COMPARATIVA MICROSOFT AUTH. VS IRONCHIP

Microsoft, con Microsoft Entra ID, ofrece una solución de identidad que se integra de forma nativa en su ecosistema y servicios. En cambio, Ironchip se distingue por su seguridad sin contraseñas y su objetivo de centralizar todos los accesos de cualquier servicio o sistema, utilizando la inteligencia de localización para prevenir fraudes de manera proactiva. Mientras Microsoft se centra en la gestión de accesos dentro de su entorno, Ironchip busca unificar la autenticación de todos tus servicios, sin importar la plataforma.

COMPARACIÓN DE CARACTERISTICAS CLAVES		
Integración con ecosistemas	Diseñado para centralizar accesos de cualquier servicio o sistema, independientemente de la plataforma.	Principalmente centrado en el ecosistema de Microsoft (Azure, 365, etc.), con complejidades fuera de este.
Métodos de autenticación	Múltiples opciones, incluyendo aplicaciones de escritorio, tarjetas, tokens USB, y correo electrónico.	Dependiente en gran medida de dispositivos móviles con y la aplicación Authenticator.
Soporte diferentes SSOO	Autenticador soportado en cualquier sistema operativo, Windows, Linux, Mac, Android e iOS.	Autenticador soportado solo en móviles Android e iOS.
Conectividad con servidores	Integración nativa con servidores propios (nube o físicos) mediante protocolos como SSH y RDP.	Si permite, pero solo a servidores Microsoft
Integraciones Ad-Hoc	Facilidad para integrar aplicaciones propietarias mediante código y HTTPS.	Dificultad para integrar soluciones fuera de las APIs de Microsoft, especialmente en aplicaciones Ad-Hoc.
Uso de localización como factor de seguridad	Uso de localización (más allá de la IP) para reconocer ubicaciones de conexión, previniendo accesos anómalos.	El uso de geolocalización se limita a la IP, ofreciendo un control de acceso menos granular.
Acceso Multi-dominio	Permite acceso a proveedores con MFA en dominios diferentes (Multidomain).	La gestión de acceso entre diferentes dominios puede ser compleja y limitada.

COMPARACIÓN DE CARACTERISTICAS CLAVES		
Gestión de alias/buzones	Capacidad para gestionar alias de correo (ej. admini@empresa.com) y asociar con identidad real.	No ofrece una gestión de alias de correo o buzones compartidos para autenticación.
Autenticaciones delegadas	Autenticaciones delegadas y dependientes de varios usuarios reales.	No permite autenticaciones delegadas.
Detección y Respuesta ante Intrusiones	Sistema de detección y bloqueo de intrusos robusto, con bajas tasas de falsos positivos.	Detección de intrusos con altas tasas de falsos positivos.
Personalización de reglas	Reglas de autenticación personalizables en base a múltiples factores, incluyendo geolocalización precisa y perfiles de usuario.	Las reglas de acceso condicional son más rígidas y se basan en un conjunto limitado de factores predefinidos.
Personalización de la interfaz	Flujo de autenticación personalizable con identidad corporativa reduciendo el riesgo de phishing.	Flujo de autenticación no personalizable, lo que facilita suplantaciones de identidad.
Alertas y SIEM/SOC	Parametrización avanzada y envío de datos y alertas a SOC/SIEM con baja complejidad.	Alta complejidad en la parametrización de alertas y la integración con herramientas de seguridad externas.
Gestión de Acceso Privilegiado (PAM)	Módulo PAM integrado que no requiere licencias adicionales, simplificando la gestión de accesos fisicos y remotos a cualquier sistema operativo Windows, Linux y Mac.	La gestión de acceso entre diferentes dominios puede ser compleja y limitada.
Modelo de costes	Precios competitivos y funcionalidades clave sin costos adicionales.	Gestión de accesos no integrado de manera nativa, y solo soporta gestión de accesos a sistemas Windows.