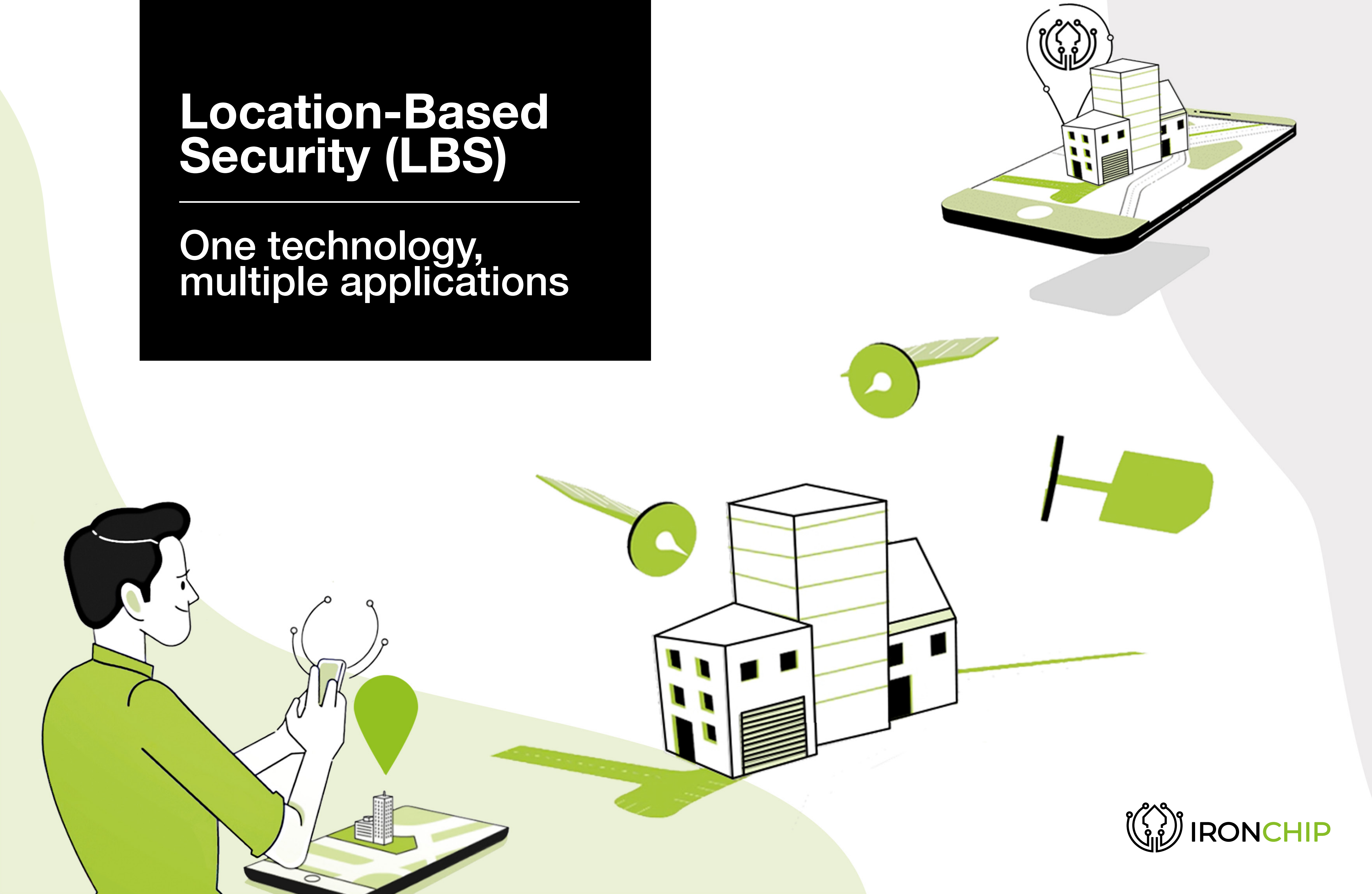
Location-Based Security (LBS)

One technology, multiple applications



IRONCHIP

Introduction....03
Towards the new trends of cybersecurity....03
Geolocation and security....04
Location-Based security....05
How it works....06
One technology, multiple applications....07
Industry use cases....08
Fintech use cases....14
Law enforcement use cases....21
Other use cases....25

index

Introduction

Digitalization, Industry 4.0 and teleworking are increasingly present in our environment, causing many companies and institutions to open their systems to the Internet, increasing the risk of having their security compromised. This digitization process has accelerated in 2020 with the arrival of the pandemic caused by the COVID-19 virus, which has caused an **increase of 125%[1] in cyber-attacks in Spain in the last year, reaching 40,000 attacks per day.**

Towards the new trends of cybersecurity

In a context in which digitalization and interconnectivity are more present than ever and, as a consequence, there has been a notable increase in cyber-attacks, seeking and betting on alternative and innovative cybersecurity solutions is more important than ever.

“People are at the center of all business, and they need digitalized processes to function in today’s environment.”**Major technology companies such as Gartner are already talking about new cybersecurity trends that include, among others, the Internet of Behaviors or IoB, “anywhere operations” or remote operations and Artificial Intelligence.**

The Internet or security of behaviours aims to capture, analyze, understand and respond to all kinds of digital representations of human behavior and interpret them using innovative technologies and machine learning algorithms.

Learning from human behavior could in many cases put an end to security breaches by identifying, eliminating and preventing anomalous or risky behavior, such as the identification and detection of false identities or credential theft, which can be used to gain access to devices or services of various kinds and thus jeopardize the security of systems.

In addition, the most common attack in digital environments is the **theft of credentials or passwords, which is the cause of 81% of security incidents**. For this reason, **Microsoft is already talking about “replacing passwords with biometrics or authentication on a device which you own”.**

If it was already vital to **ensure the security of “anywhere operations”** before, Gartner is already talking about this cybersecurity trend as something primordial after the digital acceleration and teleworking produced by the pandemic.

With teleworking, millions of companies have been forced to use remote access tools, and in **March 2020 alone, Spain recorded more than 19 million[2] attacks on RDP (Remote Desktop Protocol), one of the most used tools.**

However, remote operations do not only apply to telecommuting. To close the systems security gap, it is necessary **to implement methods to ensure all types of secure operations from any location**, and therefore it is necessary to verify that, the location from which an operation or attempt is made to access information or services, is an authorized or usual location for the user.

[1] https://www.interempresas.net/Ciberseguridad/Articulos/346890-Los-ciberataques-en-Espana-han-crecido-un-125-por-ciento-en-el-ultimo-ano-hasta-los-40000.html
[2] https://www.itdigitalsecurity.es/endpoint/2020/05/espana-registro-mas-de-19-millones-de-ataques-al-rdp-solo-en-marzo

Geolocation and security

Geolocation presents several security and usability problems, reason why it has not been present in security systems until now. The main problems can be summarized in the following two points:

1. **Most geopositioning systems are based on coordinates**, that is, using a GPS sensor the device obtains a latitude and a longitude with which you can locate a position on a map. Although it is useful for most applications, it is not for cyber security since any user with Google Maps can obtain coordinates and send a false location. Not only that, but there are hundreds of applications for mobile devices that allow you to send false coordinates, making it very easy for an attacker to steal, for example, the location of our house.
2. **Geolocation requires a GPS sensor**, something that not every device includes, preventing its use in certain equipments, such as laptops or desktops.

How do we put an end to all these problems?

The best way is to add innovative security layers that take into account the identity of the device from which the service is accessed, using secure communication channels and factors that are more difficult to spoof. That is why at Ironchip we are launching a unique technology in the market, Location-Based Security, our AI that uses wave based location as a security factor.

Location- Based Security,

“Security based on wave-based location”

In order to achieve a truly secure location that is difficult to falsify, we have replaced the typical latitude and longitude with other more advanced geolocation methods, based on Artificial Intelligence and Big Data processes.

Instead of using the GPS sensor, we are able to determine whether the device is in a secure location from the radio waves that surround it, that is, we analyze wifi signals, signals from mobile devices such as 2G, 3G and 4G, or even from IoT signals like Sigfox or Lora.

Our Artificial Intelligence process analyzes the radio waves found at the location, and creates a unique wave signature from them. This fingerprint must be sent again when the user wants to access the system.

1. Replacing the coordinates for the set of waves, we prevent any remote attacker from falsifying our location. To do this, the attacker would have to be physically in the safe location, which makes the attack extremely difficult and makes automated attacks impossible.
2. Any device with a Wifi card can be geolocated.

In addition, this geolocation technology is the first totally anonymous alternative, since by not knowing the coordinates of the location, only the waves, it is not possible to locate this location on a map.

Ironchip’s unique location technology also has the following characteristics:

Location-Based Security. Location as a security factor

- **Secure and difficult to falsify**

  Replacing the coordinates for the set of waves, we prevent any remote attacker from falsifying our location. To do this, the attacker would have to be physically in the safe location, which makes the attack extremely difficult and makes automated attacks impossible.

- **Totally anonymous**

  Ironchip’s wave based location technology is the first totally anonymous alternative to other systems that use location as a security factor since, as we do not know the coordinates of the location, only the waves, it is not possible to place this location on a map.

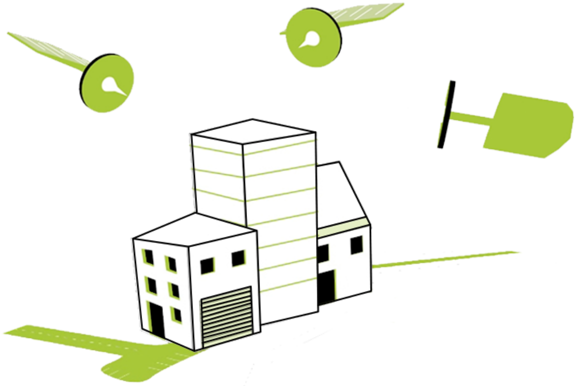
- **Encrypted information**

  We do not store the wave information anywhere, neither on the server nor on the client. Our artificial intelligence learns, and then immediately destroys the wavelet information, so we only store the predictive mathematical algorithm that, when it receives the wave information, will determine whether it is valid or not.

How it works

Analyzes the location waves

Ironchip’s Location-Based Security technology analyzes the waves detected by a mobile/desktop device to create a digital identity associated with that location. In this way, it identifies whether the device from which the operation is performed is a recognized device and, by analyzing the waves in that location, it also verifies whether the operation has been performed from a secure location or area.



A unique signature of the waves is created

By replacing the coordinates with a set of waves, Location-Based Security technology creates a secure signature associated with a specific and secure location. This makes it the first fully anonymous alternative to other systems that use location as a security factor, since it is not possible to place this location on a map.

Sending signature to validate access

The device analyzes the waves of the location and then sends a signature associated with that location to verify that the user is in a secure area. In this way, Ironchip’s technology has many uses or applications, ranging from using location as a security and authentication factor, to identifying and learning what a user’s usual places of operation are and thus using location as an extra layer of security.

One technology, multiple applications

The infinite applications of our technology are designed to guarantee high information security requirements, providing all the necessary security layers.

In a context in which digitalization and interconnectivity are more present than ever, there has been a notable increase in cyber-attacks. According to the Sonicwall cyber threat report of 2021[1], in the last year ransomware attacks and attacks on IoT devices have grown by more than 60% worldwide.

Cyber-attacks in Spain have also increased by 125% in 2020 and, according to the FBI's[2] Internet Crime Report 2020, Spain is the 14th country in the world with the most cyber attacks and the fifth in Europe.

This is a problem that affects all types of sectors, from industry to financial services and public organizations of various kinds. In this context, the searching for and betting on alternative and innovative cybersecurity solutions is more important than ever.

That is why major technology companies such as Gartner are already talking about new cybersecurity trends that include, among others, the Internet of Behaviors or IoB, "anywhere operations" or remote operations or Artificial Intelligence. In the same way, Microsoft is also betting on "replacing passwords with biometrics or authentication on a device which you own".

Ironchip's technology, Location-Based Security, is a unique technology in the market that analyzes the waves surrounding a mobile/desktop device to create a digital identity associated with that location. In this way, this technology that is based on AI and Big Data has infinite uses or applications in sectors such as industry, Fintech or Law Enforcement.

These use cases or applications range from using location as a security and authentication factor to, for example, granting or denying physical or remote access using location as a key, to identifying and learning a user's usual places of operation and thus using location as an extra layer of security to, among other things, identify identity theft.

Through our work with customers we have designed a number of use cases for different sectors. Throughout the document we will develop several security solutions and applications that Ironchip's technology can bring to different sectors such as industry, financial industry or law enforcement, among others.

[1] https://www.sonicwall.com/2021-cyber-threat-report/
[2] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Industry

Location-Based Security for industrial applications.

New technology with multiple applications in the industrial world, IoT or OT communications.

Digitalization and Industry 4.0 are increasingly present in our environment, causing many companies and institutions to open their previously isolated systems to the Internet, increasing the risk of compromising their security. This is a challenge that organizations in any sector must face, but it is of particular importance in industry, as it has found it necessary to adopt remote and more connected operation models.

In fact, according to a SonicWall[1] report, attacks on IoT devices have increased by 66% in 2020, reaching 56.9 million attacks worldwide.

Most cyberattacks are carried out by automated machines, exploiting typical weaknesses shared by different companies and systems, not unlike the vulnerabilities exploited in the 1990s. These automated attacks are based on programs with the only mission of stealing passwords, such as MIMIKATZ, one of the most used programs by cybercriminals in 2020.

In addition, passwords are often a headache for employees, as they have to remember a large number of passwords, which can lead to a security breach in the systems.

And how do we put an end to all these problems?

The best way is to add innovative security factors that take into account the identity of the device from which the service is accessed, and that use secure communication channels and factors that are more difficult to falsify than a password. If they also ensure that both users and companies have an easy and secure user experience, four out of every five attacks would be eliminated.

Using location as an access key, it would only be possible to connect to the company's services from a secure location, thus eliminating most attacks. Ironchip's technology analyzes the waves surrounding a mobile device/desktop to create a digital identity associated with that particular location, using that secure location as a key to access any system.

In other words, the operator of an industrial plant would use this device both to verify his identity and to verify that the place from which he is operating is a secure location or area, replacing or reinforcing password-based systems and making remote attacks impossible.

[1] https://www.sonicwall.com/2021-cyber-threat-report/

Physical access

It is based on the supervision and access control of suppliers and operators, allowing them to physically access a place, such as an electrical substation. As an administrator, you can determine which employee or subcontractor can access your facilities, regaining control of who can access and when.

In this way, we forget about physical access keys, biometric hardware or passwords that can normally be forgotten, lost or even shared or duplicated without our knowledge. With Ironchip you can enjoy comfortable and safe physical access:

- **Location as access cards:**
  Use the user's device and a safe place as an access card to get into the most critical spaces.
- **Temporary access:**
  Grant access to your employees the day and time you want.
- **Access control:**
  Control who, when and where each critical system is accessed.
- **Unique and non-transferable key:**
  Each employee will use their own mobile device and fingerprint, which makes the keys unique and non-transferable.

Remote access

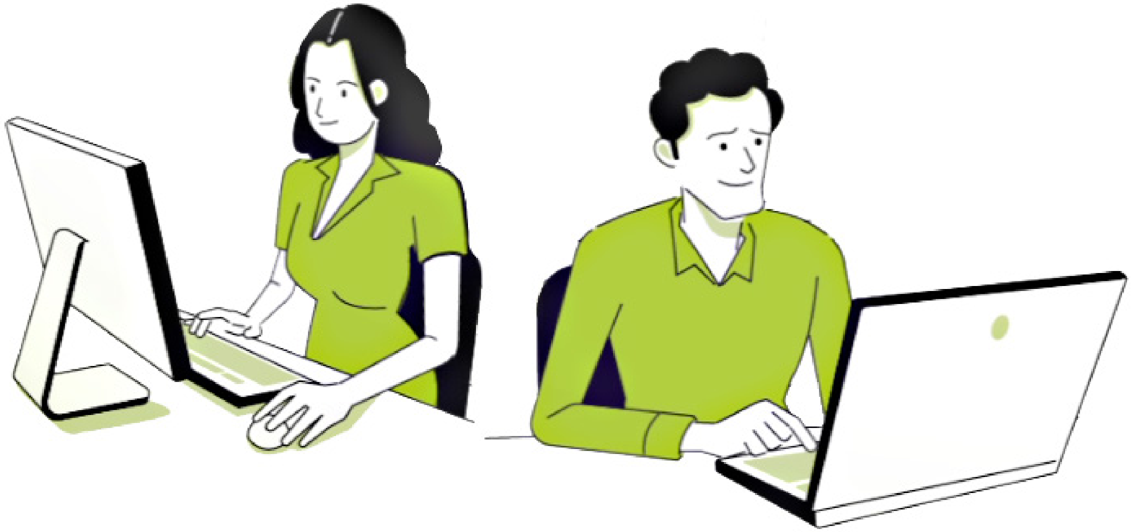
With Ironchip you can guarantee the security of remote accesses to your services and corporate network. It allows you to add our secure authentication layer to any remote access solution, both SDP and VPN, protecting these connections with your employees' safe places.

- **Located access:**
  Limit the access to your services, only allowing access from secure geolocations, avoiding all kinds of remote attacks.

- **Security:**
  Don't make security depend on a simple password or USB hardware that is difficult to install and incompatible with your systems.

- **Simple access:**
  Quick and instant access to services for your suppliers and employees with just one application.

- **Unique and non-transferable key:**
  Each employee will use their own mobile device and fingerprint, which makes the keys unique and non-transferable.



CERT/SOC security

It allows you to guarantee security in your operation centers, such as SOC, ROC or GOC, so that the services can only be accessed from the location of the operation center. That is how we end with all remote attacks that occur from outside our operation center.

- **Located access:**
  Limit the access to your most critical services, allowing only access from your operation center, avoiding all kinds of remote attacks.

- **Standards-based integration:**
  Integrate your current solutions through RADIUS, SAML or OIDC.

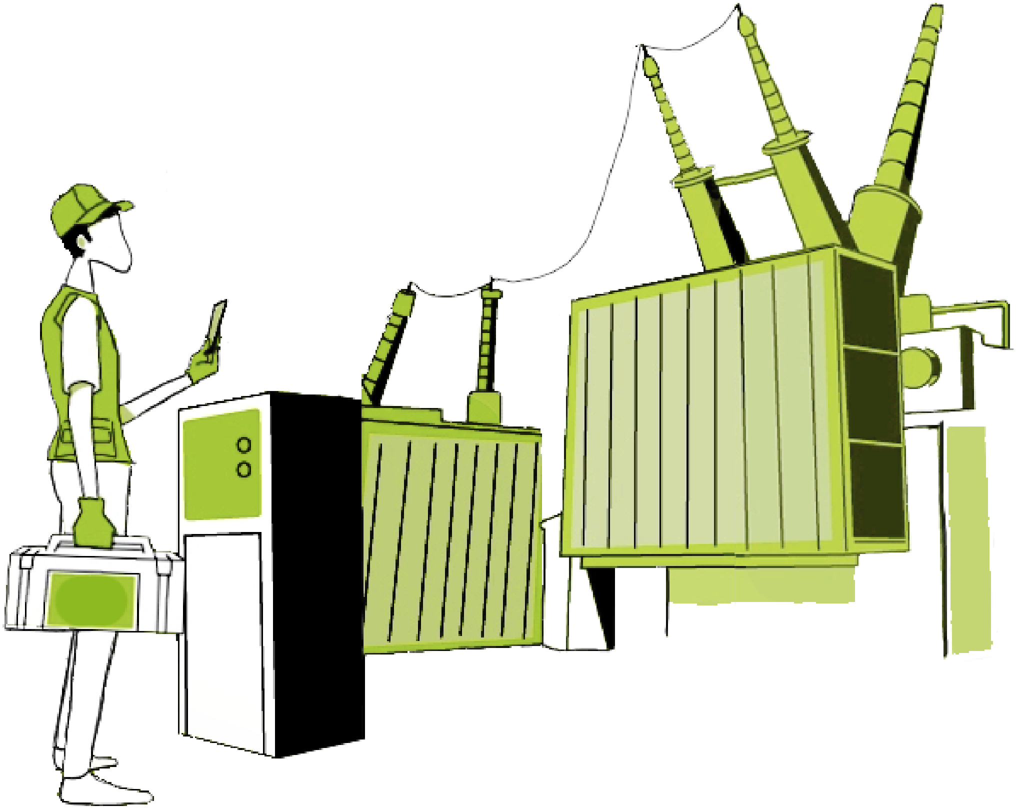
Zero Time Deployment (ZTD)

Automatic security deployment of any IoT device, using its location as a security key. With this, the company that hires our services forgets about keeping passwords.

- **Location as certification:**
  Use the installation locations of the IO devices as certificates or credentials anonymously.

- **Installation without friction:**
  Use the installation locations of the IO devices as certificates or credentials anonymously.

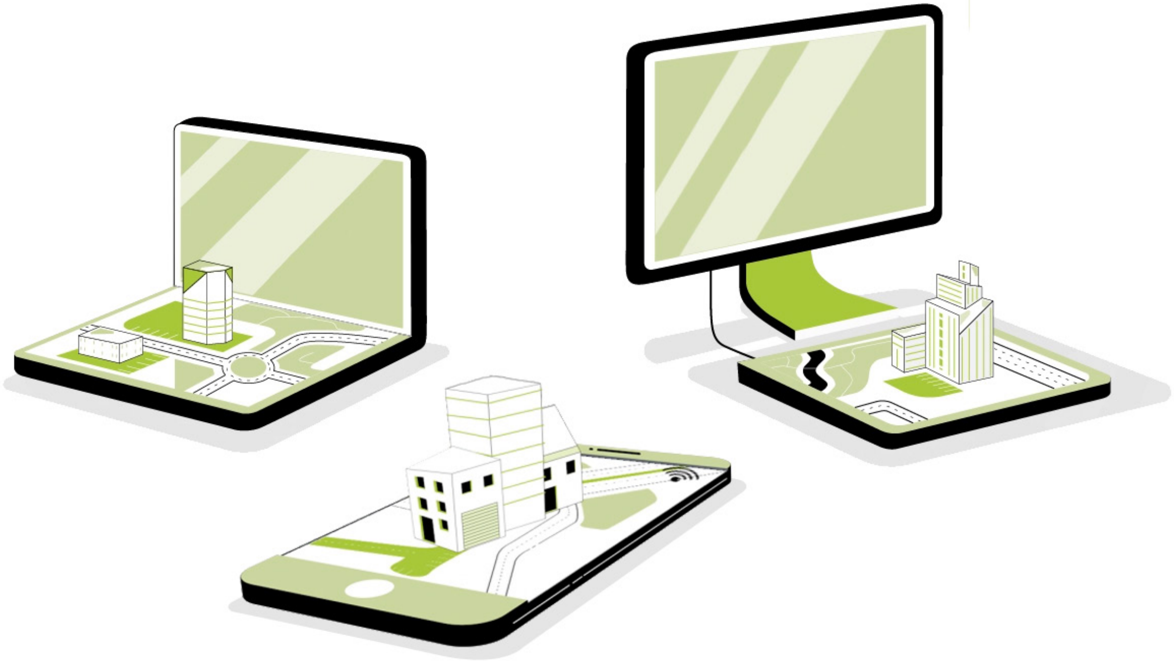
- **No more certificates:**
  Managing the security of your devices is easier than ever as there are no security certificates or passwords.



Presence control of devices

Ironchip allows you to detect and control the existence of devices in a controlled environment, such as an office, being able to detect whether a device such as a person's mobile phone is in this environment, and certifying whether the mobile belongs to a known user or unknown. This application is an alternative to the classic access control lathes, much easier to implement and cheaper.

- **Easy to use:**
  Completely transparent for the user.
- **Total control:**
  Not only do you control the physical security at the entrance, but in all your facilities.
- **Real time:**
  It detects intrusions the moment they occur.



Fintech

Location-Based Security for Fintech applications.

E-commerce, anti-fraud and exceptional cash movement solutions.

In an increasingly digitized and interconnected world, financial services have also undergone a process of digitization that has accelerated with the pandemic crisis caused by COVID-19. According to a report by Capgeminii[1], **47% of Spanish people claim to have increased their use of digital payments over the last year, a figure that stands at 45% on the global average. It is estimated that, globally, the number of online banking users will reach 3 billion by the end of 2021**, 53% more than the previous year. And everything points to this being a trend that will continue in the future.

Even so, the digitization of payments and the use of online banking brings with it a problem for both financial services and their users. This digitization of banking services has led to a **350% increase in identity theft attacks compared to 2020**, saccording to the S21sec[2] Intelligence Team.

In addition, there has been a **37% increase in phishing attacks on mobile devices**, a method of identity theft that can lead to security breaches in organizations and companies, as well as emptying the bank accounts of any user who is a victim of this attack that uses social engineering techniques.

These social engineering techniques can also lead to SIM swapping or synthetic identity scams, two types of scams in which, by impersonating the victim's identity, attackers can access the user's digital banking and perform banking operations on their behalf. In addition, in the case of SIM swapping, this scam also exposes the vulnerability of 2-step authentication systems based on SMS or calls.

For this reason, Fintech or financial services companies have found it necessary to innovate and look for new fraud detection solutions to help them be prepared.

How can we solve this problem?

The aim is to profile the modus operandi of cybercriminals, in other words; to find patterns in their behavior and to identify behavior that is likely to be fraudulent.

> Using location as a security factor serves as a fraud detection layer that helps identify whether the user that performs the transaction is a fraudulent identity.

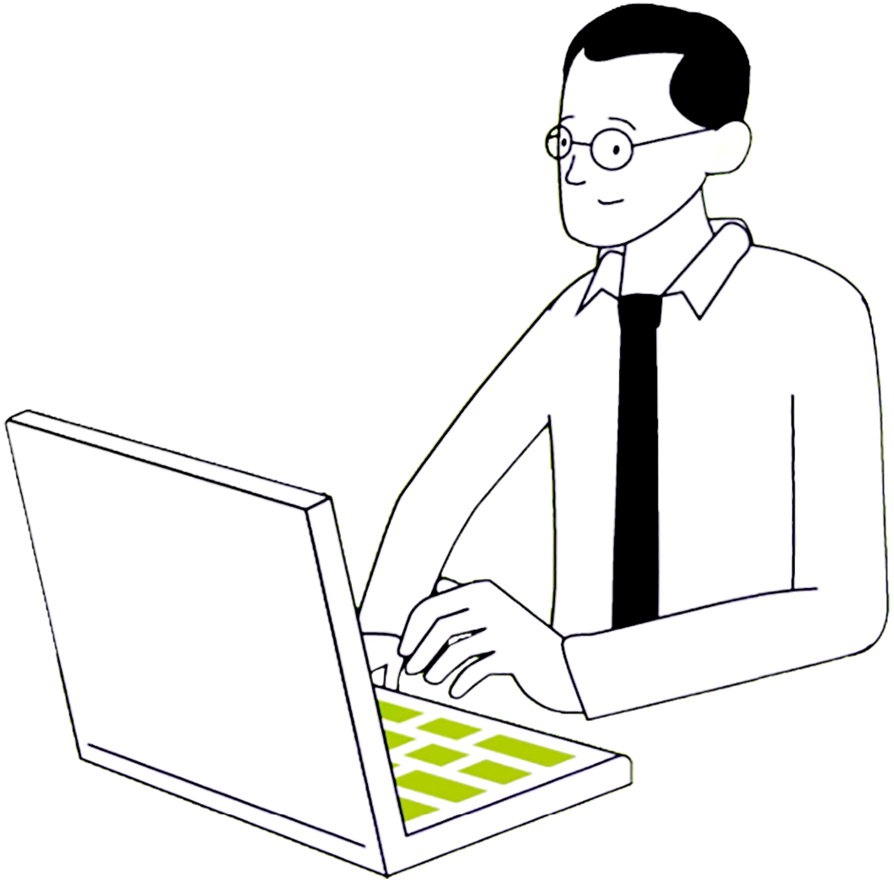
Ironchip's wave based location identifies and learns the user's usual places of operation and, therefore, detects any fraudulent behavior when operating, in other words: it identifies whether the user that performs the transaction is authorized to do so by their location.

The applications of Ironchip's technology in the Fintech sector range from fraud detection, using location as an extra layer of security and integrable to any system, to ATM protection, transaction authentication or secure in-store payment, using location as a security factor.

Executive account

Ironchip adds a layer of Location-Based Security to accounts with large amounts of assets, so that transfers can only be made, for example, from your office.

- **Located risk transactions:**
  Authentic risk transactions with our geolocation layer.
- **Protection against attacks:**
  Reduce false positives by protecting yourself against man-in-the-middle and replay attacks with Location-Based Authentication.
- **Delete the coordinate cards:**
  Replace the coordinate cards and SMS with Location-Based Authentication.



Transaction authentication / PSD2 regulation

Ironchip helps reduce fraud and comply with PSD2 regulations in banking transactions, both online transactions and those that occur in swift networks, the international network of financial communications between banks and financial entities. We protect the accounts of operators and customers with our location-based authentication, so that risky transactions pass this security filter.

- **Located risk transactions:**
  Authentic risk transactions with our geolocation layer.
- **Protection against attacks:**
  Reduce false positives by protecting yourself against man-in-the-middle and replay attacks with Location-Based Authentication.
- **PSD2 Compliant:**
  It complies with current European regulations PSD2 with our Location-Based Authentication authentication solution.

Fraud detection

With Location-Based AntiFraud you can detect fraud in transactions, taking into account the geolocation of users. Location-Based AntiFraud learns which are the usual places from which each client connects, and detects fraud if a transfer is not made from one of those places. All of this is made in a totally transparent and anonymous way.

- **Transparent security:**
  Completely transparent for the user.
- **Effective detection:**
  Eliminate false positives with a new factor, saving response time.
- **Non GPS location:**
  Thanks to LBS, no remote attacker will be able to falsify its location, as it happens with IP or GPS location.

ATM protection

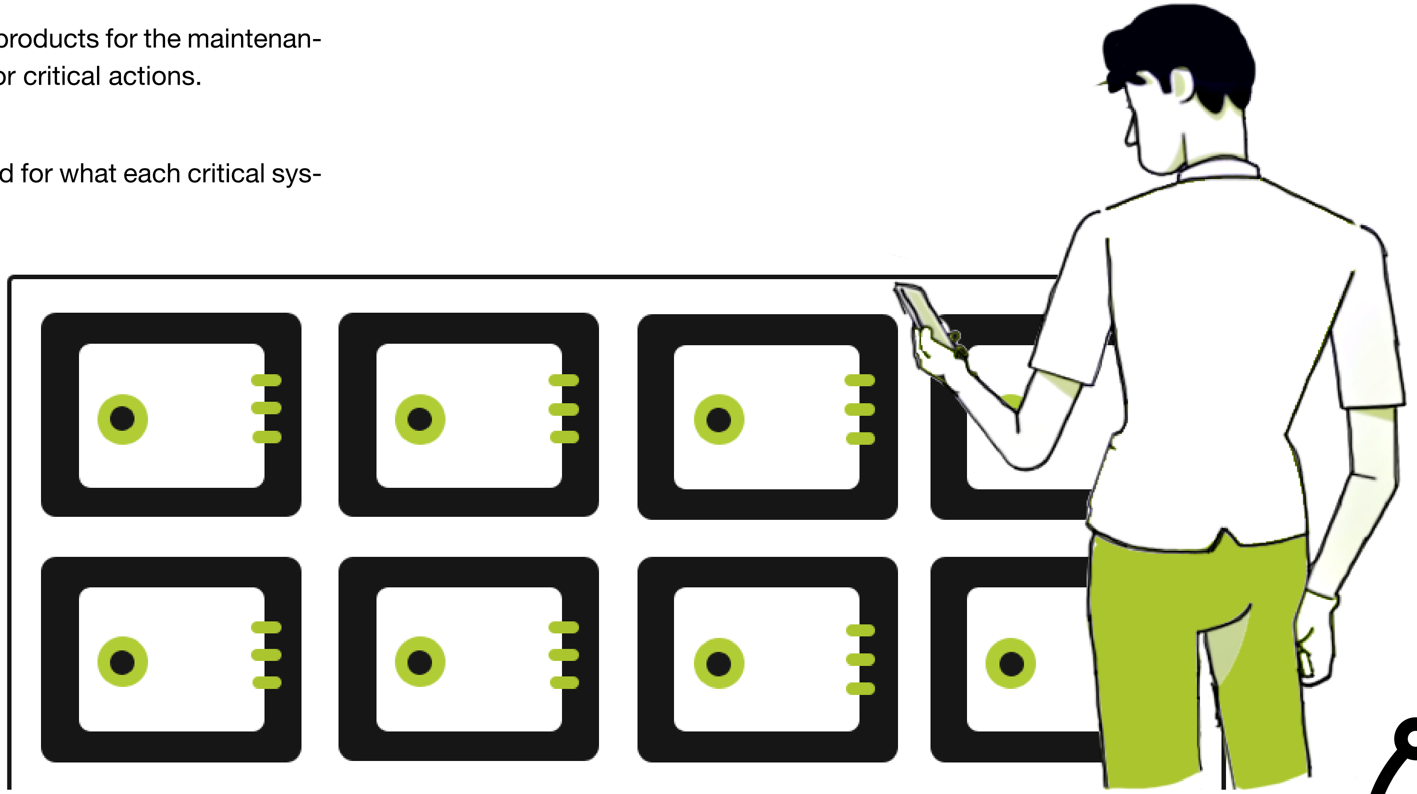
Ironchip can identify users who want to carry out a transaction at an ATM without the need for passwords or cards, proving their identity with the mobile phone and their fingerprint and certifying that the device is in front of the ATM. This ends both ATM fraud, due to card theft, and the remote attacks on these ATMs.

- **Your card on the mobile:**
  Use the user's device and a safe place as a substitute for the credit card. No need for NFC sensors or insecure Bluetooth connections.
- **Easy to use:**
  Completely transparent for the user.
- **Security for your customers:**
  Avoid physical and online card thefts. In order to withdraw money you need a fingerprint and mobile phone.

Safe boxes

Our technology allows you to generate a temporary password to open a safe box if you are in a specific place with an authorized device and fingerprint.

- **Location as access card:**
  Use the user's device and a safe place as an access card.
- **Temporary password:**
  Obtain the credentials of the products for the maintenance of the intelligent network or critical actions.
- **Tracking suppliers:**
  Control who, when, where and for what each critical system is accessed.



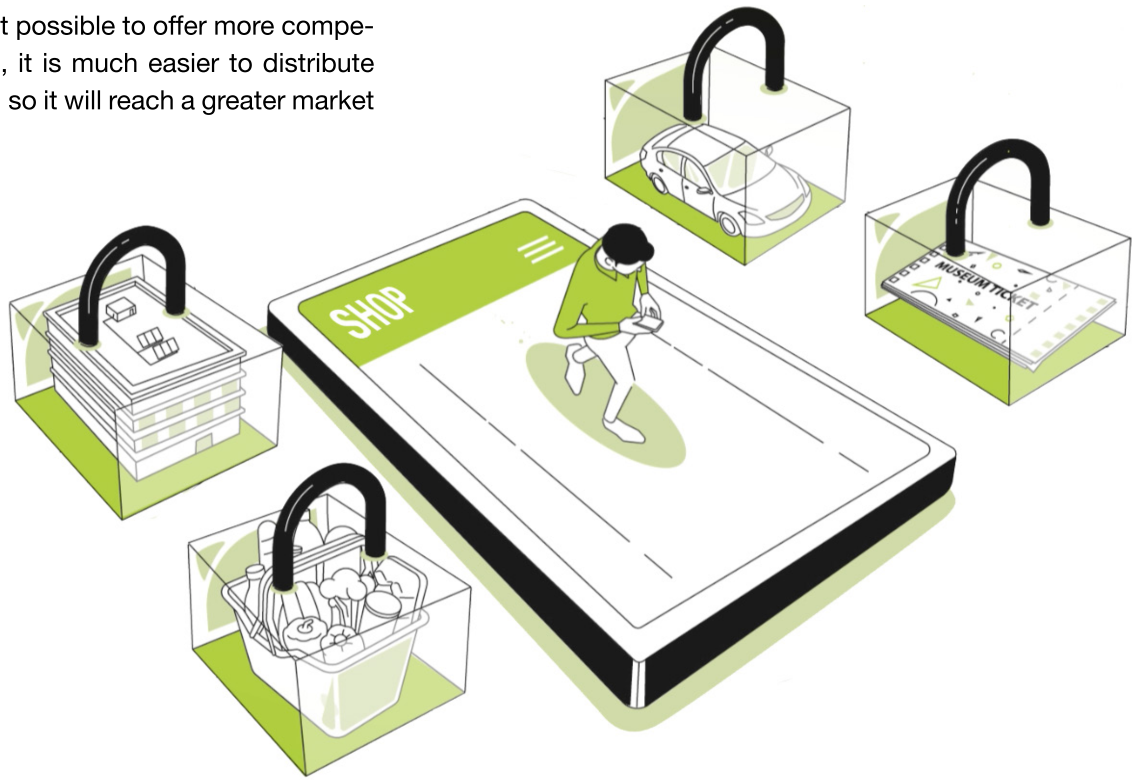
Secure store payment

Our technology makes it possible to use a mobile device as a dataphone, using the geolocation of the premises as a key to identify the business, and the user's mobile device plus their fingerprint as a credit card. This is a solution that eliminates the hardware of dataphones, making this business more scalable and with lower costs, as well as facilitating the way to pay users.

- **End with dataphones:**
  Reducing costs makes it possible to offer more competitive prices. In addition, it is much easier to distribute software than hardware, so it will reach a greater market share.

- **Secure payment:**
  Easy and contactless.

- **Theft of transactions:**
  It will not be possible to steal from establishments by impersonating their identity, since identity is the location of the premises itself, contrary to what happens with QR codes.



Law enforcement agencies

Location-Based Security for law enforcement applications.

New technology with multiple applications in the world of law enforcement and law enforcement agencies.

The digital transition, which has accelerated as a result of the pandemic crisis caused by the Covid19 virus, has caused that cyber-attacks in Spain increasing by 125% in 2020, even reaching 40,000 attacks per day. This is a problem that affects citizens as well as companies and public and private organizations, including law enforcement agencies.

In recent months, several public bodies have been the focus of several cyber-attacks. In Spain the State Public Employment Service (SEPE) suffered a cyber-attack in March 2021 that paralyzed its services throughout the state, thus affecting both the entity and the citizens as a whole. In addition, just one month later, in April 2021, the National Statistics Institute (INE) and the Ministries of Justice, Education and Economy of the Spanish Government were victims of a wave of synchronized cyber-attacks.

A security breach in this type of critical systems could paralyze many essential services in the electronic administration of a country, as well as obtain confidential information that compromises the agency and its security.

How can we solve this problem?

Ironchip's technology, Location-Based Security, has multiple applications in the field of protection of this type of organizations. Using the wave based location as a security factor, it is possible to reinforce the systems of these entities. In this way, it is possible to grant or deny access to confidential information or documentation only from a specific and secure location, using location as a key to access this documentation and thus putting an end to most remote attacks that can compromise the security of these organizations.

In addition, it can also be applicable to present and future challenges such as electronic voting. By integrating Ironchip's technology into existing security standards, the voter could set up a secure area that verifies the voter's identity in order to ensure the security of the voting system, all in a way that is transparent to the user.

Encrypted communications

Our technology encrypts communications on devices with our technology. This allows your company to have secure and secret communications.

- **Military grade encryption:**
  A TLS-based secure communication layer with an additional layer of end-to-end elliptic curve cryptography.

- **Localized messages:**
  Configure your messages so that they can only be read or sent from defined secure areas.

Electronic voting

Currently, many forms of electronic voting are not secure. Ironchip can secure these votes, protecting them with the geolocation that the voter chooses, such as their home.

- **Easy integration:**
  Integrate with security regulations and custom integrations.
- **Easy to use:**
  Completely transparent to the user.

Document traceability

Our technology protects the most confidential communications and document downloads, allowing you to have secure communications protected from leaks.

Your company's information will be totally protected, limiting access from assigned locations, knowing at all times the traceability of these and to make the detection of a data leak possible.

- **Information traceability:**
  Know who accesses the most critical services and when.

- **Located documentation:**
  Configure your most critical information so that it can only be read or sent from the secure locations defined.

- **Simple access:**
  Quick and instant access to employee services with just one application while in the secure location.

- **Encrypted communications:**
  Our technology encrypts the communications in the devices with our technology, and this allows to have secure and secret communications.

Other use cases

Geofencing

Establish virtual limits in a real geographical area to set a radius of interest in which an assigned user will be alerted when leaving the established perimeter. These are its characteristics:

- **Easy to use:**
  Completely transparent to the user.
- **Easy integration:**
  Integrate with security regulations and custom integrations.
- **Multi-device:**
  Integrate with multiple systems such as SCADA systems.

Courier service and transportation

Another clear example is the application of Ironchip for the courier service and transport market, so that delivery routes such as those used by large distributors like Amazon, new delivery channels with drones or even future autonomous vehicles cannot be hacked.

Within the transportation and courier service, we have the ability to design our own navigation systems, since the navigation system of the frigates and submarines are mostly designed taking the GPS into account.

What they do not know is that Russia or Iran are using GPS as a hacking factor, changing their coordinates in the middle of the shipment and therefore, preventing these war machines from being located.

For this case, we believe that we can make a huge difference by creating a positioning without GPS that prevents these attacks.

- **Easy integration:**

Integrate with security regulations and custom integrations.

Cybersecurity policies

The insurer will provide protection against a cyber attack and in the event that it occurs, the insurer will indemnify for damages caused on the basis of the established agreement.

- **Protection against attacks**
  The insurer will provide protection against a cyber attack and in the event that it occurs, the insurer will indemnify for damages caused on the basis of the established agreement.
- **Easy to use:**
  Completely transparent for the user.

Location-Based Security. One technology, multiple applications.
www.ironchip.com

Contact Ironchip's sales team

Aitor Zaballa

✉ aitor.zaballa@ironchip.com 📱 617 898 342