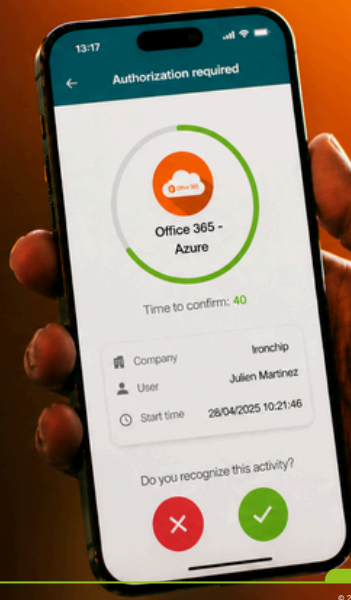
Identity platform

Unified identity management with advanced context analysis

IRONCHIP
CYBERSECURITY



Who are we?

Ironchip is an **advanced, unified identity security platform** that uses contextual identity to verify that each user is who they claim to be based on their unique physical environment.

Through intelligent access control and continuous monitoring, it protects critical business assets by allowing connections only from secure, authorized locations.

IRONCHIP
CYBERSECURITY

Cybersecurity is in our DNA

At Ironchip, security isn't just a word—it's our **commitment**. That's why we hold certifications such as LINCE from the National Cryptology Center (cpstic.ccn.cni.es).

Our solutions have been certified at the HIGH level and included in the **CCN-CERT** Security Products Catalog, which endorses their use in critical environments. Additionally, we have defined secure usage procedures for high-security scenarios (ccn-cert.cni.es)..

The Spanish government supports the company through its investment, making us a key strategic enterprise at the national level.

IRONCHIP
CYBERSECURITY

Organizations that rely on the solution

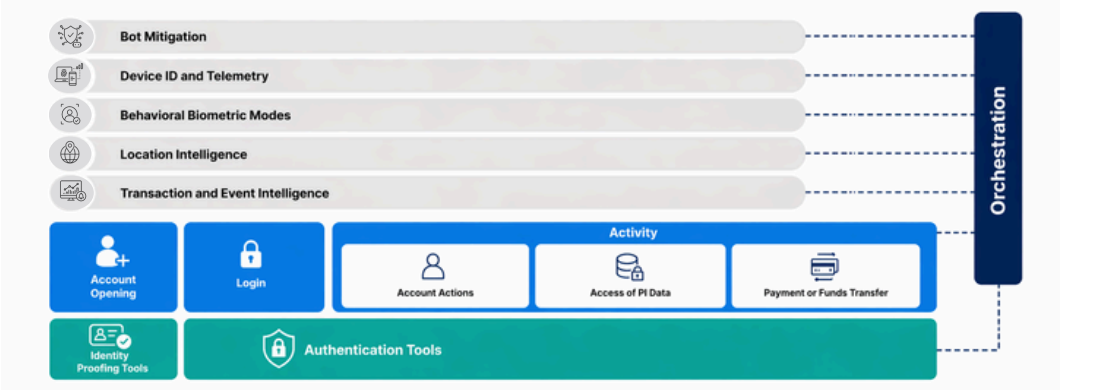
Technology

IRONCHIP
CYBERSECURITY

Location intelligence - Location identity proof

Use of location as part of the authentication and identity management system.

Gartner



Source: Gartner
755906_C

IRONCHIP
CYBERSECURITY

Location-based detection technology

Common Operation Zones

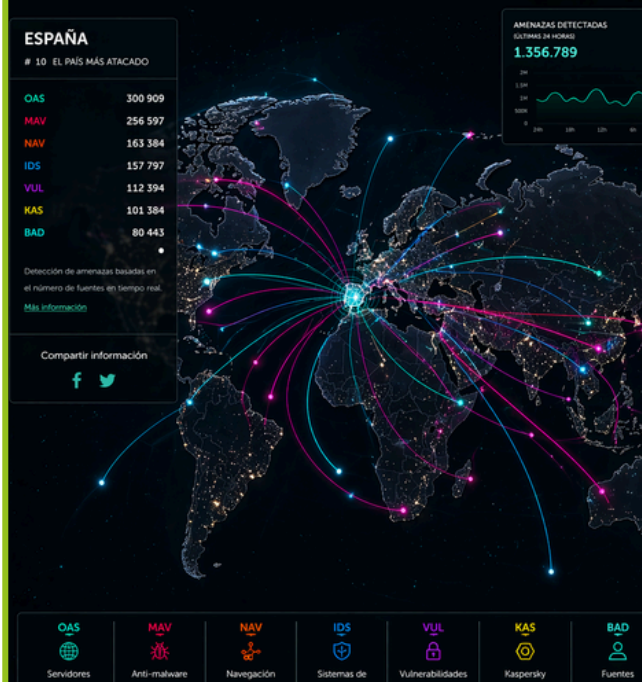
The majority of identity processes take place in trusted locations.

Untrusted Location

92% of attacks occur remotely, from a location the user has never been in.

99% of fraudsters commit fraud from the same location at least twice.

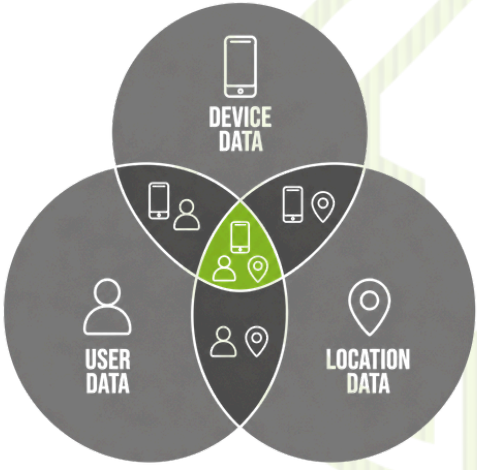
IRONCHIP
CYBERSECURITY



Behavioral localization

Our technology uniquely links the device to its actual location using artificial intelligence and environmental signals (Wi-Fi and cellular networks).

This approach allows us to **model precise behavioral patterns**, which are essential for the secure identity of the future. The ability to understand where the user is and how they interact with their resources offers unprecedented control, setting the definitive standard for security and authentication in digital systems.



IRONCHIP
CYBERSECURITY

Identity **Platform**

IRONCHIP
CYBERSECURITY

Our safety pillars

Passwordless experience

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.

Unified identity

Our platform integrates seamlessly with all your corporate tools, centralizing identity management and ensuring the privacy of your data.

OIDC, LDAP, SMAL, RADIUS, HTTPS

Risk-based security

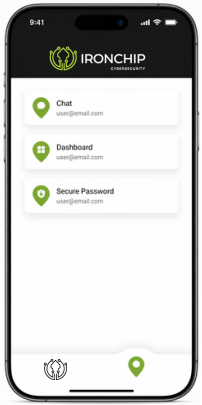
We do not store login credentials on our servers to ensure security. Zero account thefts thanks to device- and location-based intrusion detection.

Multi-device access

Don't your employees have company phones? Ironchip works on Android, iOS, Windows, Linux, and Mac. Plus, you can enhance your security with hardware tokens or USB devices. Or you can even authenticate without agents.

IRONCHIP
CYBERSECURITY

The simplest passwordless experience



Passwordless Authentication

Device Intelligence + Biometry + Hardware Keys

User experience

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

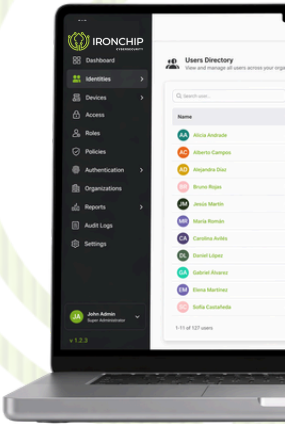
Easiest Management

Identity lifecycle

- Highs, lows, changes and integrations with a single click.
- No passwords, no renewals, no codes...
- No dead points. Full visibility of your identity.
- **Multitenant** solution: : Manage different organizational and territorial units from a single tool.

Data-driven intelligence

- **Complete traceability:** Everything that happens within the tool is fully recorded.

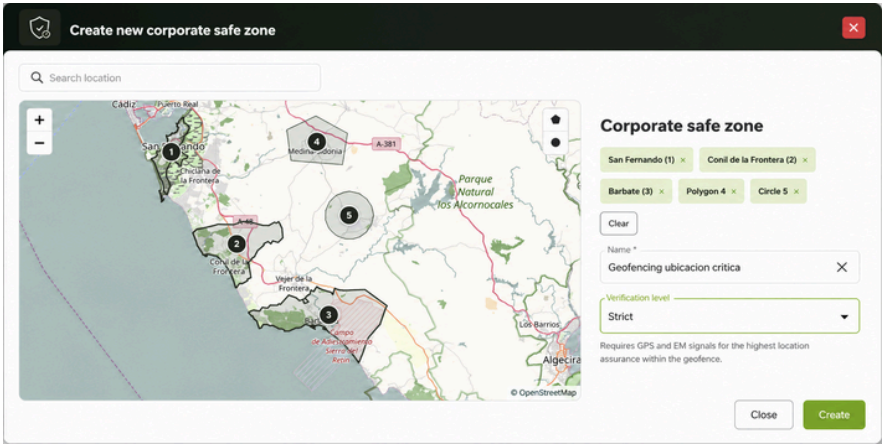


We place the **user experience at the heart** of our design, enabling us to replace passwords with more secure methods that are easier to use and manage.

IRONCHIP

Location as a login credential

Defining secure zones to control access to critical applications and resources



Context-based identity and risk analysis

Zero Knowledge Proofs

Sovereign corporate identity

- **Security:** We do not store credentials on our servers to ensure security.
- **No unnecessary vendors:** No risk of attacks on the identity provider.

Zero account takeovers

- **Anti MITM:** Secure connections impossible to decipher by a third party.
- **Anti Phishing:** The access key is never left on the device, preventing phishing attacks.

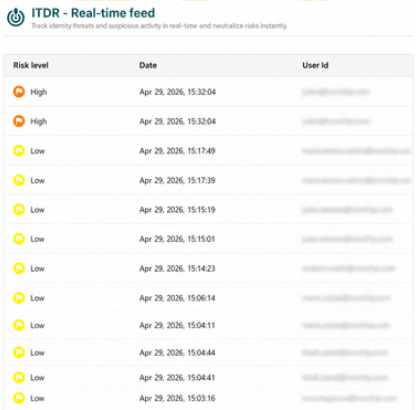
Identity Threat Detection & Response

Transparent risk analysis

- **Scam detection:** We detect social engineering attacks such as phishing or identity spoofing.
- **Real-time alerts:** Detects and/or blocks attacks in real time.

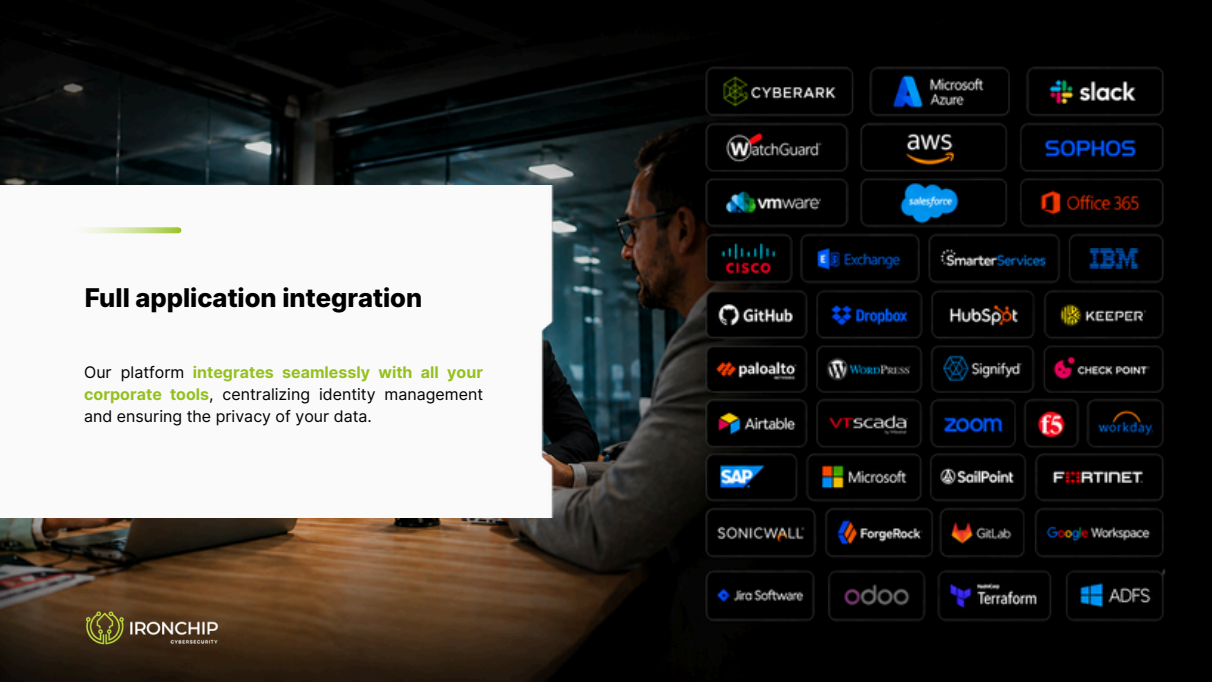
Unique detection methods

- **Location intelligence:** We detect location falsifications, impossible travel, VPNs, Tor, etc.
- **Device tampering detection:** We know if the device has been altered through rooting, emulation, or jailbreaking.



IRONCHIP CYBERSECURITY

We do not store login credentials on our servers to ensure security. Zero account thefts thanks to device- and location-based intrusion detection.



Full application integration

Our platform **integrates seamlessly with all your corporate tools**, centralizing identity management and ensuring the privacy of your data.

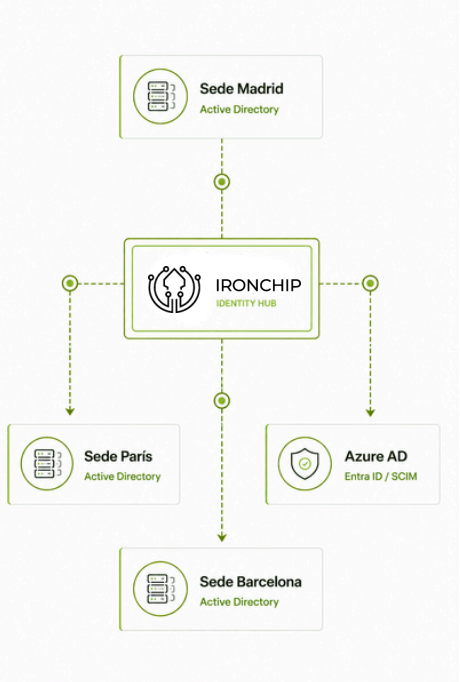
IRONCHIP
CYBERSECURITY

Identity Synchronization and Continuous Monitoring

Real-time synchronization of all identities, eliminating gaps between on-premises and cloud environments.

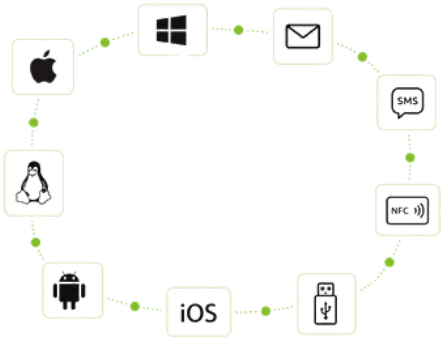
Our ADConnect agent securely and automatically integrates with any on-premises Active Directory. Using SCIM, we connect directly to Azure AD (Entra ID) and other cloud providers.

Every role change or deactivation is instantly propagated to Ironchip, ensuring that no unauthorized access remains active.



IRONCHIP
CYBERSECURITY

All authentication methods

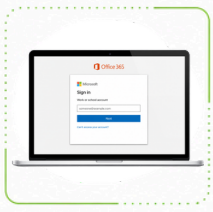


Seamless security, on any device.
Implement contextual identity wherever you need it. From native mobile and desktop apps to passwordless and physical methods:

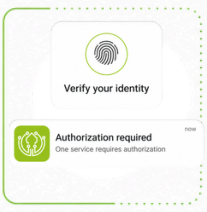
- Devices: Full cross-platform support and dedicated apps.
- Physical possession: Enhance security with USB tokens or NFC/RFID technology.
- Direct connectivity: Quick access via Magic Links and SMS verification.

IRONCHIP
CYBERSECURITY

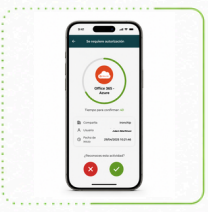
Mobile phone solution



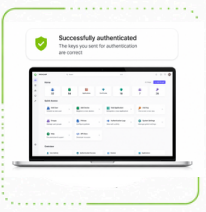
The user is attempting to access the Office 365 corporate resource



Receive a push notification on your mobile device



Open the notification and approve access via the mobile app



Contextual identity is verified; if it is valid, access is granted, and if it is invalid, access is blocked and the SIEM or administrator is alerted.

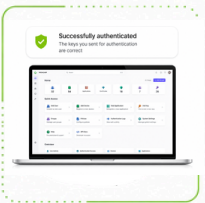
IRONCHIP
CYBERSECURITY

Desktop app solution

The user is attempting to access the Office 365 corporate resource

Receive a push notification in your desktop app

Open the notification and approve access through the desktop app



Once authenticated, the user can access the requested resources

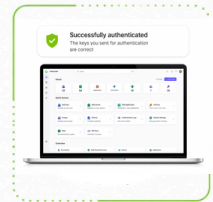
IRONCHIP
CYBERSECURITY

USB token solution

The user plugs in their USB drive and tries to access the Office 365 corporate resource

The USB token syncs with the desktop app and generates the identity using the two keys stored in the desktop app and the USB token

The app reads the generated key and performs authentication



Once authenticated, the user can access the requested resources

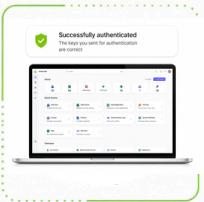
IRONCHIP
CYBERSECURITY

NFC Card Solution

The user swipes their NFC/RFID card through the reader to attempt to access the Office 365 corporate resource

The reader reads the card's identification and converts it into the AD's identity

The card serves as proof of your ownership and is used to fill in the service information to activate the authorization



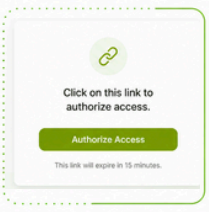
Once authenticated, the user can access the requested resources

IRONCHIP
CYBERSECURITY

Solution for supplier or third-party access

The user attempts to access the corporate resource remotely

You'll receive an email with a Magic Link



Click the link to authorize access

Once authenticated, the user can access the requested resources

IRONCHIP
CYBERSECURITY

Case **studies**

IRONCHIP
CYBERSECURITY

Ayuntamiento de ALCOBENDAS

Sector
Public administration

Location
Spain

Size
Over 1,000 employees

Access Control and Threat Detection in the Public Sector

Authentication via a mobile app combined with SIEM monitoring for real-time detection and response

CHALLENGE

The City Council faced the challenge of securing access to critical systems in an environment with multiple users, devices, and connected services. The lack of centralized visibility made it difficult to detect anomalous access and respond to threats in real time. Furthermore, the growing exposure to attacks using compromised credentials required strengthening both authentication and continuous monitoring. All of this had to be integrated without increasing the operational burden and while complying with regulations such as the ENS.

SOLUTION

A solution was implemented that integrates mobile app authentication with SIEM monitoring capabilities, enabling real-time monitoring and correlation of events. This facilitates the detection of anomalous access attempts and the triggering of automated responses, thereby strengthening security without increasing operational complexity.

RESULTS

- **Early detection of anomalous** access through event correlation
- **Greater visibility and control** thanks to continuous SIEM-style monitoring
- **Automated response** to suspicious access attempts

> Users usually tend to resist change, but I should point out that in this case, it's being very well received thanks to the positive user experience it's providing.

– José Luis Miguel, Security Manager, Alcobendas City Council

IRONCHIP

Santander

Sector
Banking

Location
Spain

Size
Over 200,000 employees

Access control in **corporate environments without the use of mobile devices**

Desktop-based authentication that enables secure access without relying on mobile devices

CHALLENGE

Santander needed to implement a multi-factor authentication solution compliant with regulations such as the ENS, ensuring secure access to its digital ecosystem. Reliance on mobile devices posed a limitation in environments where users did not have them or could not use them. This made it difficult to ensure consistent access to critical systems across the entire organization. Furthermore, it was necessary to maintain accessibility without compromising security or the user experience.

SOLUTION

A desktop-based multi-factor authentication solution was implemented that combines a password and OTP without requiring a second device. This ensures secure access to corporate systems from any environment, while maintaining control and accessibility for all users.

RESULTS

- Secure access to corporate systems without the need for mobile devices
- **Compliance with regulations such as ENS** without compromising accessibility
- **Greater control and centralized access** management in global environments

> Seamless, hassle-free login thanks to our desktop solution for Linux, Mac, and Windows.

IRONCHIP

nalanda

Sector
Technology

Location
Spain

Size
+200 employees

Access protection via physical **token authentication**

Access to sensitive data via physical token-based authentication, ensuring frictionless security

CHALLENGE

Nalanda needed to secure access to sensitive information stored on its corporate devices, ensuring that only authorized users could access it. The reliance on mobile devices for authentication posed an operational limitation in its environment. Additionally, it was necessary to implement a robust system without compromising ease of use for employees. All of this had to ensure full access control while maintaining process efficiency.

SOLUTION

A customized multi-factor authentication solution was implemented that replaces the use of a mobile device with a physical token, distributing the identity verification process between the user and their device. This ensures secure access to corporate systems while maintaining a simple user experience.

RESULTADOS

- **Secure access to sensitive data** without relying on mobile devices
- **Greater control and visibility** for IT teams in managing access
- **Seamless authentication that maintains efficiency in d**aily use

> We believe that it is a company that is constantly evolving and growing, focusing on customer needs to meet their expectations.
>
> **– System administration**

IRONCHIP

IRONCHIP
CYBERSECURITY

Do you have real control over identity management in your organization?

These questions reflect the actual level of control you have over your digital identity. Any area not covered represents a potential vulnerability.

If the answer to any of these questions is no, it's time to take action.

Talk to us

- Do you have users **without mobile devices** who need robust MFA, but you're not sure how to provide it?
- **Could you instantly block access** if a user is in the right city but at an unauthorized location?
- Is your current **MFA vulnerable to notification fatigue** (push spam) or phishing attacks?
- **Is your IT team struggling** to manually manage identity onboarding and offboarding across multiple platforms?
- Do you comply with the **strictest regulations (NIS2, ISO 27001)** regarding access control and traceability?
- **Do you have full control** over third-party and external vendor access to your critical infrastructure?
- Can you verify **with absolute certainty the exact physical locations** from which your employees are connecting?
- Are you **able to consolidate all your Active Directory environments** (on-premises and cloud) and audit policy changes in real time?
- **Does your current system alert you to anomalous behavior** the moment someone accesses your systems?
- Are your r**emote access connections via RDP or SSH** protected by more than just a simple password?

IRONCHIP
CYBERSECURITY

Verify identities before they become a security incident.

IRONCHIP
CYBERSECURITY

IRONCHIP
Identity Security Platform

Beurko Viejo 1, Barakaldo
Paseo de la Castellana 200, Madrid

+34 944 075 954
www.ironchip.com