IRONCHIP

Fight Against Identity Threats

Ironchip's Identity & Access Management and Fraud Detection solutions powered by location intelligence technology

www.ironchip.com

1. **Ironchip**
    - ¿Quiénes somos?
    - Partners y Colaboradores
    - Nuestros clientes
2. **Nuestra tecnología y productos**
    - Localización segura de Ironchip
    - La localización aplicada a la identidad
    - Nuestros productos de ciberseguridad
3. **Identity Platform**
    - Ventajas
    - Solución personalizable
    - Modos de autenticación configurables
    - Métodos recomendados por roles
    - Protección de identidad y accesos
    - ¿Cómo funciona? Location Intelligence
    - Add-Ons: Windows logon, Linux logon, Mac logon, Desktop application
    - Intrusion Detection System
    - Casos de éxito
4. **Fraud Detection**
    - Detección de fraude por localización
    - Propuesta de valor
    - Casos de éxito

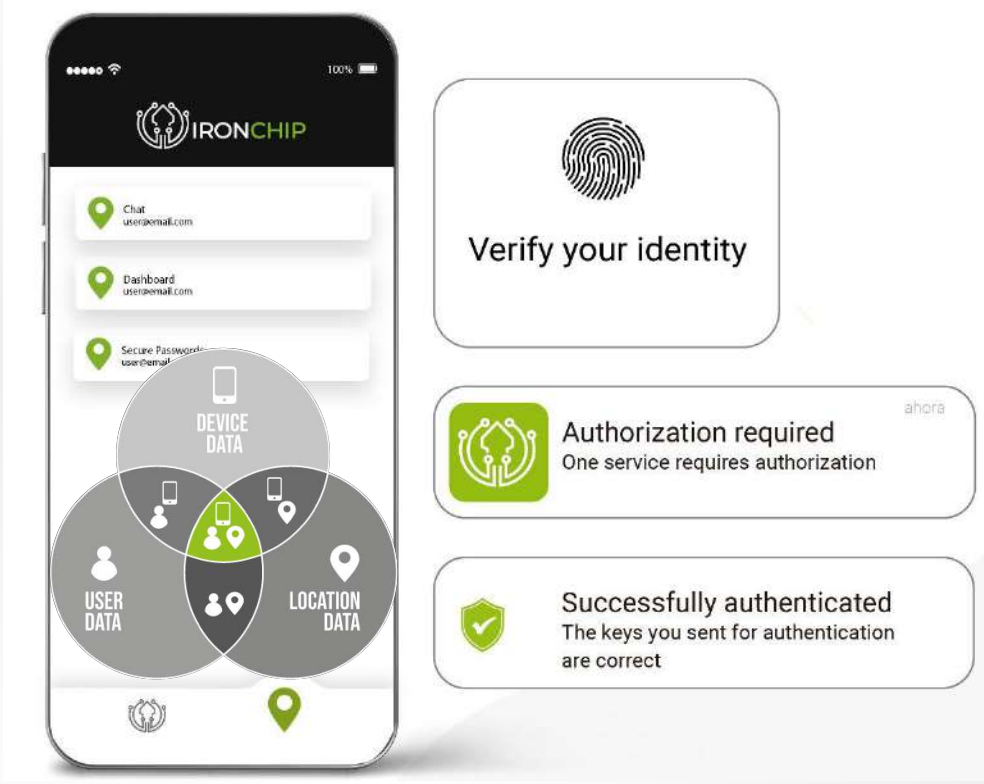
IRONCHIP

¿Quiénes somos?

Ironchip es una compañía de ciberseguridad global, especializada en protección de identidad digital y detección de fraude de nueva generación.

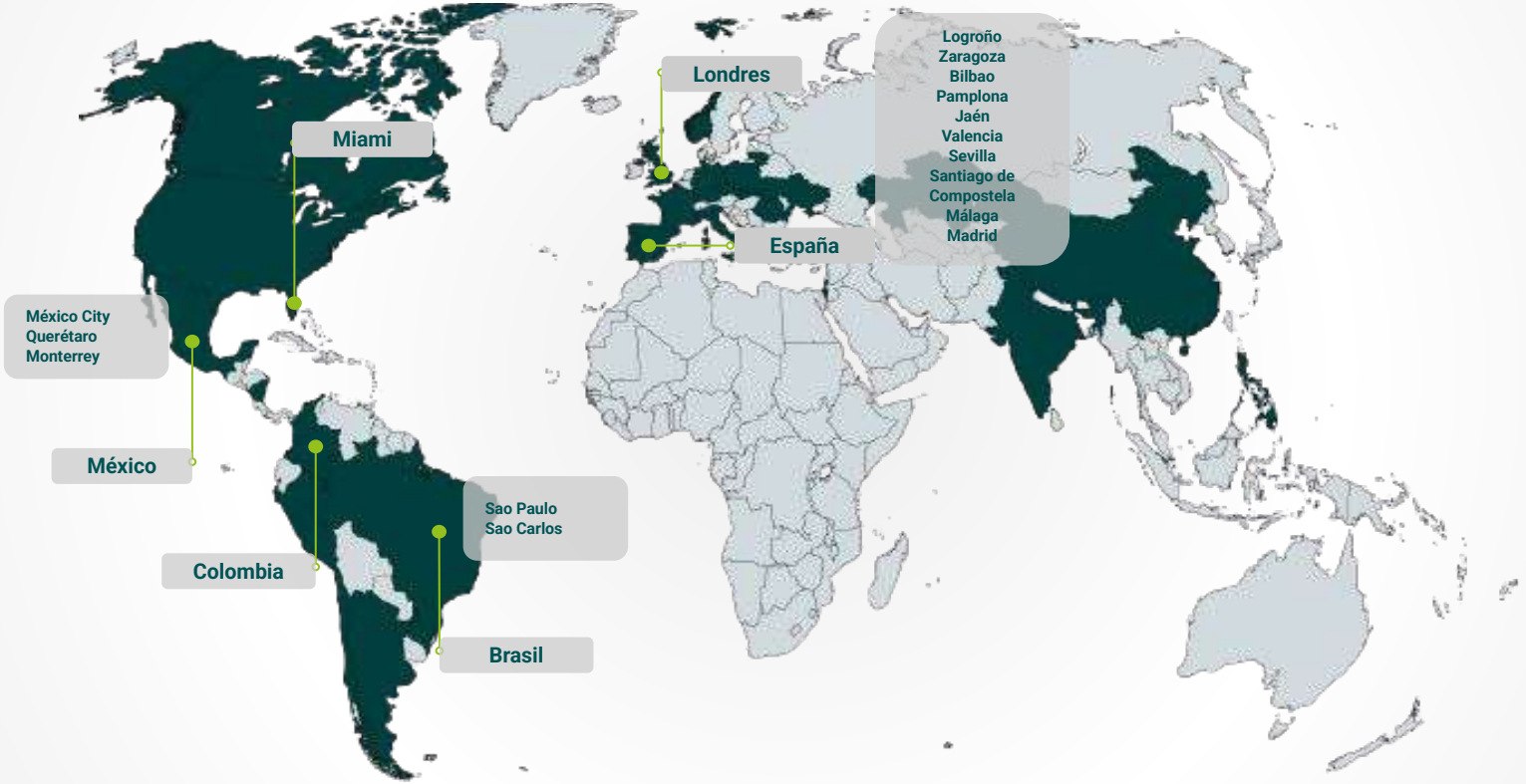
Con una **tecnología única en el mundo,** las soluciones de Ironchip ofrecen al cliente una **protección integral de la identidad** de todos sus servicios y recursos, así como también los de sus colaboradores.

Nuestra **tecnología de localización inteligente,** ofrece una trazabilidad, visibilidad y control en tiempo real de todos los usuarios, accesos y recursos, garantizando a las compañías una **seguridad 360.**



IRONCHIP

Escala Global



IRONCHIP

Ciberseguridad en nuestro ADN

En Ironchip, la **seguridad** no es solo una palabra, es nuestro **compromiso**. Por eso, nos sentimos orgullosos de contar con el aval de los más exigentes organismos de **certificación**.

Nuestras soluciones han sido certificadas con el nivel ALTO, la máxima calificación posible, por las entidades más prestigiosas del sector.

El gobierno de España avala la compañía mediante su inversión, convirtiendonos en empresa clave estratégica a nivel nacional.

IRONCHIP

Sectores en los que operamos

Industria	Banca	Servicios	Pharma Salud	Gobierno
Protección de Identidad y Accesos	Protección de Identidad y Anti Fraude	Protección de Identidad y Detección de intrusos	Protección de Accesos servicios críticos	Accesos servicios y equipos críticos
Accesos centralizados	*Transacciones seguras y protección de accesos*	*Monitorización proveedores*	*Protección Información sensible*	*Equipos y departamentos críticos*

Nuestros clientes

+100 Clientes

En Ironchip, nuestros clientes son nuestra prioridad absoluta, y nuestra dedicación a la excelencia en cada interacción es la piedra angular de nuestra garantía de servicio.

Tecnología y productos

www.ironchip.com

01 Tecnología de Detección basado en localización

Transacciones seguras por comportamiento

Zonas de operaciones habituales

La **mayoría** de los procesos de identidad tienen lugar en **ubicaciones confiables**.

Ubicación No Confiable

El **98%** de los ataques ocurren de forma remota, desde una ubicación en la que el usuario nunca ha estado.

El **99%** de los estafadores cometen fraude desde la misma ubicación en dos ocasiones.

Usuarios y operaciones en una única solución

Tipos de transacciones protegidas

92% 

Registro de usuario

El 92% de los usuarios se registran en una aplicación desde lugares habituales

74% 

E-commerce

El 74% de las compras se realizan desde lugares habituales

68% 

Inicio de sesión

El 68% de los inicios de sesión se realizan desde lugares habituales

94% 

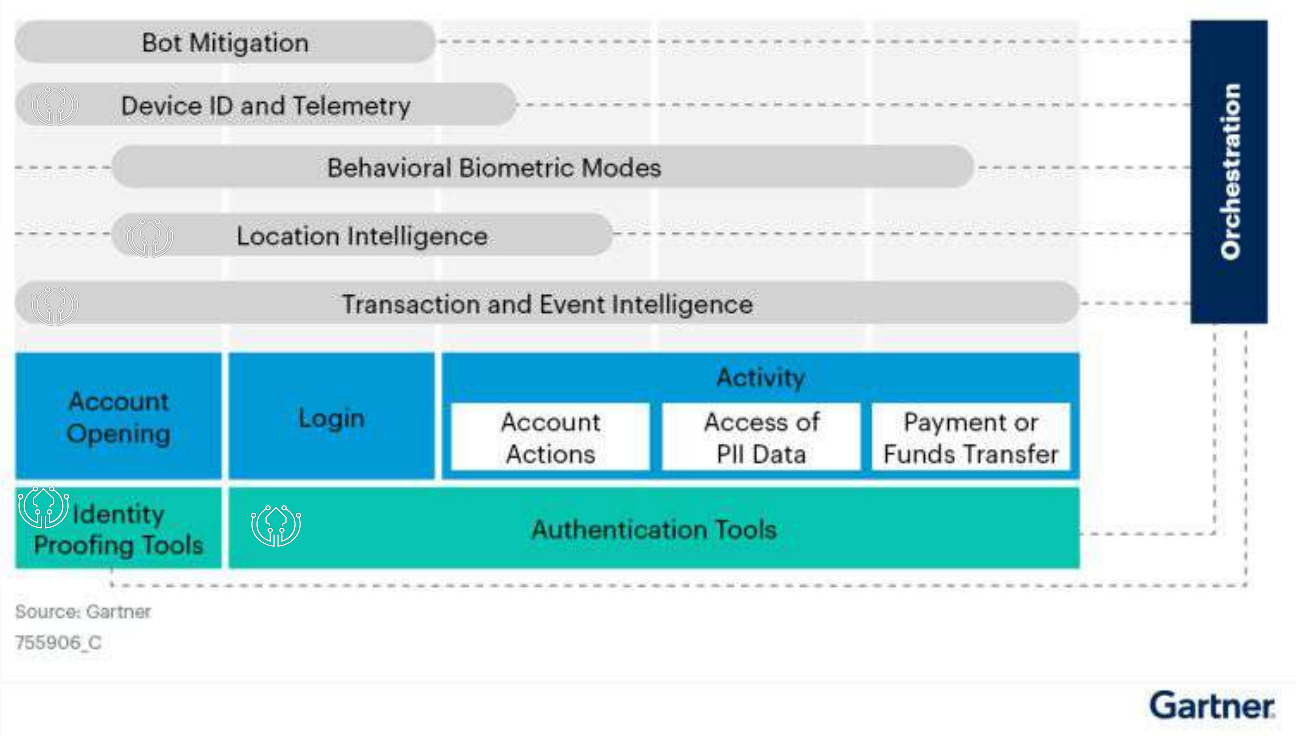
Transacciones +10.000€

Más del 95% de las transacciones de altos importes desde lugares habituales

Location intelligence

Location identity proof

Alcance de las capacidades de Online Fraud Detection a lo largo de un recorrido digital típico del cliente.



¿Cómo funciona?

Transacciones seguras y localizadas

¿Que es una Zona Segura?

Una zona segura es un **lugar único, anónimo e infalsificable**

¿Cómo se genera una zona segura?

Una zona segura se genera captando y analizando las ondas **2G, 3G, 4G, 5G, WIFIs y GPS** cada vez que un usuario opera una aplicación móvil o web.

Cada interacción enseña **a la IA propia de Ironchip** la relación entre los lugares en el tiempo, y esto permite utilizar esos relaciones lugar-dispositivo como parte de la identidad de cada usuario.

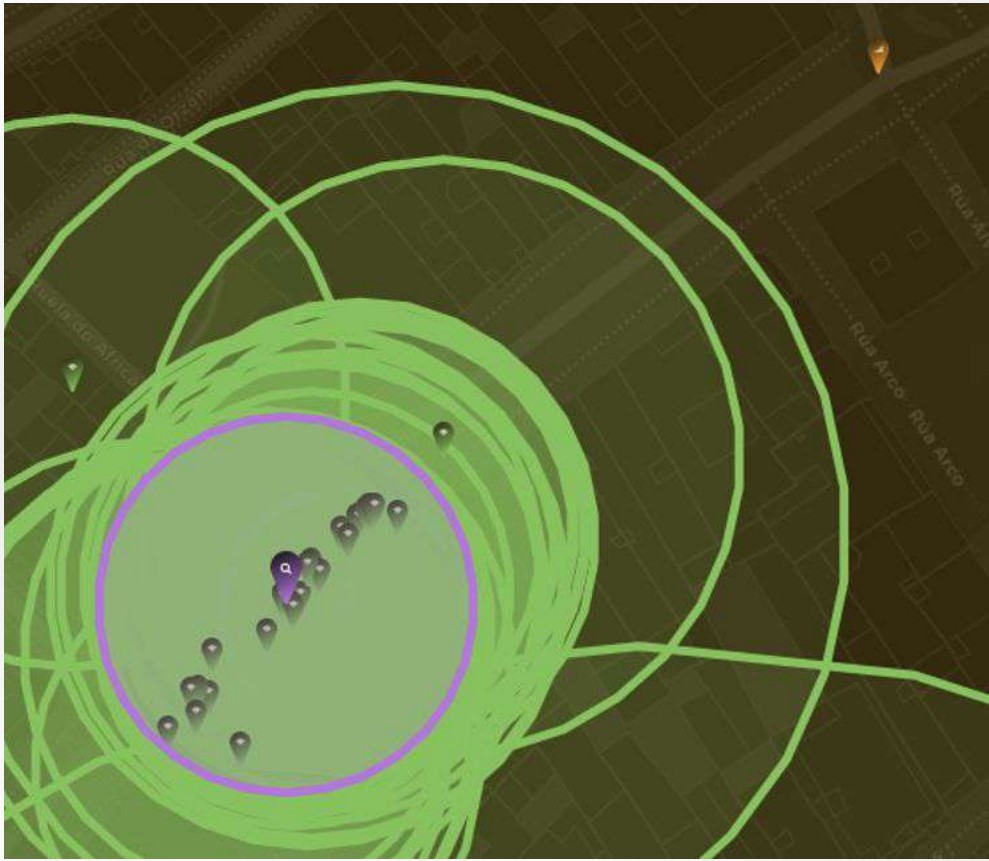


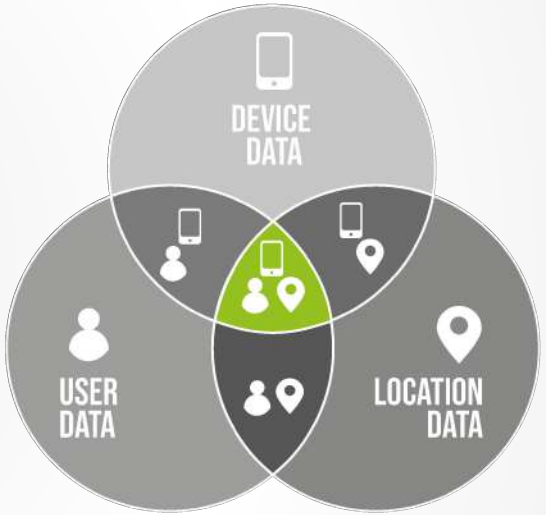
Image 1. Generated safe zone example with GPS, EM (2G, 3G, 4G, 5G) & IP signals.

Comportamiento de usuario

Localización en el comportamiento

La vinculación entre el lugar y el dispositivo que integramos en nuestra tecnología, junto con la inteligencia artificial de localización basada en señales de redes móviles y WIFIS, junto con los datos del usuario, es fundamental para la **generación de patrones de comportamiento**.

Esta combinación permite entender el comportamiento del usuario y su ubicación de manera precisa, lo que resulta indispensable para una identidad segura en el futuro. La capacidad de **comprender dónde se encuentra el usuario y cómo interactúa con sus dispositivos** es inigualable, y representa la clave para garantizar la seguridad y la autenticación en los sistemas digitales.

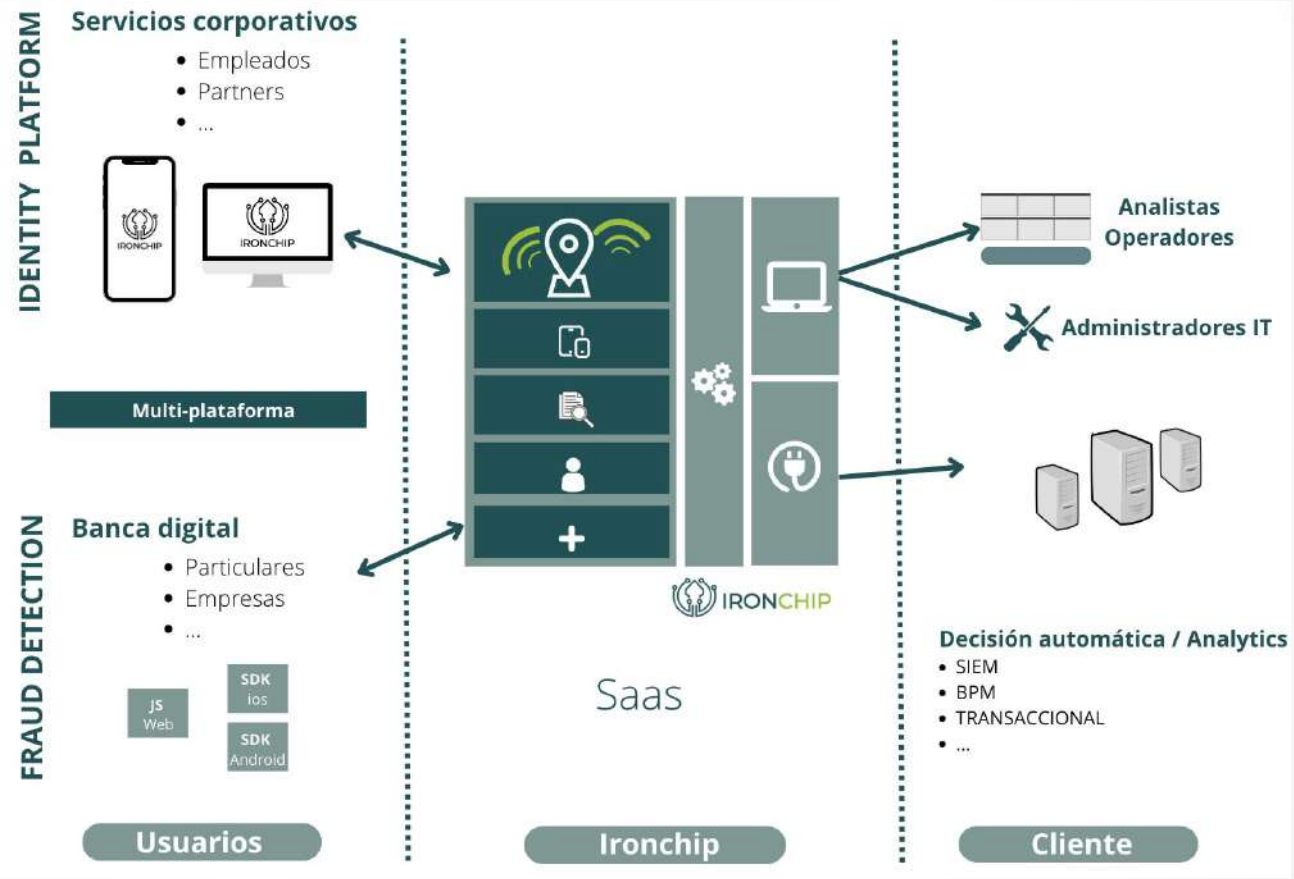


IRONCHIP

Tecnología de localización aplicada a la identidad digital

IRONCHIP

Nuestros productos de seguridad



Identity Platform

www.ironchip.com

Identity Platform

Modelo de madurez y seguridad de las soluciones de autenticación

El **Customer Authentication Strong and Maturity Model (CASMM) v2** es la versión actualizada del marco de referencia global que ayuda a las organizaciones a **evaluar la madurez de sus prácticas de autenticación**. Esta nueva versión se basa en la experiencia adquirida con la versión anterior e incorpora las últimas tendencias y mejores prácticas en materia de autenticación.

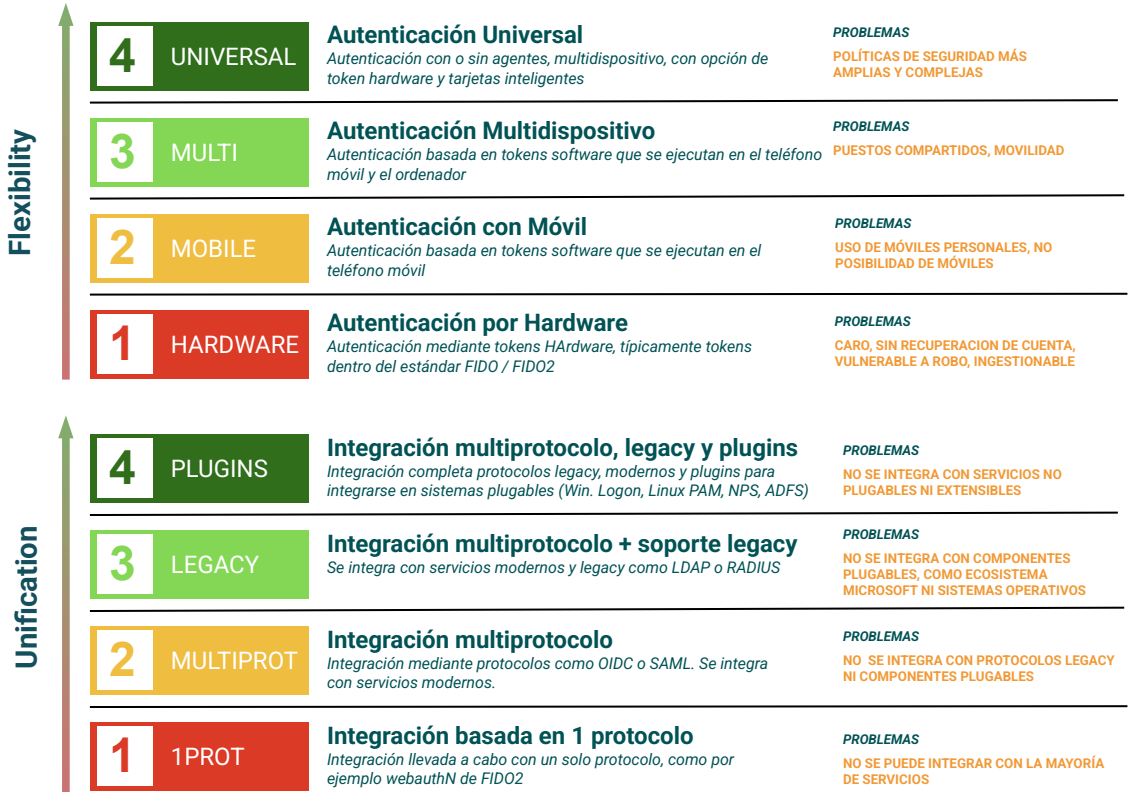
Ironchip Identity Platform consigue que las compañias se situen en el nivel 8 de este estandar, **evitando ataques de phising, malware, sim swapping, toma de cuenta y obtención de credenciales**.

Además, nuestra plataforma de identidad mejora el dia a dia de los usuarios y los administradores, **reduciendo hasta en un 60% las incidencias relacionadas con la identidad**

Identity Platform

Modelo de flexibilidad y unificación de las soluciones de autenticación

El **Customer Authentication Flexibility and Unification Model (CAFUM) v1** es la versión adaptada del marco de referencia global CASMM, con el que Ironchip ayuda a las organizaciones a **evaluar la escalabilidad de sus prácticas de autenticación**. Esta nueva versión se basa en la experiencia adquirida en los proyectos ejecutados con Ironchip



Identity Platform

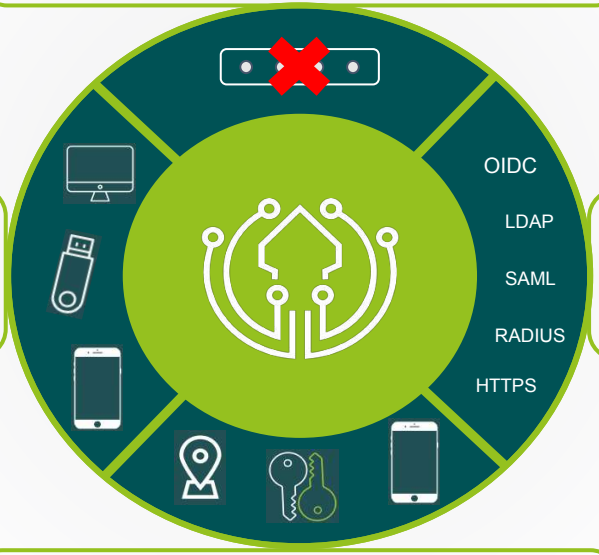
Una experiencia unificada ligada a la excelencia

La experiencia más sencilla

Colocamos la experiencia del usuario en el núcleo de nuestro diseño, siendo capaces de sustituir el uso de contraseñas por factores más seguros y faciles de utilizar y administrar.

Flexibilidad sin limites

¿Tus empleados no tienen móvil corporativo? Ironchip funciona en android, iOS, Windows, Linux y Mac. Además, puedes reforzar tu seguridad con hardware tokens o dispositivos USB. O incluso autenticarte sin agentes



Identidad unificada

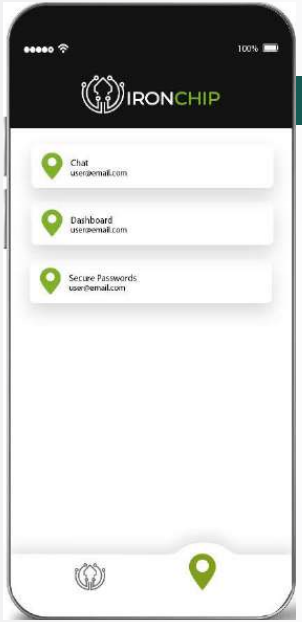
Nuestra plataforma se integra sin problemas con todas tus herramientas corporativas, centralizando la gestión de la identidad y asegurando la privacidad de tus datos.

Seguridad basada en riesgo

No almacenamos credenciales en nuestros servidores para garantizar la seguridad. Cero robos de cuenta gracias a detector de intrusos basado en dispositivo y ubicación

Identity Platform

La experiencia Passwordless más sencilla



Passwordless Authentication

Device Intelligence + Biometry + Hardware Keys

User experience

- **Effortless** 3 identity proofs 1 interaction
- **Secure:** Phising, Malware & Sim Swapping resistant
- **Passwordless** Without passwords, OTPs...

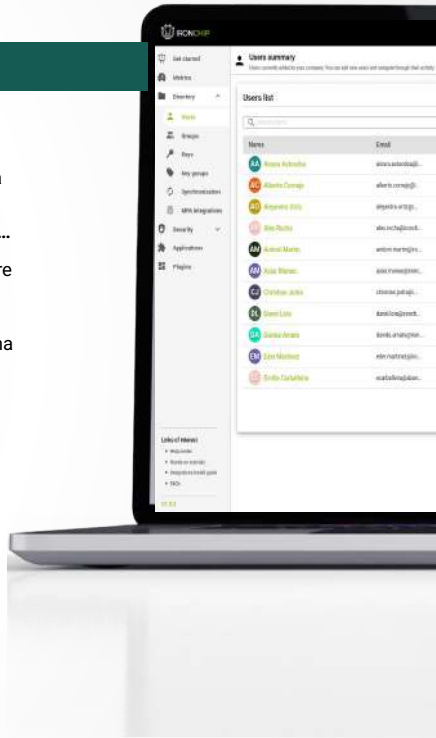
Easiest Management

Ciclo de vida de identidad

- **Altas, bajas, modificaciones e integraciones a golpe de click.**
- **Sin passwords, sin renovaciones, sin códigos…**
- **Sin puntos muertos.** Visibilidad completa sobre TODA tu identidad
- **Solucion multi-tenant:** Gestiona diferentes unidades organizativas y territoriales desde una única herramienta

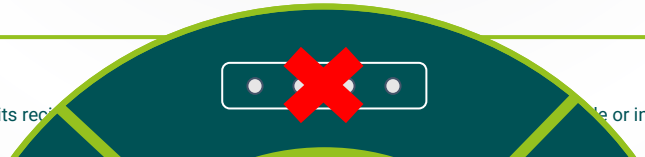
Datos, datos y más datos

- **Trazabilidad completa:** Todo lo que ocurra dentro de la herramienta queda registrado



La experiencia más sencilla

Colocamos la experiencia del usuario en el núcleo de nuestro diseño, siendo capaces de sustituir el uso de contraseñas por factores más seguros y faciles de utilizar y administrar.



Seguridad basada en riesgo

No almacenamos credenciales en nuestros servidores para garantizar la seguridad. Cero robos de cuenta gracias a detector de intrusos basado en dispositivo y ubicación

Zero Knowledge Proofs

Identidad soberana corporativa

- **Seguridad:** No almacenamos credenciales en nuestros servidores para garantizar la seguridad.
- **No más sustos innecesarios:** Sin posibilidad de ataques al proveedor de identidad.

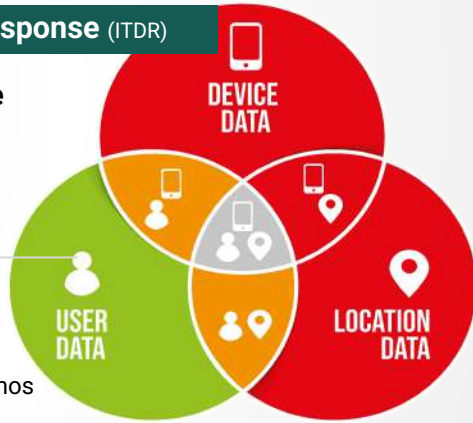
Cero robos de cuenta

- **Anti MITM:** Conexiones seguras imposibles de descifrar por un tercero
- **Anti Phising:** La clave de acceso nunca abandona el dispositivo, impidiendo los ataques de Phising

Identity Threat Detection & Response (ITDR)

Análisis de riesgo transparente

- **Detección de scams:** Detectamos ataques de ingeniería social como el vishing o la suplantación de identidad
- **Alertas en tiempo real:** Detecta y/o bloquea los ataques en tiempo real

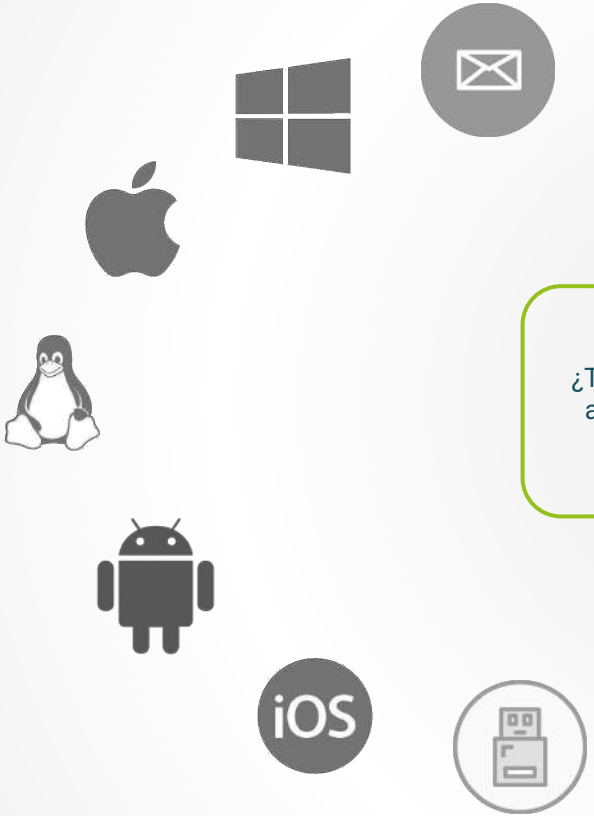


Métodos de detección únicos

- **Inteligencia de localización:** Detectamos falsificaciones de ubicación, viajes imposibles, VPNs, Tor ...
- **Tampering de dispositivo:** Sabemos si el dispositivo ha sido alterado, mediante root, emulación o depuración.

Identity Platform

Flexibilidad sin limites



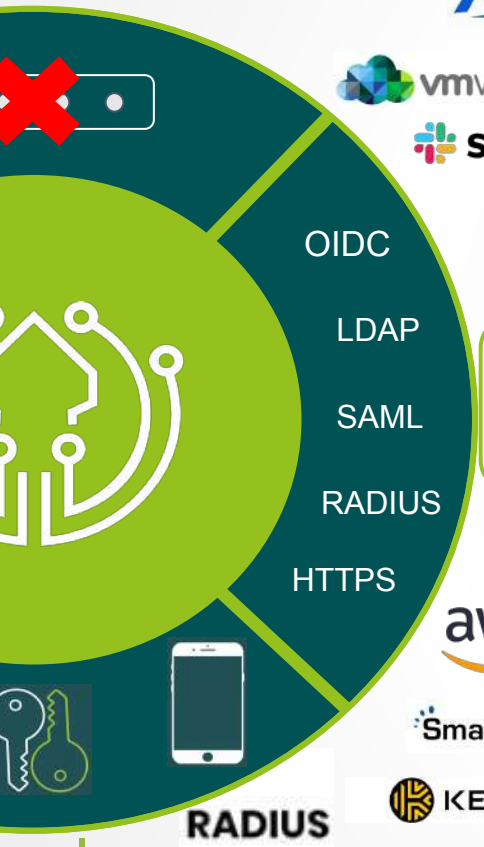
Flexibilidad sin límites

¿Tus empleados no tienen móvil corporativo? Ironchip funciona en android, iOS, Windows, Linux y Mac. Además, puedes reforzar tu seguridad con hardware tokens o dispositivos USB. O incluso autenticarte sin agentes mediante correo electrónico.

Identity Platform

Unificación total

IRONCHIP



Identidad unificada

Nuestra plataforma se integra sin problemas con todas tus herramientas corporativas, centralizando la gestión de la identidad y asegurando la privacidad de tus datos.

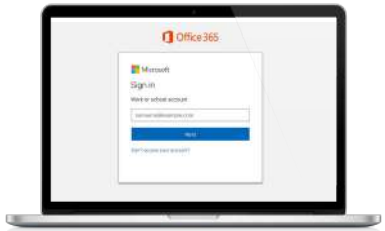
CYBERARK
Microsoft Azure
OpenID Connect
Exchange
paloalto NETWORKS
vmware
slack
LDAP
VT Scada
salesforce
Signifyd
WordPress
WatchGuard
Jira Software
SONICWALL
zoom
Office 365
f5
SOPHOS
ForgeRock
Airtable
CISCO
FORTINET
Google Workspace
GitLab
odoo
IBM
workday
SAML
HubSpot
HashiCorp Terraform
CHECK POINT
aws
opennac enterprise
SailPoint
Dropbox
HashiCorp Boundary
HashiCorp Vault
Pulse Secure Acquired by Ivanti
SAP
SmarterServices
Microsoft Windows Logon
zscaler
KEEPER
ADFS
GitHub
citrix

Identity Platform

Solution for employees with mobile phones

IRONCHIP

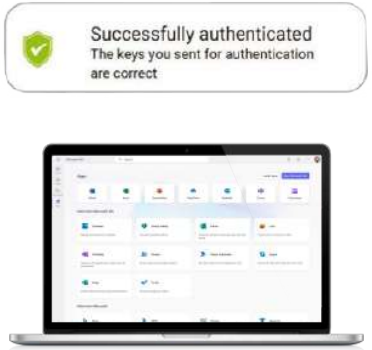
User tries to access the corporate resource Office365



Receive a push notification on your mobile device

Opens the notification and approves access via the mobile application

Once authenticated, the user can access the requested resources.

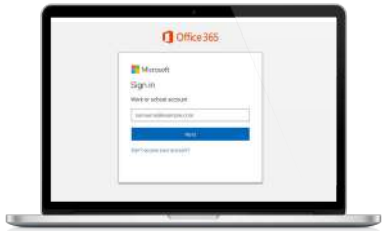


Identity Platform

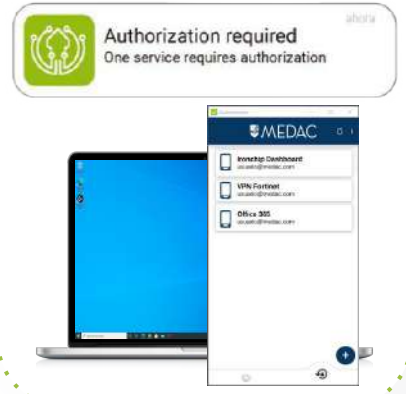
Solution for employees with corporate/proprietary computers

IRONCHIP

User tries to access the corporate resource Office365

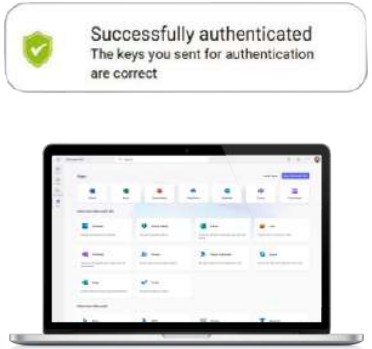


Receive a push notification in your desktop application



Open the notification and approve access via the desktop application.

Once authenticated, the user can access the requested resources.



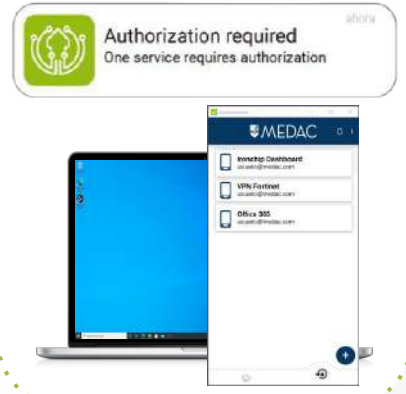
Identity Platform

Solution for employees with rotating workstations and multi-user workstations

IRONCHIP

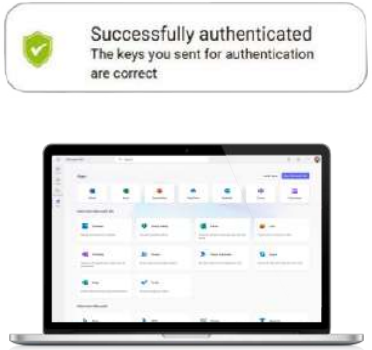
The user connects his USB and tries to access the corporate resource Office365

Receive a push notification in your desktop application



Open the notification and approve access via the desktop application.

Once authenticated, the user can access the requested resources.

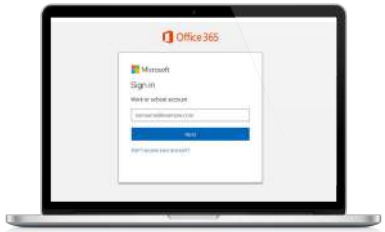


Identity Platform

Solution for employees with rotating workstations and multi-user workstations

IRONCHIP

The user connects his NFC CARD or TOKEN and tries to access the Office365 corporate resource.



Receive a push notification in your desktop application

Open the notification and approve access via the desktop application.

Once authenticated, the user can access the requested resources.

Identity Platform

Solution for supplier access

IRONCHIP

The user attempts to access the corporate resource

Receive an email with a Magic Link

Click on this link to authorize access.

Once authenticated, the user can access the requested resources.

License model

IRONCHIP

FREE

Enable passwordless authentication to seamlessly integrate and configure access to your services, endpoints and applications.

Authentication:

- Agentless Authenticator
- Computer Authenticator
- Mobile Authenticator

Identity & Access Management:

- Users, groups & devices management
- 1-10 users

Plugins:

- NPS Plugin
- Microsoft ADFS Plugin

Security:

- Access logs

Metrics & Others:

- Basic metrics

ENTERPRISE

Passwordless authentication enhances security with advanced configuration and monitoring features. Includes standard capabilities, plus:

Authentication:

- USB Token Authenticator
- Smartcard Authenticator

Identity & Access Management:

- Automatic provision from other directories i.e. Acitve Directory
- Configure conditional access policies

Plugins:

- LDAP Server
- Windows, Linux & MAC Logon

Security:

- Permissions Management
- Configurable IP whitelist
- Activity logs

Metrics & others:

- Realtime timeline
- Corporative Look&Feel

PREMIUM

The Ironchip's identity full experience to zero account takeover

Authentication:

- Location-based autentication
- Context-based autentication

Identity & Access Management:

- Secure location Management
- Generate corporate perimeter of trust

Intrusion Threat Detection 6 Response:

- Detect identity threats
- Define customized risk rules based on the context
- Block attacks automatically
- Get realtime reports via API

Metrics & others:

- Advanced metrics
- Syslog / API for SIEM integration

Identity Platform

Casos de éxito

www.ironchip.com

Identity Platform

Caso de éxito - Ulma Construcción

Reto

La exigencia de ofrecer servicios accesibles de manera remota y segura a nivel global planteaba desafíos críticos de seguridad para Ulma Construcción, dado que dichos servicios son vulnerables a ataques externos a través de conexiones remotas como las VPN y RDP.

Propuesta

Ironchip propuso la personalización de la autenticación para distintos perfiles dentro de la empresa. De este modo, implementan diversos métodos de autenticación multifactor (MFA) como notificaciones push, emails, contraseñas, códigos OTP, entre otros, adaptando así las soluciones para las conexiones remotas.

Solución

Ulma Construcción reforzó la seguridad de sus conexiones remotas corporativas al introducir un segundo factor de autenticación ajustado a los diversos perfiles de usuario. Esta solución, que ofrece opciones personalizadas para distintos roles, no solo incrementó la productividad, sino que también aseguró el cumplimiento de regulaciones de seguridad. Con más de 1.500 empleados y colaboradores externos, todos requeridos a utilizar un segundo factor de autenticación para acceder a los sistemas de Ulma, se garantiza un nivel de seguridad óptimo.

Identity Platform

Caso de éxito - Conservas Ortiz

Reto

Garantizar la seguridad de los datos del cliente en los dispositivos corporativos mediante una autenticación multifactor que no requiere el uso de un móvil corporativo, asegurando el acceso incluso en puestos calientes donde un dispositivo es utilizado por varios usuarios.

Propuesta

Conservas Ortiz barajo Ironchip para soluciones de ciberseguridad adaptadas, implementando Ironchip Identity Platform con acceso seguro a través de un **token físico**. Este método cumplia las directrices de la empresa para la implementación de doble factor en el inicio de sesión de windows.

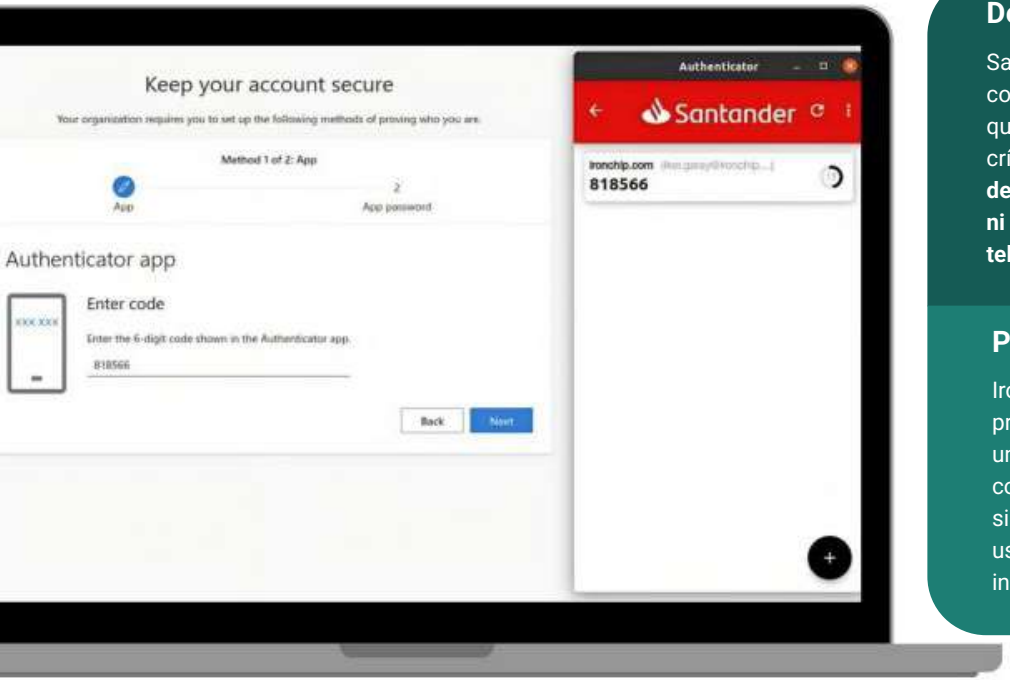
Solución

Conservas Ortiz seleccionó a Ironchip para sus necesidades de ciberseguridad personalizadas, implementando Identity Platform mediante un token físico. Esta solución no solo protege el acceso a los recursos, sino que también proporciona visibilidad y control a los administradores de IT, mejorando así la eficiencia y la seguridad global de la empresa. Además, cumple con las políticas de seguridad asociadas con la norma ISO 27001.

DESDE 1891 CONSERVAS ORTIZ

Identity Platform

Caso de éxito - Santander Global



Desafío

Santander Global buscaba cumplir con la nueva regulación del ENS que exige un MFA para servicios críticos como Azure, pero **sin depender de dispositivos móviles ni conexión con números de teléfono personales**.

Propuesta

Ironchip trabajo en una propuesta de valor basada en una aplicación de escritorio con OTP integrable y sincronizable con todos los usuarios de su AD en su infraestructura.

Solución

Santander ha implementado una solución eficiente usando la aplicación de escritorio configurada en modo "Contraseña + OTP", mejorando la productividad y cumpliendo con normativas para empleados. Además, cubre las siguientes necesidades:

- Cumplimiento del ENS.
- No utilización de móviles corporativos ni nº de teléfono personales.
- Identificación de usuarios en los puestos calientes, donde múltiples usuarios se conectan al mismo dispositivo.

IRONCHIP

Fraud Detection Platform

www.ironchip.com

Anomalous behaviour

Los nuevos (y viejos) fraudes

SIM SWAPPING
6.500.000 M$

VISHING
Crecimiento 625%

SYNTHETIC ID
20% Fraude financiero EEUU

PHISHING
486.000.000 M$

Anomalous behaviour

Detected fraud behaviours

IRONCHIP

Detectamos los fraudes más avanzados

SIM SWAPPING

VISHING

PHISHING

SYNTHETIC IDENTITIES

MONEY MULE

Con un conjunto de métodos únicos

DEVICE FINGERPRINT

LOCATION INTELLIGENCE

DEVICE SWAPPING

TAMPERED DEVICE

TAMPERED APPLICATION

¿Cómo funciona?

SDK & API

Datasource SDK

Una librería iOS/Android/Javascript que puede integrarse en cualquier móvil/aplicación web para capturar la información necesaria.

Fraud detection API

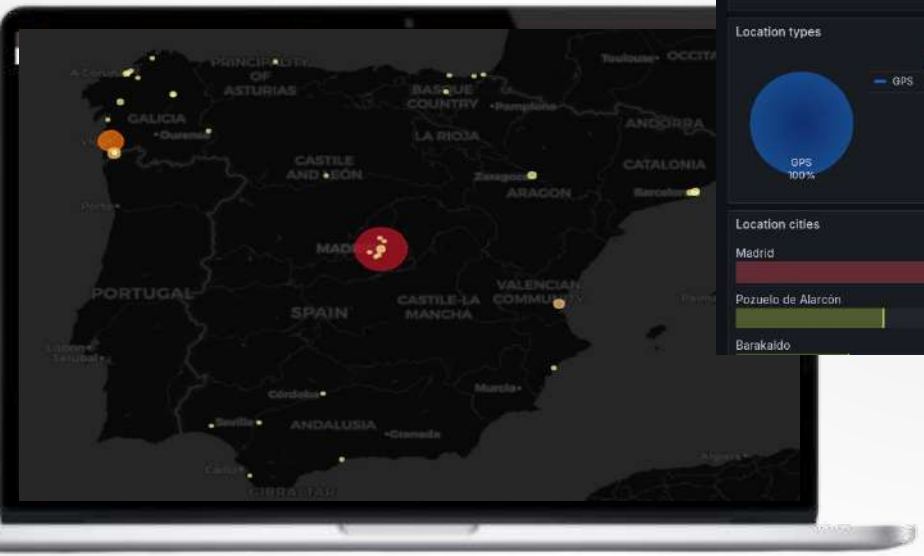
Una HTTP API para solicitar resultado integrables con cualquier BPM o SIEM.

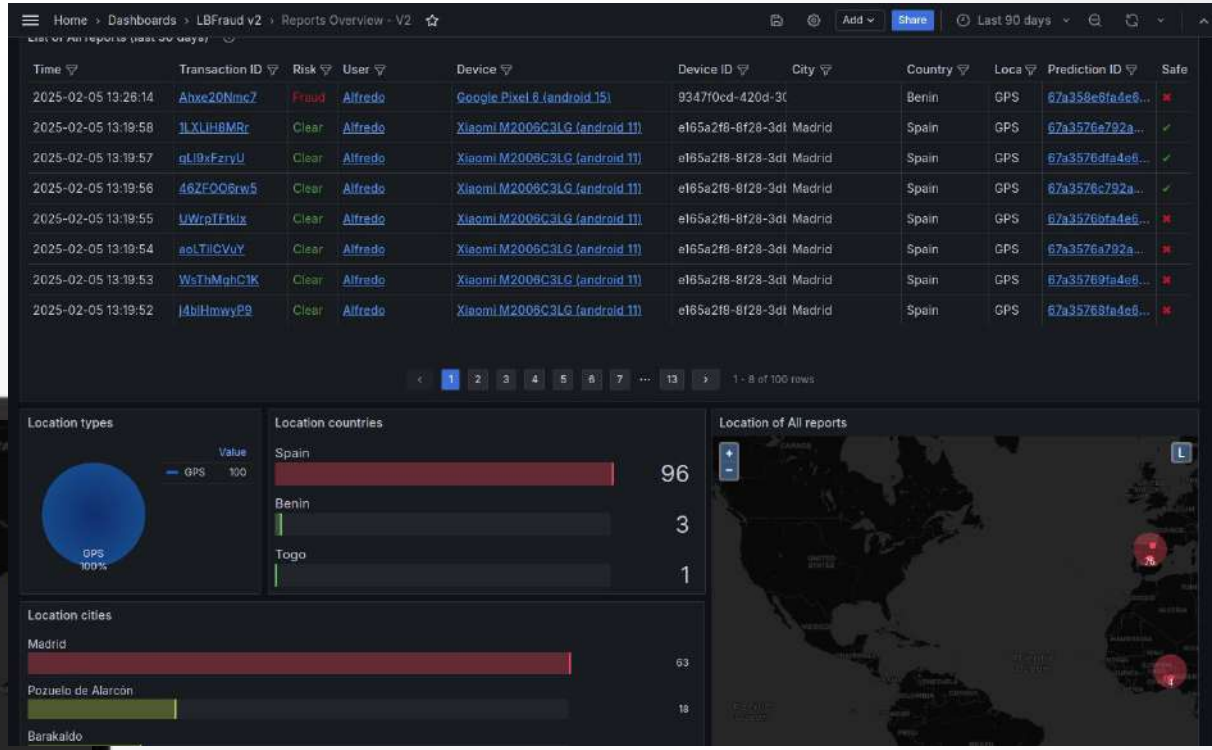
```
//  Login Operation

IronchipLBFraudSDK.executeTransaction("random_identifier_generated",
                                      "user_1234","login",null)


// Transfer Operation HashMap

HashMap <String, String> transferInformation = new HashMap<String, String>();
                                    transferInformation.put("Param_1", "XXX");
                                    transferInformation.put("Param_2", "YYY");
                                    IronchipLBFraudSDK.executeTransaction("random_identifier_generated",
                                    "user_1234","transfer",transferInformation)
```

03 ¿Cómo funciona?

Dashboard

- Mapa de calor con puntos negros del origen de los ataques.
- Reportes históricos de los ataques por usuario descargables.

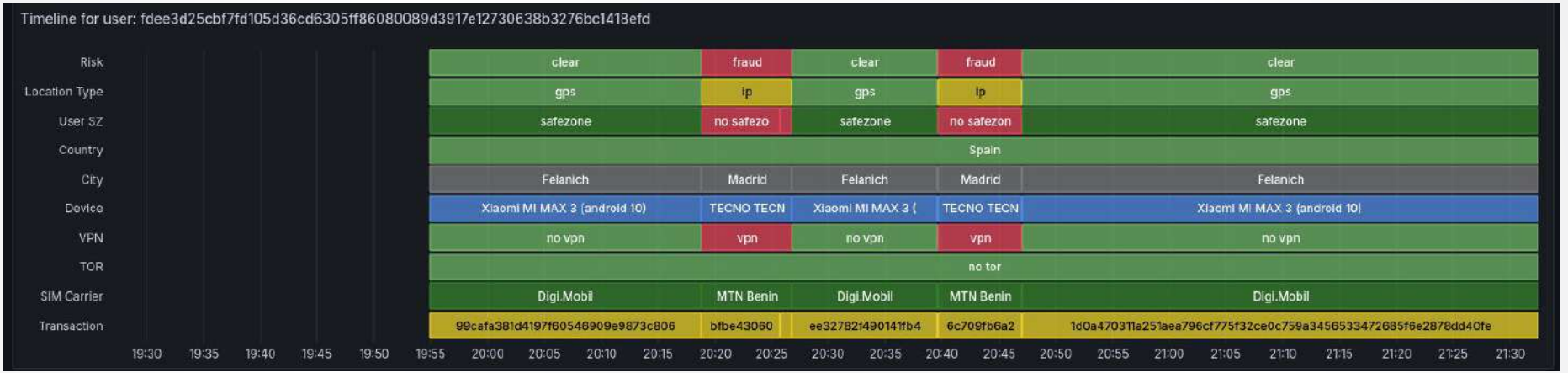




- Análisis forense de los casos a petición.
- Motor de reglas configurable.
- Alerta en tiempo real. (SLA < 1 seg)

04 Anomalous behaviour

¿Y si el hacker no nos da el GPS?: Pillando a un Money Mule



Uso Repentino de VPN:

El 12 de septiembre se observó por primera vez una conexión a través de una VPN, específicamente NordVPN. Esto supone una desviación significativa del comportamiento habitual del usuario.

Cambio de SIM Carrier:

El dispositivo pasó de estar conectado en España a otra ubicación, también reportada como España, pero con una tarjeta SIM de origen en Benín. Esto fue posible mediante un cambio de proveedor de servicios móviles, de DiGI (España) a MTN Benin.

Viaje imposible:

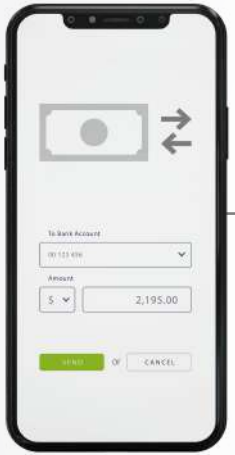
En 5 minutos viajo de España a Benin. Un cambio de ubicación tan drástico en tan poco tiempo es logísticamente imposible sin el uso de herramientas tecnológicas para manipular la ubicación.

Cambio de ISP:

Además, se identificó un cambio de proveedor de internet. El usuario pasó de estar conectado a través de Red Digital de Telecomunicaciones de las Islas Baleares S.L. (España) a conectarse a través de NordVPN, lo cual coincide con la aparición de la tarjeta SIM de Benín.

Anomalous behaviour

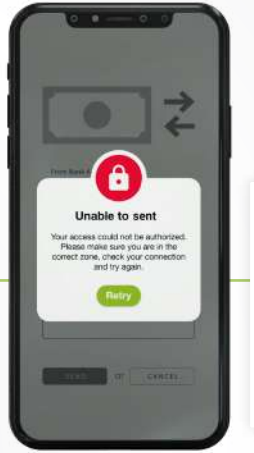
Risk operation I - SIM Swapping



IRONCHIP

Fraud risk

- New device
- Spoofed GPS
- Spoofed IP
- Non-typical location

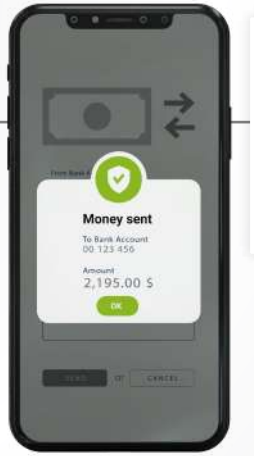


Ironchip analiza información de la localización y detecta el fraude antes de que ocurra.

Otras soluciones

Low risk

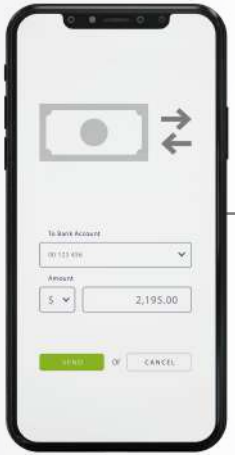
- New device



Otras soluciones analizan sólo la información del dispositivo. Si es nuevo no pueden detectar si es fraude
o no.

Anomalous behaviour

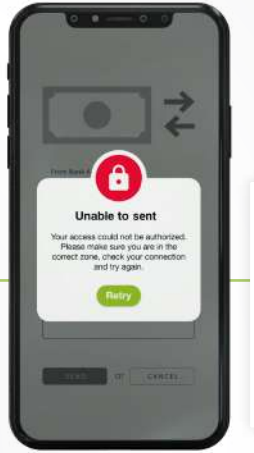
Risk operation Ⅱ - Vishing attacks



IRONCHIP

Fraud risk

- New device
- Last iteration with different pattern.
- Last iteration in call to PIN validation.



Ironchip analiza información de la localización y detecta el fraude antes de que ocurra.

Otras soluciones

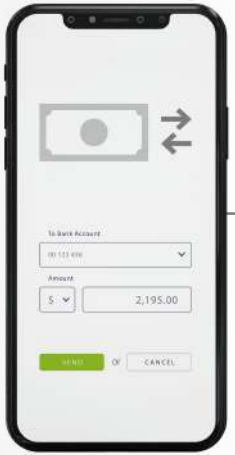
Low risk

- New device

Otras soluciones analizan sólo la información del dispositivo. Si es nuevo no pueden detectar si es fraude
o no.

Anomalous behaviour

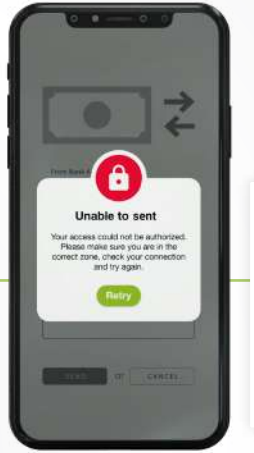
Risk operation Ⅲ - Synthetic identity



IRONCHIP

Fraud risk

- New device
- New account
- Blacklist risky place more than 4 times.

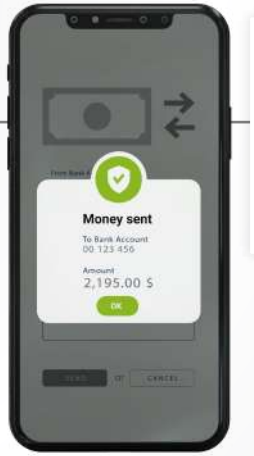


Ironchip analiza información de la localización y detecta el fraude antes de que ocurra.

Otras soluciones

Low risk

- New device



Otras soluciones analizan sólo la información del dispositivo. Si es nuevo no pueden detectar si es fraude o no.

IRONCHIP

Fraud Detection Platform

Casos de éxito

www.ironchip.com

05 Location Fraud Detection

Caso de éxito - ABANCA

Desafío

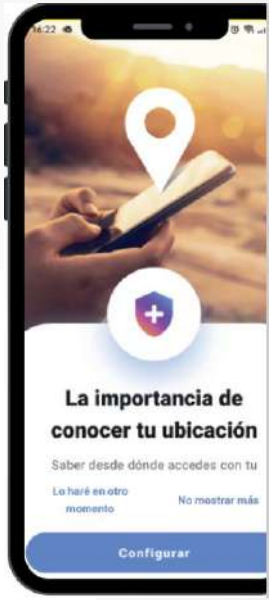
ABANCA requería mejorar sus sistemas de análisis de fraude de IBM debido a la incapacidad para distinguir entre dispositivos individuales, lo que resultaba en pérdidas por fraude debido a su rápido crecimiento y expansión.

Propuesta

Ironchip ofreció su solución innovadora de Fraud Detection, basada en inteligencia de ubicación, para complementar los sistemas de IBM. Asimismo, colaboró estrechamente para adaptar la solución a las necesidades detectadas, mejorando los sistemas existentes, como con la incorporación opcional del GPS.

Solución

Tras un exhaustivo análisis y una prueba de concepto, Abanca ha mejorado significativamente sus sistemas al introducir una capa adicional de prevención de fraude basada en la localización y la diferenciación de dispositivos. La incorporación opcional de GPS en sus procesos de incorporación, inicio de sesión y restablecimiento de PIN ha sido fundamental para este avance. Este enfoque no solo ha aumentado la eficiencia operativa, sino que también ha incrementado la efectividad en la detección de fraudes.



IRONCHIP

Fight Against Identity Threats

Ironchip's Identity & Access Management and Fraud Detection solutions powered by location intelligence technology

www.ironchip.com