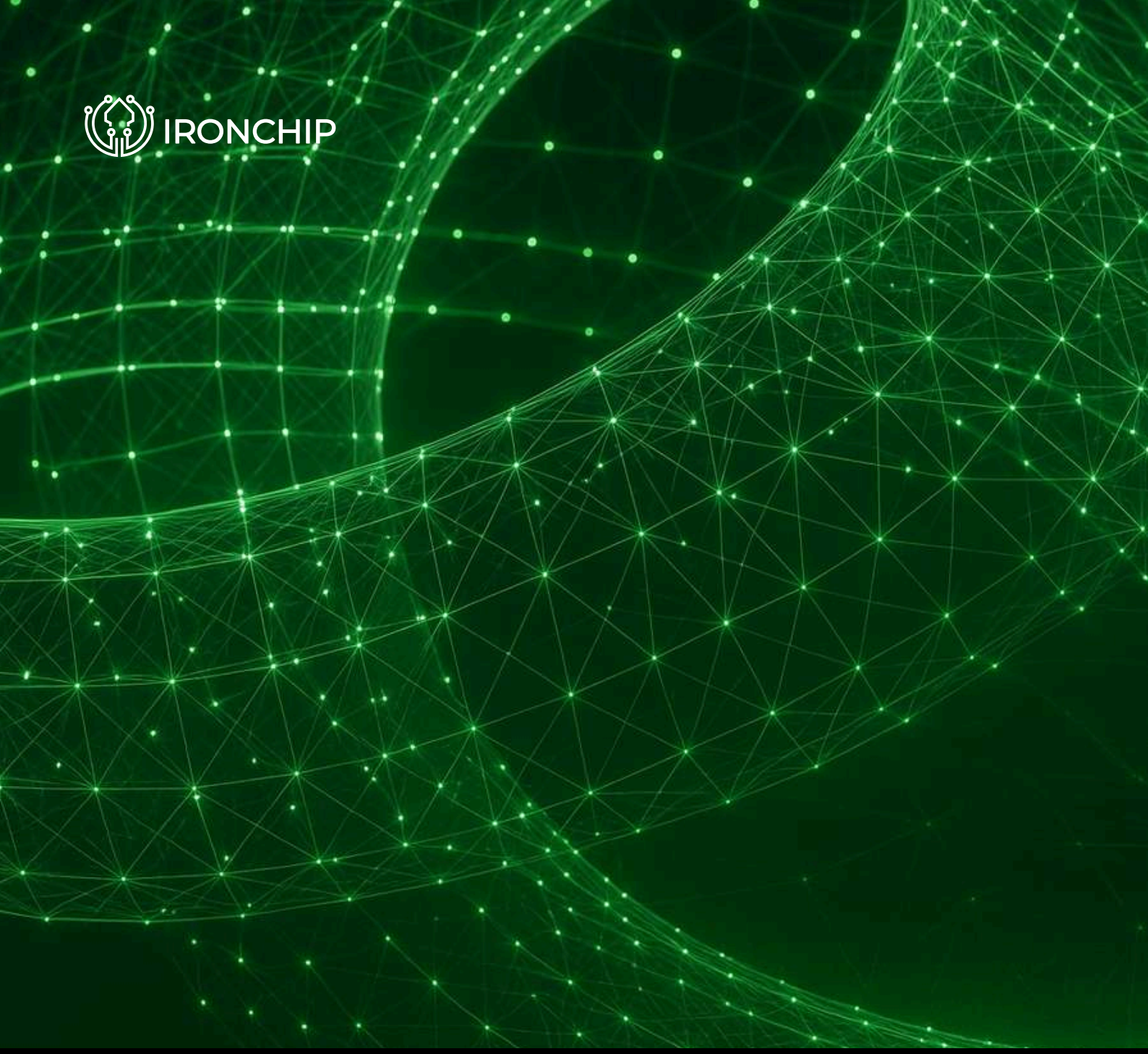

Comparativa técnica

Ironchip VS Fortitoken

Análisis comparativo de características técnicas

Comparativa técnica: Ironchip vs Fortitoken

IRONCHIP

Especialización

Plataforma de identidad avanzada especializada en autenticación sin contraseñas y detección y respuesta automática ante robos de cuenta basada en localización segura.

FORTINET

Especialización

Firewalls y elementos de red. De manera residual trabajan Fortitoken, una solución de autenticación minima compatible solo con elementos de Fortinet.

Por qué esta comparativa?

La seguridad digital exige soluciones que combinen fiabilidad, innovación y cumplimiento normativo. En este documento se contrastan dos enfoques: la autenticación sin contraseñas y basada en geolocalización de confianza de Ironchip, frente al modelo tradicional de autenticación por tokens digitales. Esta comparativa permite identificar cómo Ironchip aporta una capa adicional de seguridad y usabilidad frente a alternativas convencionales.

	Ironchip	Fortinet
FILOSOFÍA DE SEGURIDAD		
Paradigma Principal	✓ Identidad de Confianza Cero (Zero Trust Identity). No confía en ningún factor por sí solo y verifica continuamente la identidad basándose en el contexto físico y digital.	✗ Autenticación Multifactor (MFA/2FA). Se centra en añadir una segunda capa de verificación (algo que tienes o eres) a la contraseña.
Enfoque	✓ Proactivo y Continuo. Analiza el contexto de cada interacción para detectar comportamientos fraudulentos antes de que se completen.	✗ Reactivo. Responde a una solicitud de inicio de sesión con un desafío de autenticación.
TECNOLOGÍA DE UBICACIÓN		
Método de Geolocalización	✓ Basado en Análisis de Radiofrecuencia (RF). Crea una "huella digital" única de la ubicación física analizando las señales de red (2G-5G, WiFi, etc.).	✗ Basado en Geolocalización por IP. Utiliza la dirección IP pública del dispositivo para estimar su ubicación.
Fiabilidad y Precisión	✓ Extremadamente Alta y Fiable. La ubicación física se verifica con certeza criptográfica. Permite crear "Zonas Seguras" verificadas.	✗ Baja y Decreciente. Vulnerable a la falsificación con VPNs, proxies y afectado por CGNAT. Impreciso por naturaleza.

	Ironchip	Fortinet
TECNOLOGÍA DE UBICACIÓN		
Detección de "Viaje Imposible"	✓ Automática y Precisa. Detecta instantáneamente si un acceso se origina desde una ubicación físicamente imposible en relación con el último acceso legítimo, basándose en la huella de RF.	✗ Limitada y Poco Fiable. Puede generar alertas basadas en cambios de IP entre países, pero es propenso a falsos positivos (viajes, uso de VPNs) y falsos negativos (un atacante usando una VPN local).
ANÁLISIS DE DISPOSITIVO		
Identificación del Dispositivo	✓ Identificación Unívoca del Dispositivo (Huella Digital). Crea un identificador único y persistente para cada hardware, independientemente de reinstalaciones de apps o formateos.	✗ Identificación básica, a menudo ligada a la instancia de la aplicación FortiToken o a registros en FortiClient EMS.
Detección de Tampering	✓ Avanzada y Profunda. Detecta root/jailbreak, emuladores de dispositivos, aplicaciones en modo depuración y otras herramientas típicas de malware y ciberdelincuentes.	✗ Básica (con FortiClient EMS). Puede detectar si un dispositivo está rooteado (Android) o jailbreakeado (iOS).
Análisis de Comportamiento	✓ Análisis de Comportamiento del Usuario y del Dispositivo (UEBA). Aprende patrones de uso para detectar anomalías que puedan indicar un compromiso.	✗ Nulo. El análisis se centra en el estado del dispositivo, no en cómo se utiliza.

	Ironchip	Fortinet
DETECCIÓN DE AMENAZAS		
Ataques de Ingeniería Social	✓ Resistente. Aunque el atacante robe las credenciales, el acceso se bloqueará al originarse desde un dispositivo no reconocido y/o una ubicación imposible.	✗ Vulnerable. Si un atacante roba la contraseña y el código OTP (por ejemplo, mediante un ataque Man-in-the-Middle), FortiToken validará el acceso.
Fraude por SIM Swapping	✓ Inmune. La autenticación está ligada a la huella digital del dispositivo físico, no al número de teléfono o la tarjeta SIM. Un cambio de SIM no afecta la seguridad.	✗ Vulnerable. Si el 2FA se basa en SMS o llamada, un ataque de SIM swapping exitoso le da al atacante el control total del segundo factor.
INTEGRACIÓN Y CASOS DE USO		
Ecosistema Principal	✓ Agnóstico al Proveedor. Se integra con cualquier servicio o plataforma, sea de Fortinet, Cisco, Palo Alto, o cualquier otro.	✗ Fortinet Security Fabric. Fuerte integración con FortiGate, FortiAuthenticator, FortiClient EMS. Diseñado para funcionar de manera óptima dentro de este entorno.
Aplicaciones Soportadas	✓ Cualquier Activo Digital: - Apps en la nube (Microsoft 365, G-Suite, Salesforce) - Apps de desarrollo propio (in-house) - Acceso a estaciones de trabajo (Windows, Linux, Mac) - Acceso a VPNs y VDI.	✗ Acceso VPN, acceso a aplicaciones protegidas por FortiGate, servicios en la nube (vía SAML/RADIUS desde FortiAuthenticator).

	Ironchip	Fortinet
INTEGRACIÓN Y CASOS DE USO		
Acceso sin Contraseña (Passwordless)	✓ Nativo. Permite un acceso totalmente sin contraseña, utilizando el propio dispositivo como un factor de autenticación seguro y verificado por biometría y contexto.	✗ Limitado. El foco principal sigue siendo el 2FA (algo que sabes + algo que tienes).
Políticas de Acceso Condicional	✓ Avanzadas e Hiper-Contextuales. Basadas en ubicación física verificada por RF, confianza del dispositivo, hora, patrón de comportamiento, y cualquier combinación de estos factores.	✗ Básicas. Basadas en IP, tipo de dispositivo, grupo de usuario, y estado del endpoint (con FortiClient).
Autenticadores multiOS	✓ FortiToken Mobile y tokens físicos; experiencia más centrada en movilidad o tokens.	✗ Autenticador que funciona en cualquier SO (móvil y ordenador); además USB & NFC.

	Ironchip	Fortinet
MODELO DE COSTE Y VALOR		
Estructura de Coste	✓ Modelo de suscripción por usuario que incluye todas las capacidades avanzadas de detección y respuesta.	✗ Basado en licencias por usuario (paquetes perpetuos o suscripciones) y coste de hardware (tokens físicos). El coste inicial puede ser bajo pero limitado en funcionalidad.
Retorno de la Inversión (ROI)	✓ Previene ataques sofisticados (ATO, fraude, ingeniería social) que tienen un impacto económico y reputacional devastador. El ROI se mide en las brechas que nunca ocurrieron.	✗ Previene ataques básicos de fuerza bruta o uso de contraseñas robadas.

Ironchip, una solución de calidad ligada a la excelencia

Autenticación sencilla y fluida que mejora la experiencia del usuario.

Adaptación garantizada a los estándares de seguridad más exigentes.

Tecnología preparada para crecer junto con las necesidades de la organización.

Protección activa frente a accesos fraudulentos y amenazas emergentes.

Accesos unificados y sin contraseñas, sin necesidad de formación extra.

Compatibilidad garantizada con entornos corporativos y proveedores externos.

> Ironchip implementa su producto en un punto clave de la autenticación de manera sencilla, no costosa y combinada con una experiencia de usuario difícil de encontrar hoy en día.
>
> — Fátima Cereijo, Gerente de Control de Fraude y Privacidad en Abanca

Fight Againts identity threats

IRONCHIP TELCO S.L
info@ironchip.com