IRONCHIP

Casos de Uso de Ironchip para Administraciones Públicas

Fortaleciendo la Ciberseguridad con Cumplimiento ENS e Identity Threat Detection and Response (ITDR)

¿Por qué Ironchip? Versatilidad y Seguridad Passwordless

La gestión de información crítica (datos ciudadanos, expedientes, infraestructuras) exige una protección inquebrantable, a menudo con recursos limitados y equipos muy diversos. Ironchip es el aliado estratégico que ofrece soluciones sin contraseñas, robustas, versátiles y seguras.
Una de las características importantes de la tecnología Ironchip es que está certificada y gracias a ellos en el catálogo **CPSTIC** del **CCN** , imprescindible para el cumplimiento del **ENS** dentro de las AAPP

Versatilidad en Métodos de Autenticación:

- USB, Smart Cards NFC.
- Equipos portátiles y de sobremesa (Windows, Linux, Mac).
- Móviles Android e iOS.

Naturaleza Totalmente Passwordless: Elimina contraseñas, neutralizando phishing, keylogging y fuerza bruta.

Identity Threat Detection and Response (ITDR): Detección y neutralización automática de robos de cuenta y accesos no autorizados mediante inteligencia de localización y análisis de comportamiento. Frustra ataques de ingeniería social y falsificación de biometría.

IRONCHIP

FINANCIADA POR ENISA

MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

Gobiernos y AAPP : Fortaleciendo la Gobernanza Digital

Caso de Uso 1

Protección en Acceso Remoto (Citrix) sin móviles

Las administraciones públicas en España utilizan Citrix por una combinación de factores que incluyen la **seguridad, la flexibilidad, la eficiencia y la continuidad del negocio**, especialmente relevantes en un contexto de transformación digital y auge del teletrabajo.

Problema

- Los modelos de autenticación tradicionales (con contraseñas) son vulnerables a ataques de phishing y de credenciales robadas, especialmente en entornos de teletrabajo, donde el riesgo de ingeniería social aumenta.
- La falta de una aplicación móvil corporativa única o la reticencia del personal a usar sus dispositivos personales para autenticación dificulta la implementación de soluciones MFA robustas y uniformes
- Control y visibilidad total de los accesos como requiere el ENS, en muchos casos, las administraciones no conocen desde donde se están conectando o lo hacen de lugares no confiables, poniendo en riesgo la institución.

Solución

- Elimina el phishing al ser passwordless, ya que no hay contraseña que robar o interceptar, haciendo la autenticación más resistente a la mayoría de los ciberataques.
- En Ironchip permitimos el uso de tarjetas NFC, tokens USB, aplicaciones de escritorio, mailing o utilizar ubicaciones como identificación.
- ITDR detecta patrones anómalos (cambios bruscos de geolocalización, horarios inusuales, dispositivos no reconocidos) en tiempo real, incluso si el dispositivo móvil no es corporativo o si el acceso se realiza desde un equipo sin app específica, enviando la información a los SOCs..

IRONCHIP

Gobierno de La Rioja

En el Gobierno de La Rioja, la implementación de la tecnología de **Ironchip** ha sido un pilar fundamental para nuestra seguridad y gestión de accesos. Lo que más nos satisface es la **cobertura integral** que nos ofrece, permitiéndonos asegurar el servicio de **Citrix** y unificar el inicio de sesión en todos nuestros equipos, ya sean **Windows, Linux o Mac**.

Además, la capacidad de enviar toda esta información a nuestro **SOC** es crucial. Nos proporciona una **visibilidad centralizada** de todos los accesos, facilitando la **monitorización y detección proactiva de cualquier comportamiento anómalo**. Ironchip ha simplificado nuestra arquitectura de seguridad y nos da la tranquilidad de saber que estamos vigilando cada interacción de forma eficiente.

"El **modelo de autenticación sin móviles** es increíblemente cómodo y nos permite una **integración total con cualquier aplicación**, incluyendo las nuestras. Mantenemos nuestra **identidad corporativa en todas las vistas**, ofreciendo una experiencia de usuario fluida y coherente. **Seguridad, comodidad y marca, todo en uno.**"

Tomás Gómez, CISO

Gobiernos y AAPP : Fortaleciendo la Gobernanza Digital

Caso de Uso 2

Protección de Acceso Físico y Remoto (Windows, Linux, Mac)

Las administraciones públicas en España utilizan Citrix por una combinación de factores que incluyen la **seguridad, la flexibilidad, la eficiencia y la continuidad del negocio**, especialmente relevantes en un contexto de transformación digital y auge del teletrabajo.

Problema

- Heterogeneidad de sistemas operativos (Windows, Linux, Mac) en las administraciones, lo que complica una gestión de seguridad unificada, consistente y escalable, exigiendo soluciones específicas para cada plataforma.
- Persistencia de la dependencia de contraseñas débiles o reutilizadas para el acceso a equipos, lo que representa un punto ciego crítico y una puerta de entrada para ataques de fuerza bruta o robo de credenciales.
- La ausencia de un método de autenticación centralizado y seguro para todos los dispositivos y SO, lo que conduce a una gestión descentralizada y a menudo menos robusta de la seguridad de los puntos finales.

Solución

- Ofrece seguridad passwordless unificada para todos los sistemas operativos, simplificando drásticamente la gestión y auditoría de la autenticación en el parque informático.
- Proporciona agilidad y seguridad por no utilizar contraseñas con métodos de acceso (USB, smart cards NFC, autenticación desde móviles), con un doble factor automático en modo online y offline.
- Gestión centralizada y monitorizada de todos los dispositivos y distribución vía GPO fácil. Control total de los dispositivos y lugares de conexión.

Parlamento vasco

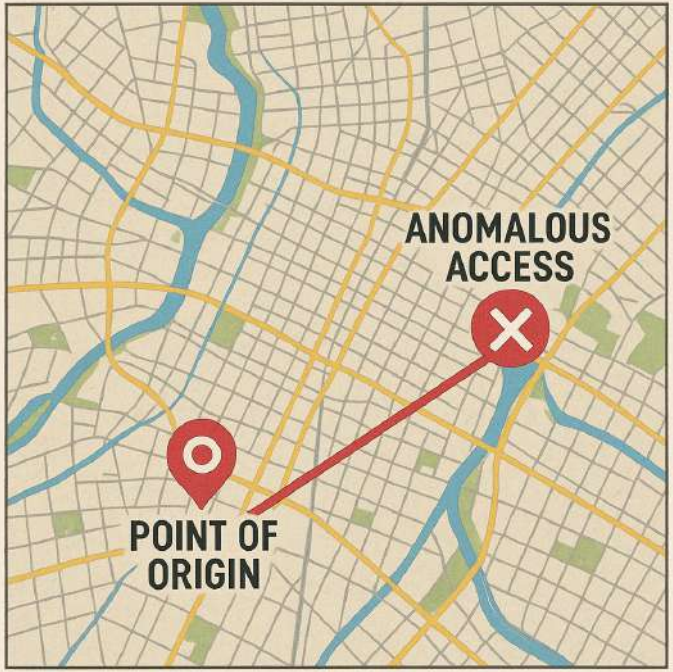
Reduce drásticamente la superficie de ataque al eliminar las contraseñas, mejora la experiencia de usuario al simplificar el acceso, y permite una gestión de seguridad más eficiente y centralizada, cumpliendo con el ENS (Identificación y Autenticación, Protección de la Información).

“Eliminar las contraseñas en Windows ha sido un acierto para el Gobierno Vasco. Como director, valoro cómo reduce el trabajo operativo de TI al eliminar los reseteos y, para los políticos, el acceso es ahora mucho más cómodo, online y offline. ***Una mejora clara en eficiencia y usabilidad.”***

Juanjo Arruza, Director de Sistemas

Gobiernos y AAPP : Fortaleciendo la Gobernanza Digital

Caso de Uso 3



Protección de Acceso de proveedores

Los accesos remotos de proveedores a través de VPN o RDP puede poner en peligro las instituciones. Con Ironchip, es fácil implantar sistemas de MFA para proveedores sin exigencia de hardware o dispositivos móviles.

Problema

- En muchos casos, los proveedores se conectan remotamente usando mail genéricos como proveedor@company. No obstante, es difícil conocer realmente la identidad que se conecta realmente.
- Las conexiones remotas se pueden realizar desde lugares no confiables, lo que puede poner en riesgo la seguridad de las compañías.
- A veces implementar o forzar sistemas MFA en proveedores es difícil por obligar a tener un móvil corporativo o sistemas basados en hardware.

Solución

- Ironchip permite el uso de alias para diferenciar los usuarios reales que se conectan a través de emails genéricos.
- Ironchip controla los lugares de conexión, permitiendo exclusivamente conexiones desde lugares confiables gracias a la tecnología de localización inteligente propia basada en ondas y no en IP por medio del ITDR incorporado.
- Ironchip permite el uso de USB de menos de 1 € sincronizados con aplicaciones de escritorio o incluso con email con magic link, que al pulsar actúan de MFA.

Ayuntamiento de Alcobendas

La implementación de estas tecnologías, desde **RDP** y **Azure** hasta **Global Protect VPN** y los **servidores Linux**, ha traído consigo una serie de beneficios tangibles para el Ayuntamiento de Alcobendas. La **seguridad** se ha reforzado considerablemente, protegiendo nuestra infraestructura y datos críticos. A su vez, la **accesibilidad** y la **flexibilidad** para nuestros usuarios han mejorado drásticamente, permitiendo un trabajo eficiente tanto dentro como fuera de la oficina. Finalmente, la capacidad de **customizar todas las interfaces** con nuestra identidad corporativa no solo fortalece la marca del ayuntamiento, sino que también fomenta una mayor confianza y familiaridad entre nuestros empleados y colaboradores, combinando la protección con una experiencia de usuario única y cohesionada.

*"En el Ayuntamiento de Alcobendas, la combinación de **RDP, Azure (con Office), Globalprotect VPN y nuestros servidores Linux** es clave. Lo que más nos gusta es cómo, además de la **seguridad**, todas las interfaces están **customizadas con los logos del ayuntamiento**. Es la fusión perfecta entre **identidad y protección**."*

Jose Luis Miguel, Director IT

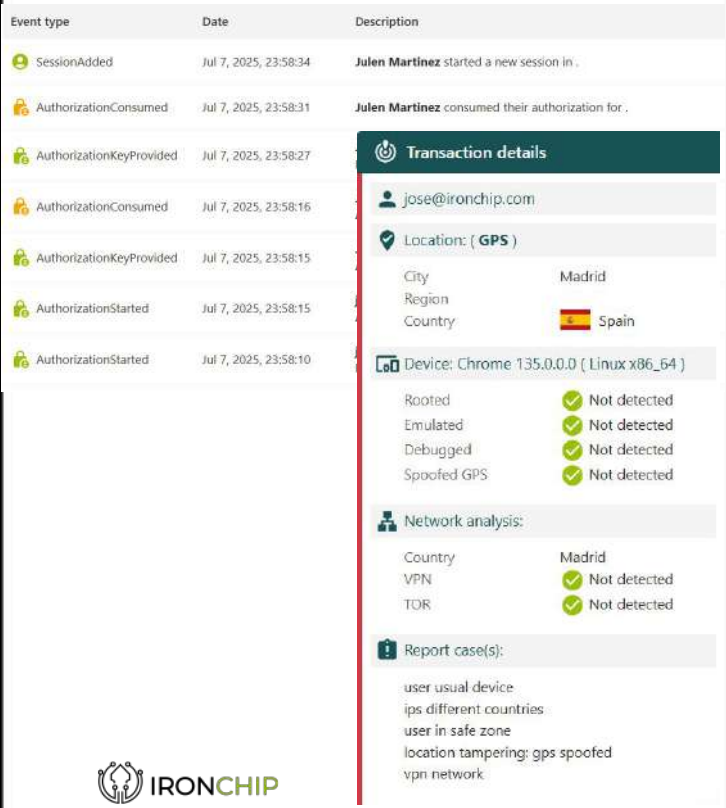
IRONCHIP

Especificaciones para el sector salud Caso de uso

Fortaleciendo la Ciberseguridad con Cumplimiento ENS e Identity Threat Detection and Response (ITDR)

Salud: Visibilidad de los activos confidenciales

Caso de Uso 4



IRONCHIP

Protección de activos digitales

La protección de historiales clínicos o activos digitales es muy relevante en el ámbito sanitario. En muchos casos el uso de correos genéricos puede no hacer identificable el acceso real. Ironchip monitoriza todos los accesos y vigila todos los accesos en busca de anomalías.

Problema

+ Las consecuencias devastadoras de un acceso no autorizado a información sanitaria (historias clínicas, datos personales) o a sistemas críticos del hospital, que pueden resultar en pérdida de confianza y multas.
+ Los ataques de ingeniería social son cada vez más sofisticados y difíciles de detectar por métodos tradicionales de seguridad, engañando incluso a usuarios precavidos.
+ La posibilidad de suplantación de identidad o el uso de credenciales robadas puede pasar desapercibida hasta que el daño ya está hecho, generando un impacto significativo.

Solución

+ Utiliza algoritmos avanzados de aprendizaje automático y conductual para crear perfiles de comportamiento únicos y dinámicos para cada usuario, detectando desviaciones y diferenciando ususario reales incluso con mails genericos.
+ **Detecta en tiempo real comportamientos inusuales** (acceso a historiales no relacionados con la especialidad del médico, accesos fuera de horario laboral, volumen inusual de descargas) que sugieren un robo de cuenta.
+ Proporciona un registro detallado e inalterable de cada interacción (usuario, hora, método, ubicación, recurso, acción), **ofreciendo una trazabilidad completa y unificada**.

Salud

"En IMQ, la implementación de las tarjetas corporativas como método de autenticación ha sido un cambio revolucionario. Lo que más valoramos es la facilidad de uso que ofrece a todo nuestro personal. Se ha eliminado la complejidad de recordar múltiples contraseñas, agilizando enormemente los procesos diarios. La experiencia es tan intuitiva que ha sido adoptada de forma natural, mejorando la eficiencia operativa y la seguridad de acceso a nuestros sistemas."

Víctor Atienza, CISO Clínica San Miguel

"Lo que más valoramos es la ***trazabilidad completa y sencilla de todas las descargas de informes confidenciales****. Esto nos permite asegurar la confidencialidad de la información de nuestros pacientes con una facilidad que no habíamos experimentado antes.* ***Ironchip ha simplificado drásticamente nuestra capacidad de auditoría y cumplimiento.*** *"*

José Manuel Mollá, Director IT

Conclusión: Resiliencia e identidad digital fácil y fortalecida

Con Ironchip, las administraciones públicas y hospitales no solo alcanzan y superan las exigencias normativas del Esquema Nacional de Seguridad (ENS), sino que transforman su postura de ciberseguridad de manera proactiva. La solución totalmente passwordless elimina los riesgos inherentes a las contraseñas, como el phishing o la ingeniería social, ofreciendo una flexibilidad inigualable en los métodos de autenticación, adaptándose a cualquier entorno sin depender de aplicaciones móviles corporativas.

Gracias a su avanzada capacidad de Identity Threat Detection and Response (ITDR), Ironchip no solo detecta, sino que bloquea en tiempo real el robo de cuentas y los accesos no deseados, incluso frente a la falsificación de biometría. Esto se traduce en un fortalecimiento integral de la Confidencialidad, Integridad, Trazabilidad, Autenticidad y Disponibilidad (CITAD) de la información, garantizando una mayor resiliencia digital y consolidando la confianza ciudadana en los servicios públicos esenciales.

Your next generation identity

Paseo de la Castellana , 200 Madrid
Beurko Berria, 17. Barakaldo
info@ironchip.com