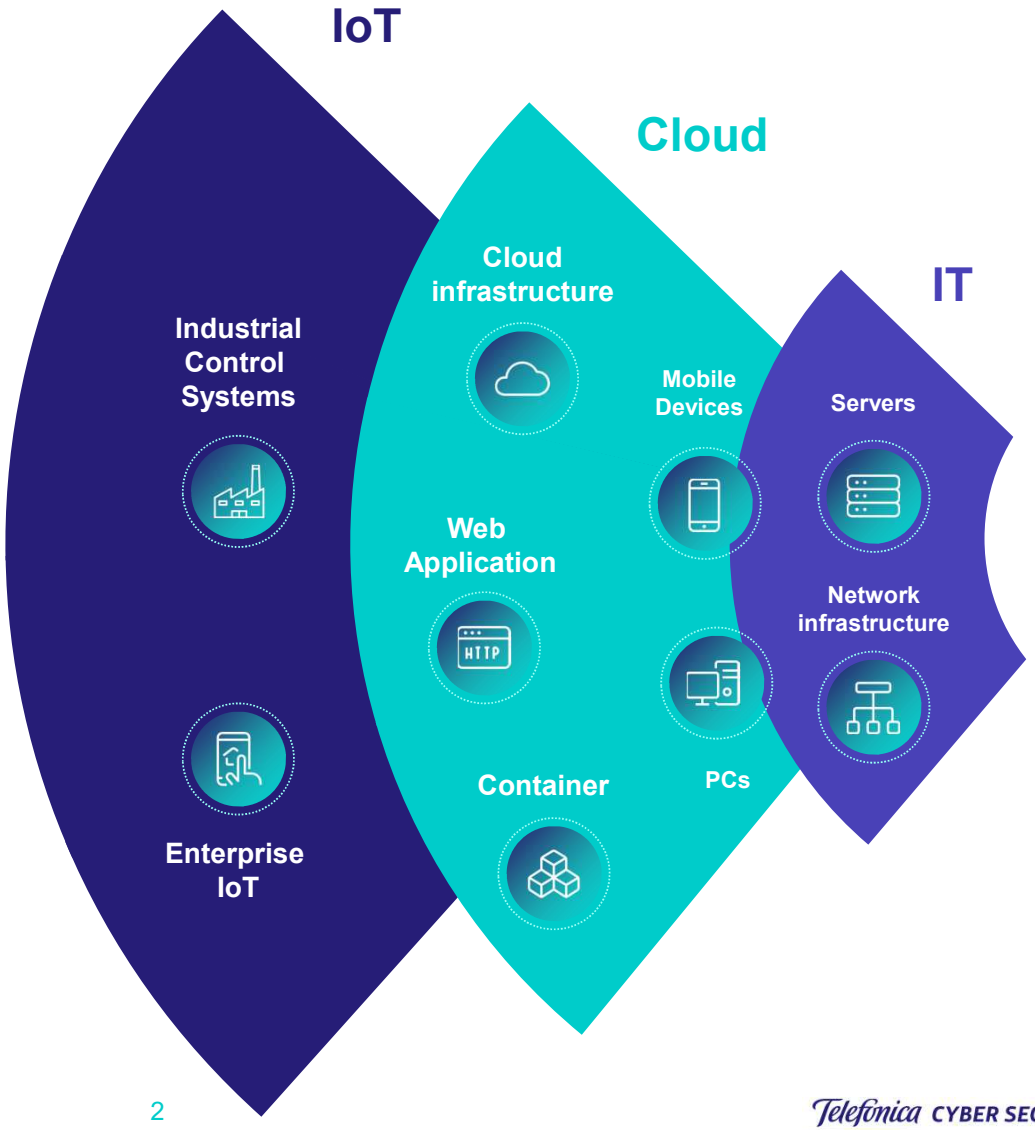
Eleven Paths

OT and IoT Security

Helping our customers to securely embrace the next digital wave

Telefónica CYBER SECURITY COMPANY

IoT (and IIoT)
is a new wave in the digital world evolution that makes the organization attack surface more elastic

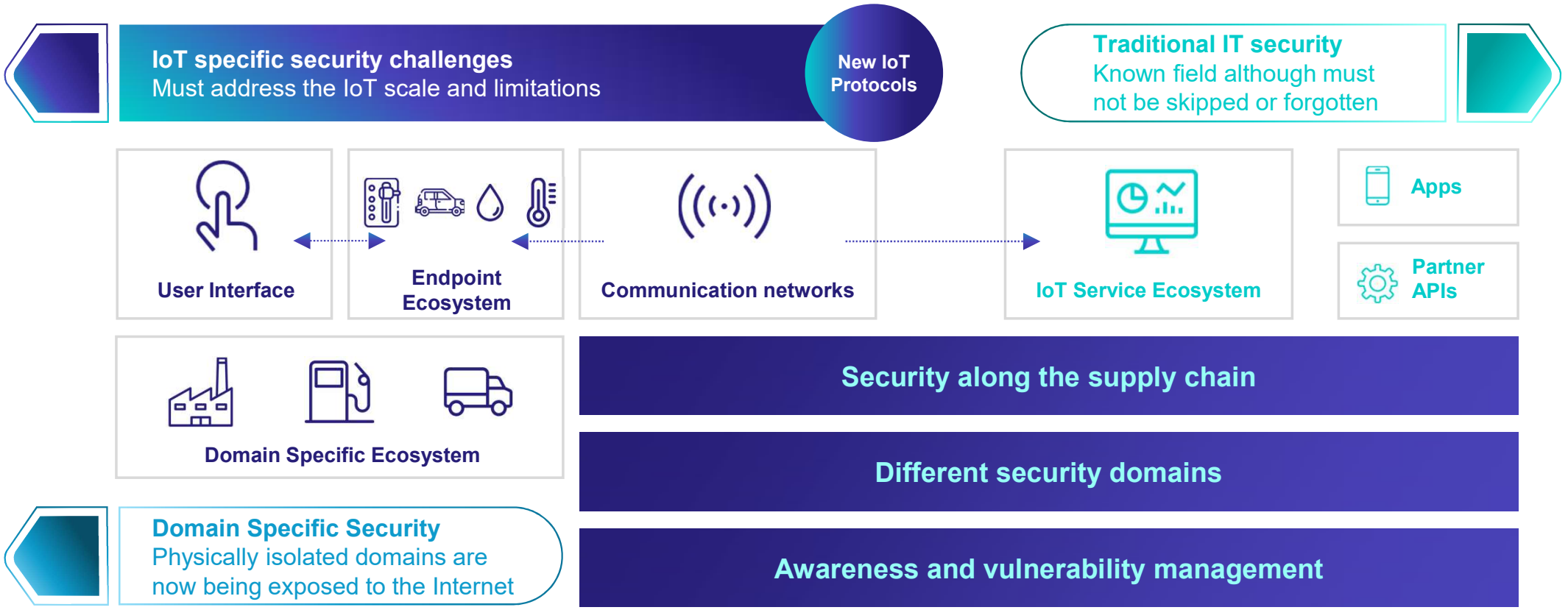


ElevenPaths

Telefónica CYBER SECURITY COMPANY

IoT Security

IoT brings a set of security challenges that must be tackled with an e2e approach



IoT brings a set of security challenges that must be tackled with an e2e approach

Challenges

Solutions

01

e2e Security

The heterogeneity of the IoT architecture components (i.e. devices and platforms) and the number of actors involved in the supply chain requires professional services for security auditing and consulting.

Professional Services

02

Device identification and mutual authentication

Each IoT device must have its own application-level identifier and there must be a mutual authentication between the device and the IoT platform.

Secure Credentials

03

IoT traffic visibility and security monitoring

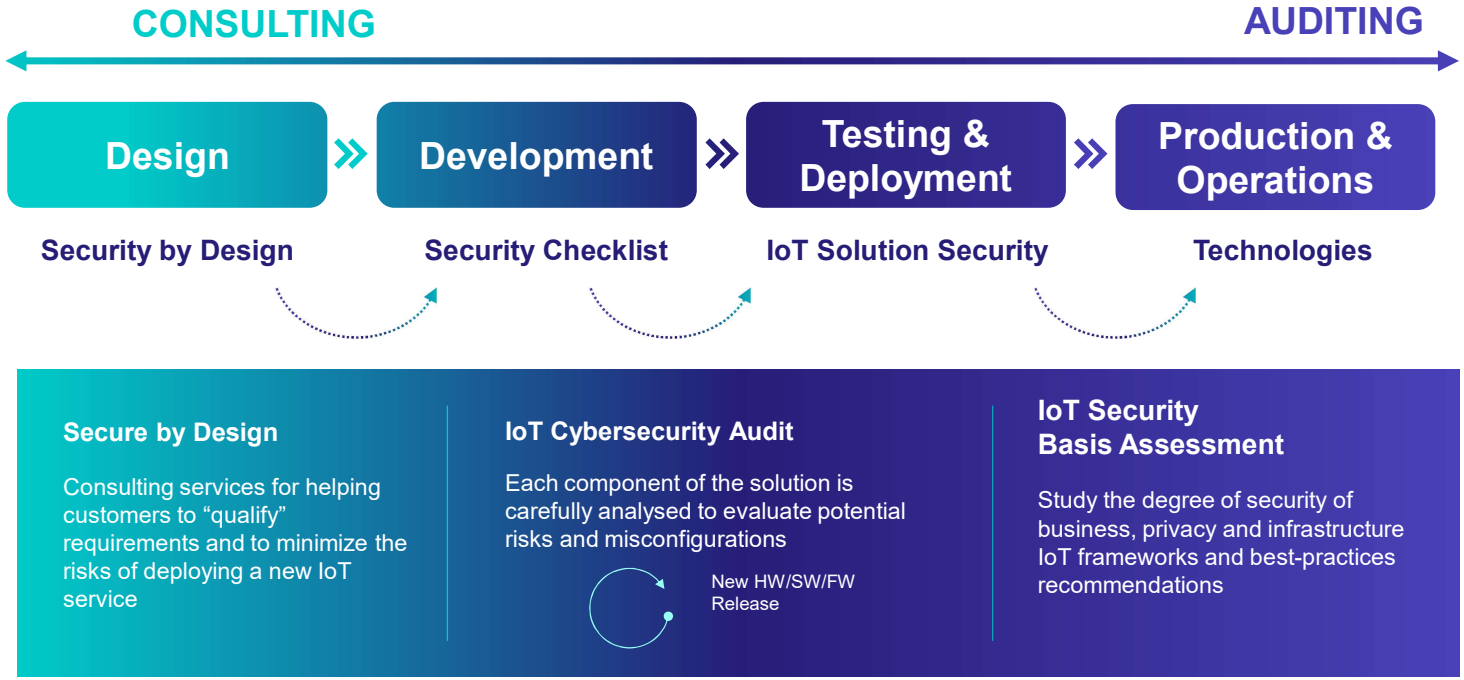
IoT Connectivity customers need to be aware of all the devices that are using the IoT lines and to detect when anomalous and malicious behaviour takes place.

IoT Threat Detection

IoT Security - Professional Services

Consulting & Auditing

Key during the whole life-cycle of your IoT Project



IoT Security

Professional Services

The Internet of Things (IoT) is increasingly present in our daily lives. The IoT ecosystem is a young ecosystem that needs computer security protection measures in order not to be compromised. In addition, it is made up of multiple actors such as IoT devices, networks, applications or cloud platforms that need to be analysed to ensure that they comply with the best security recommendations.

From Telefónica, we understand perfectly the problem of security and its possible consequences. For this reason, we work to guarantee the peace of mind of our customers knowing that their IoT solution includes the best practices in security matters, whilst they have all the appropriate defence mechanisms. We support our customers during the whole life-cycle of an IoT deployment, establishing a strategic end-to end security approach to support customers in the different phases that make up a technological project at IoT.

ElevenPaths

Target Segments

SME and Large Enterprises

Energy, manufacturing, retail, utilities, mining, water management, building automation, oil & gas, connected vehicle, transportation, automotive, healthcare sectors

Benefits

Keep security under control along the whole IoT supply chain: from device manufacturer, communication service providers, to private infrastructure or public cloud platforms

Keep focus in your business while IoT security specialists identify the risks brought by new specific IoT technologies and devices.

Generation of practical recommendations against the detected vulnerabilities. Likewise, an active evaluation of the implementation of those recommendations.

Features

Secure by Design: Consulting service for helping customers to start from secure designs and make sure they meet “qualification” requirements to minimize the risks of deploying a new IoT service

IoT Cybersecurity Audit: Technical audit focused to verify that the security requirements are met and, hence, to ensure that the IoT deployment is protected against the identified risks. Our specialists perform penetration tests to:

- Analyse each component of the solution
- Evaluate potential misconfigurations
- Includes FW, HW and physical testing

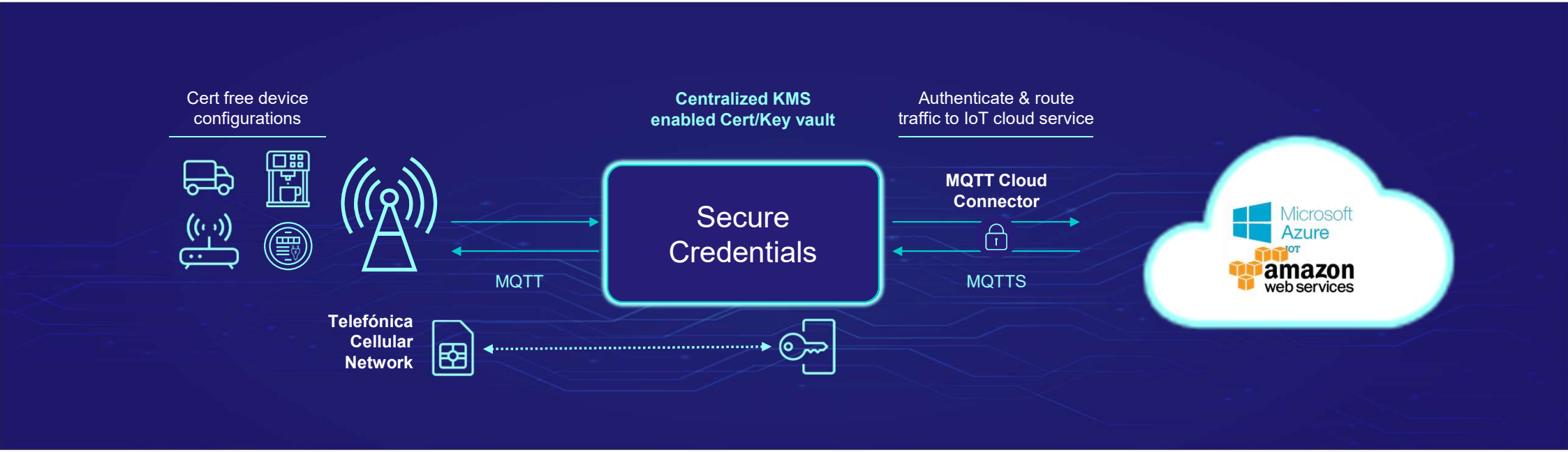
IoT Security Basis Assessment: Following recognized IoT framework recommendations, our consultants will evaluate the security posture of the customer’s IoT deployment at business, privacy and infrastructure levels

Service Offering

Telefónica assists their customers to secure IoT deployments with IoT specialised security consultants, understanding their specific needs and building the right security solution in any project phase establishing a strategic end-to end security approach.

Secure Credentials

Simplifying cellular device access to the cloud



IoT Security

Secure Credentials

Generalized attacks against IoT devices are not a theoretical concept, they are already a reality. Mirai malware, discovered in 2016, aimed at devices such as Internet-enabled cameras (IP cameras) and other IoT products. Mirai's attacks were successful because this malware uses common default credentials (such as a username and password set by the "administrator") and poor device configuration.

If you cannot trust IoT devices… can you trust in the data they collect? If you cannot trust in collected data… … can you take business decisions based on their analysis? To secure your business, trusting your IoT devices is a must. Each IoT device must have its own identifier and there must be a mutual authentication between the device and the IoT platform.

Target Segments

SME and Large Enterprises using cellular IoT connectivity and Public Cloud IoT services

Energy, manufacturing, retail, utilities, mining, water management, building automation, oil & gas, connected vehicle, transportation, automotive, healthcare sectors

Benefits

The main benefits for customers of Secure Credentials are:

Simplify the credential Life-Cycle management: Inbuilt management and reporting controls give oversight of data flows, certificates status and eliminate unnecessary overages.

Cost reductions by mitigating the risks of error-prone tasks.

Reduced development effort: No need for security software development or install required on the IoT edge: "Cert free" device configurations". Minimal effort and time to securely connect IoT edge to the cloud and/or on-premise

Ease of scale: Start with a single device and on-demand grow to thousands of connected devices (Long tail IoT)

Features

Routing and secure communications to cloud services

Automates the set up of cloud identity and certificates

SIM card and Telefónica network as a trusted anchor to verify the identity and integrity of IoT devices.

Use of cellular identity to seamlessly link to cloud-side credentials for secure end-to-end IoT communication

Forwards traffic to cloud IoT service

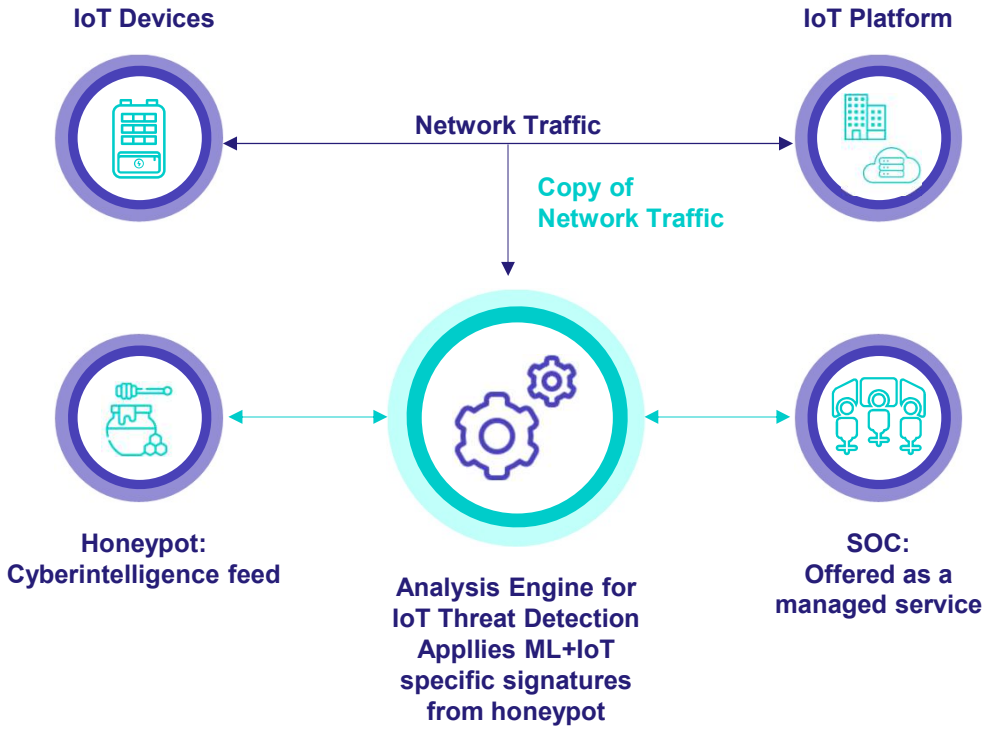
Service Offering

IoT device identity plays a crucial role in the authentication process against the IoT platform. Secure Credentials automates the process of providing a secure identity to IoT devices for accessing Public Cloud IoT services.

IoT Threat Detection

Visibility » **Threat Detection** » **Mitigation**

Visibility	Threat Detection	Mitigation
Visibility and profiling of devices (extracting normal patters of their behavior)	Detection of anomalies and attacks by means of ML and IoT specific cyberintelligence feeds	Easy integration with main firewalls and SIEMs



IoT Security

IoT Threat Detection

In IoT, the E2E is complex, heterogeneous and variable. There are several situations that threaten the different parts of the IoT architecture, like attacks to the IoT platform, attacks to/from Internet, attacks to the IoT devices, illegitimate requests between devices, etc. Moreover, new attacks are being created specifically to target IoT devices.

Because of these potential attack vectors it is necessary to gain visibility on the behavior of IoT devices and perform security monitoring to make sure that devices do exactly what they are supposed to do. IoT Threat Detection is a solution designed specifically to protect the E2E in IoT environments. Being leveraged on the network, it provides visibility and detects both anomalies and attacks. Analyzing the traffic by using Machine Learning techniques and cyberintelligence feeds extracted from an IoT/OT honeypot network, it can detect both known and unknown attacks.

ElevenPaths

Target Segments

Companies with IoT devices that have cellular connectivity (although it could be applied to other types of connectivity) in different verticals such as utilities, connected car, smart cities, healthcare, energy, manufacturing, retail, building automation, transportation, automotive, etc.

Benefits

Agentless solution that provides E2E protection: The solution does not need to install anything on the devices. Given the limited resources of some IoT devices and the volume of devices, is an advantage. It can protect the whole E2E, detecting attacks or anomalies in any element of the architecture.

Managed service at IoT scale: The service is managed by the Telefónica SOCs distributed around the world, making sure to deliver the best service to customer and discarding false positives. Besides receiving periodic reports, customers are alerted when an incident is detected. The service scales to IoT dimensions.

No impact in connectivity SLAs: Since the solution analyzes a copy of the traffic, the IoT service is not affected in any case. It neither introduces delays nor affects the SLAs for connectivity.

Features

Visibility and profiling: The solution brings visibility on the behavior of IoT devices and other elements of the architecture. It can profile devices, i.e. extract the patterns of their normal behavior. It is done using Machine Learning algorithms.

Threat detection: Once the normal behavior is identified, deviations from that can be detected. It includes anomalies and attacks including high traffic volume, malware infections, tampering of the device, misconfigurations, etc. Besides Machine Learning techniques, IoT specific signatures are applied to identify the type of threat.

Easy integration for mitigation: For the application of mitigation actions after detection, it is possible to easily integrate IoT Threat Detection with firewalls, SIEMs or other elements from the main vendors.

Service Offering

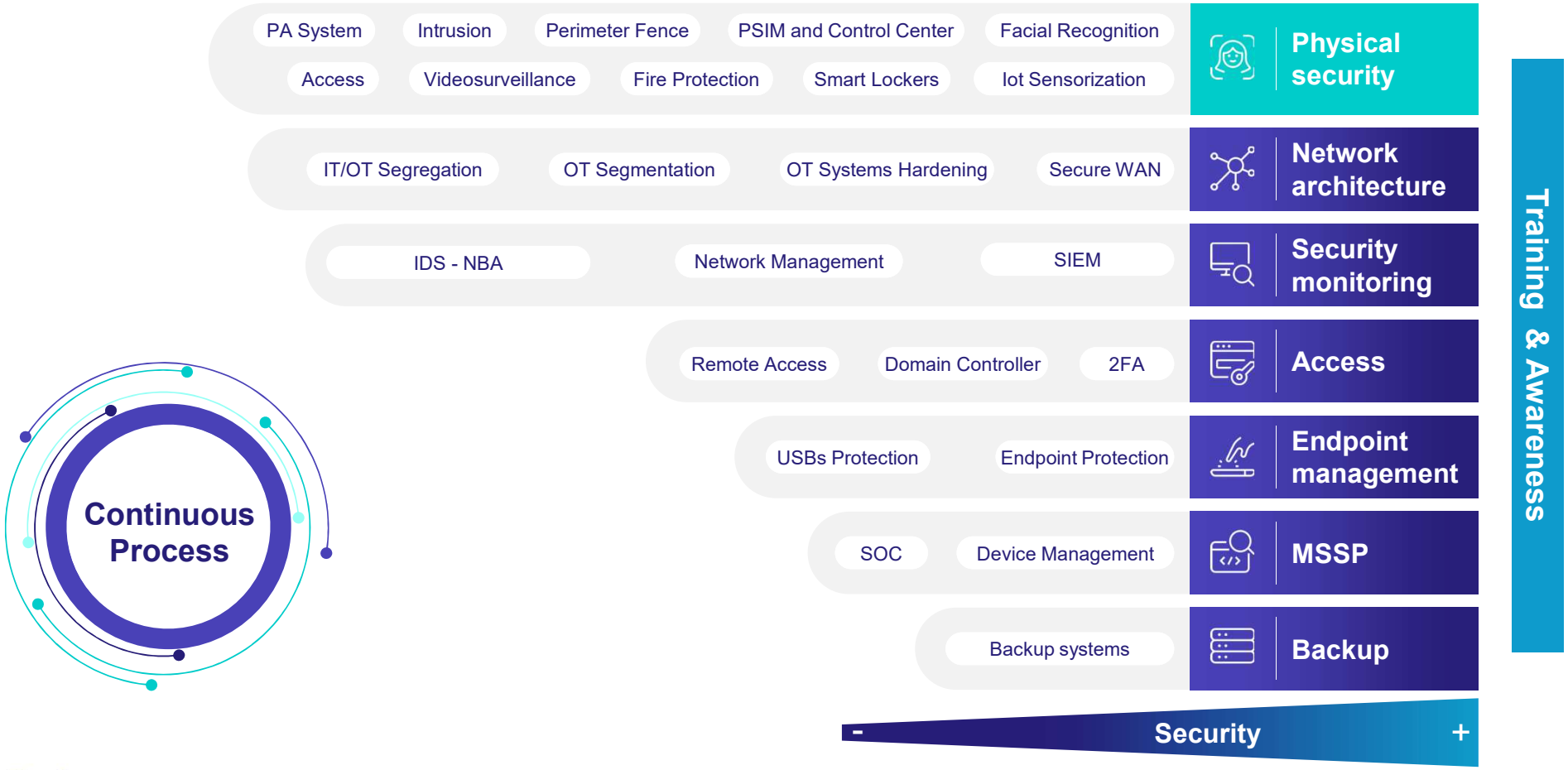
Managed service

Modalities:

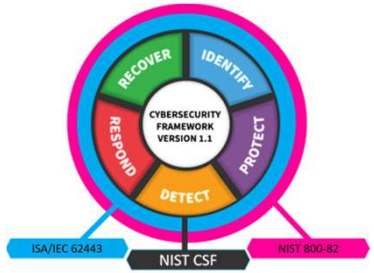
- On premise
- On network

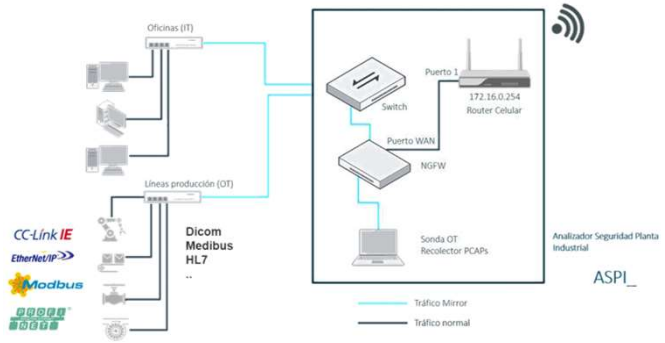
OT Security

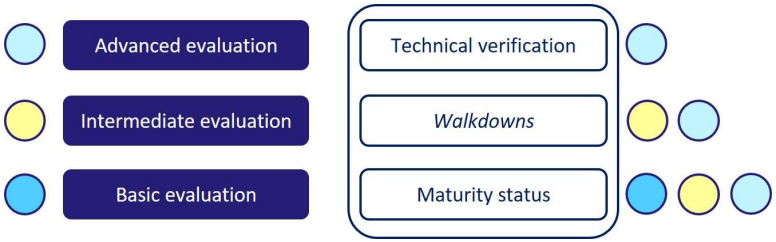
Portfolio of solutions for an industrial company



Consultancy







NIST

ISA

ISO 27001

NERC CIP

ens Esquema Nacional de Seguridad

What and Where?

Telefonica provides security teams with mixed experience in cybersecurity and industrial systems, which is aware of the specificities of applying cyber to OT networks and systems, to help you understand your risks and plan your cybersecurity controls roadmap.

Energy, manufacturing, retail, utilities, water management, food & beverage, chemical, pharmaceutical, building automation, railways, oil & gas, transportation, mining, automotive, healthcare sectors

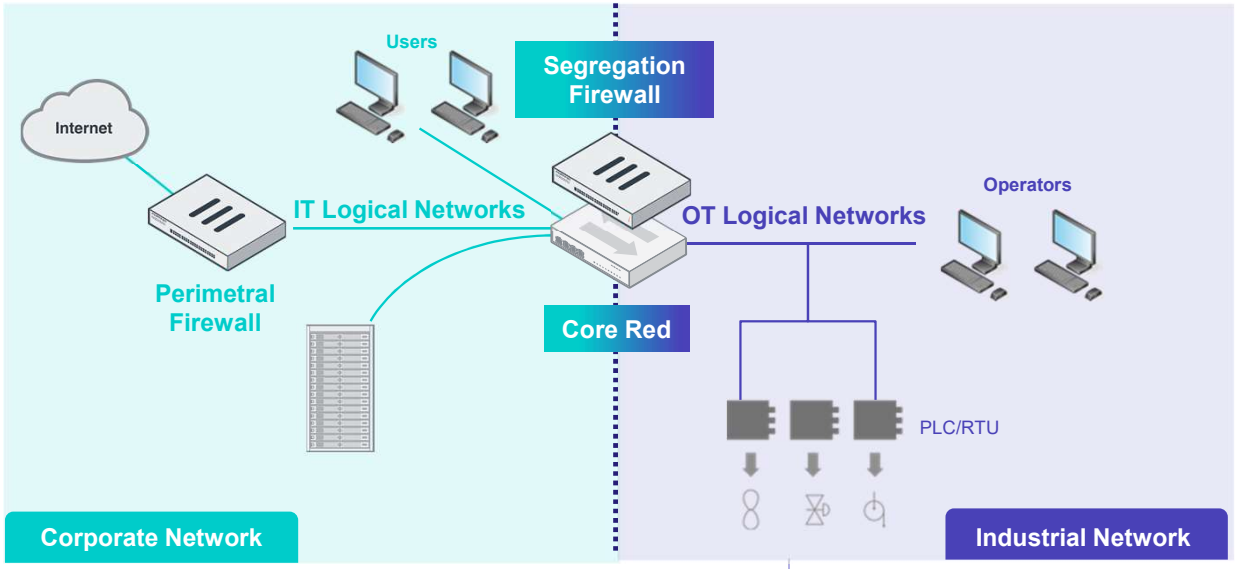
Features

A short few-days assessment based on network traffic analysis and remote interactions with key people and the ASPI_ technology.
Or a deep assessments with onsite work and exhaustive security risk posture as a result

Benefits

Assessment report that includes AS-IS situation (assets inventory, risks, security gaps, etc.) and mitigation measures to fill the gaps.
Get a real and accurate security posture
Get a realistic phased-plan & recommendations to improve your security posture

IT/OT Segregation



NGFW Policies

Isolated Environments

Visibilty

Access Control

What and Where?

The control networks have been growing in recent years, mixing with corporate networks, increasing their connectivity to increase business possibilities and respond to customer needs. With the disappearance of the mythical "air gap" between the networks, the exposure surface has increased exponentially for both networks and a logical separation is necessary to protect both limiting the exposure surface with a clear segregation between OT and IT networks.

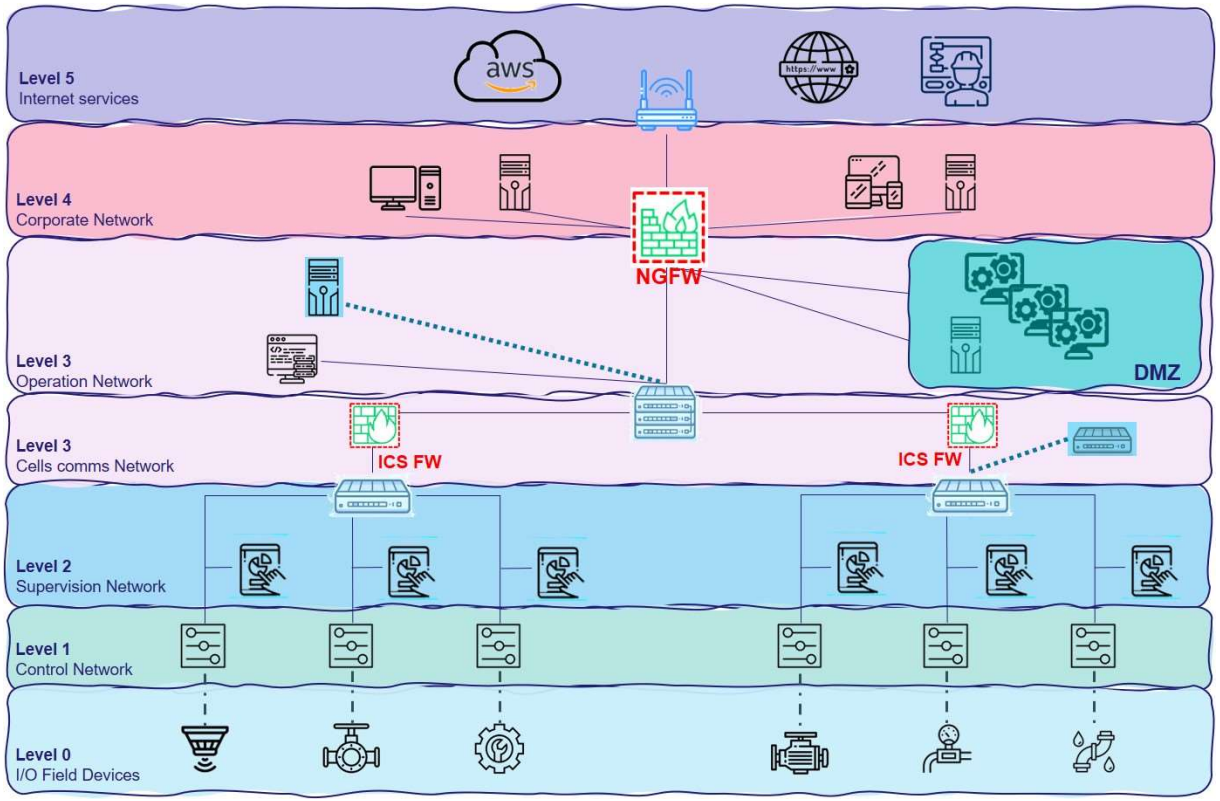
Features

Identifies applications inside network traffic
Protects to consolidate networking and security
Segregation also strengthens breach detection; any unauthorized access attempt is an indicator of a possible intrusion, blocking such attempts automatically alerting all affected applications to the presence of a threat

Benefits

NGFW Policies
Access Control
Visibility
Zone Isolation
SSL encrypted traffic
VM possibilities

OT Segmentation



What and Where?

To control networks more granularly, industrial processes and devices must be separated within the OT context following the best recommendations. The devices used to implement segmentation must withstand the harsh demands of industrial environments.

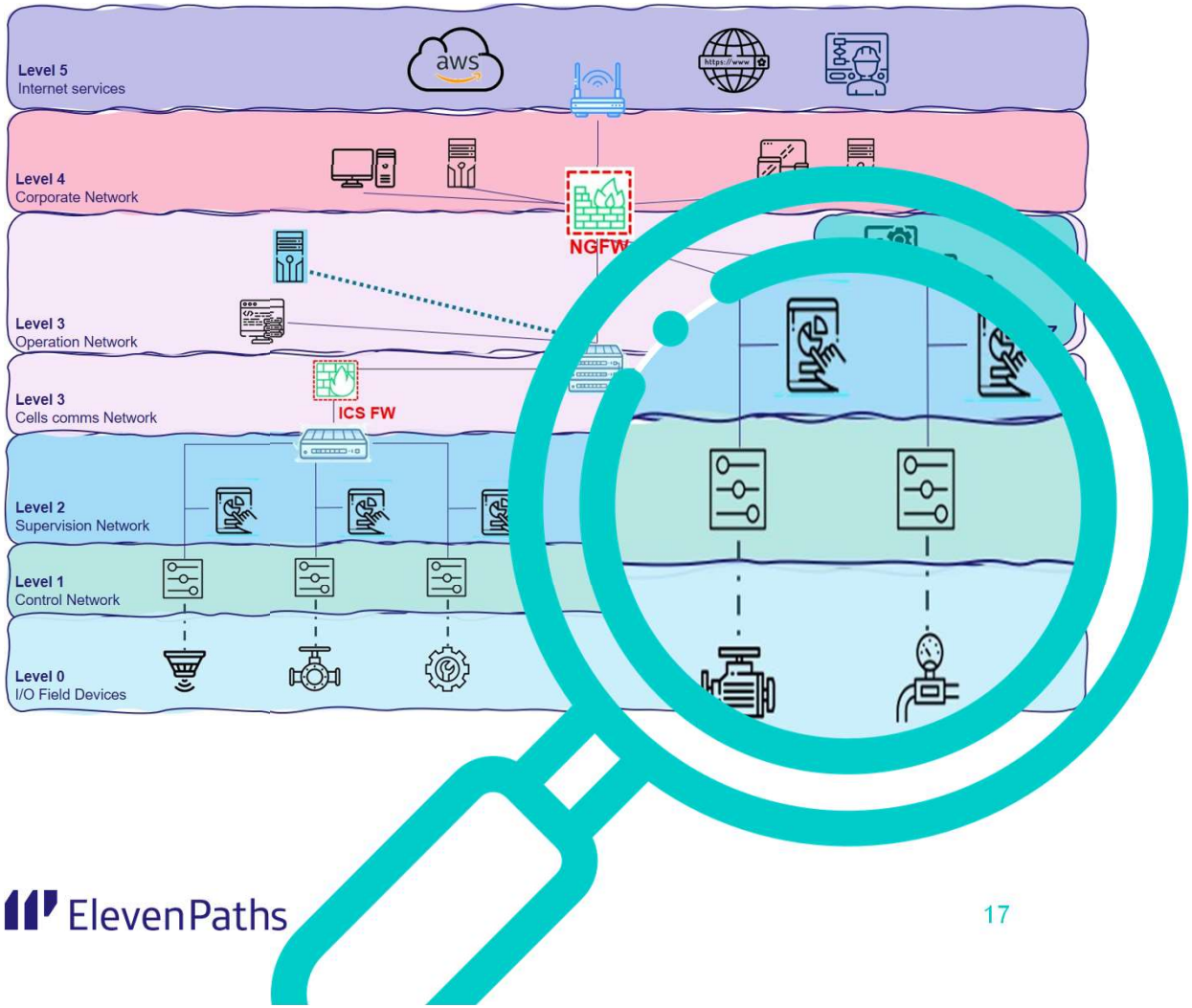
Features

Industrially-hardened, all-in-one security appliance
Ruggedized Design fanless and use of robust components
Ease of Management systems that allow rapid provision and deployment, monitoring of device and threat status while providing actionable reports

Benefits

Ruggedized equipment
Strong electromagnetic compatibility (EMC)
Efficient heat dissipation system and self warming
DIN mounting kit allowed
IP67
VM possibilities to use in high ruggedized embedded system

OT Security Monitoring



What and Where?

The networks convergence brings up a security challenge. The first of the challenges is to have a complete IT + OT/IoT context that allows knowing how to focus on security and what measures to establish. For this, it is necessary to identify, know how it communicates and how to classify the different assets in the networks. Only in this way, the most appropriate security measures can be considered. And thus, to detecting and to identifying the possible threats from the industrial environment.

Features

Get context from the customer´s network environment
Provide relevant results throughout the project
Get a first insight of the customer OT security posture, in this phase the contextualization is still pending
Present the results of the OT security posture contextualization

Benefits

Confidently Use Solution Designed Specifically for OT, IoT, IIoT & IoTM
Quickly Monitor ICS and other Networks and Processes with Real-time Insights
Readily Implement Custom Solutions with Flexible Architecture
Exceptional Forensics and Troubleshooting Services
Efficiently Act on OT and IoT Cybersecurity Threats and Risks
Behavior based anomaly detection, rules and signature-based detection and advanced correlation for detailed insights

ElevenPaths

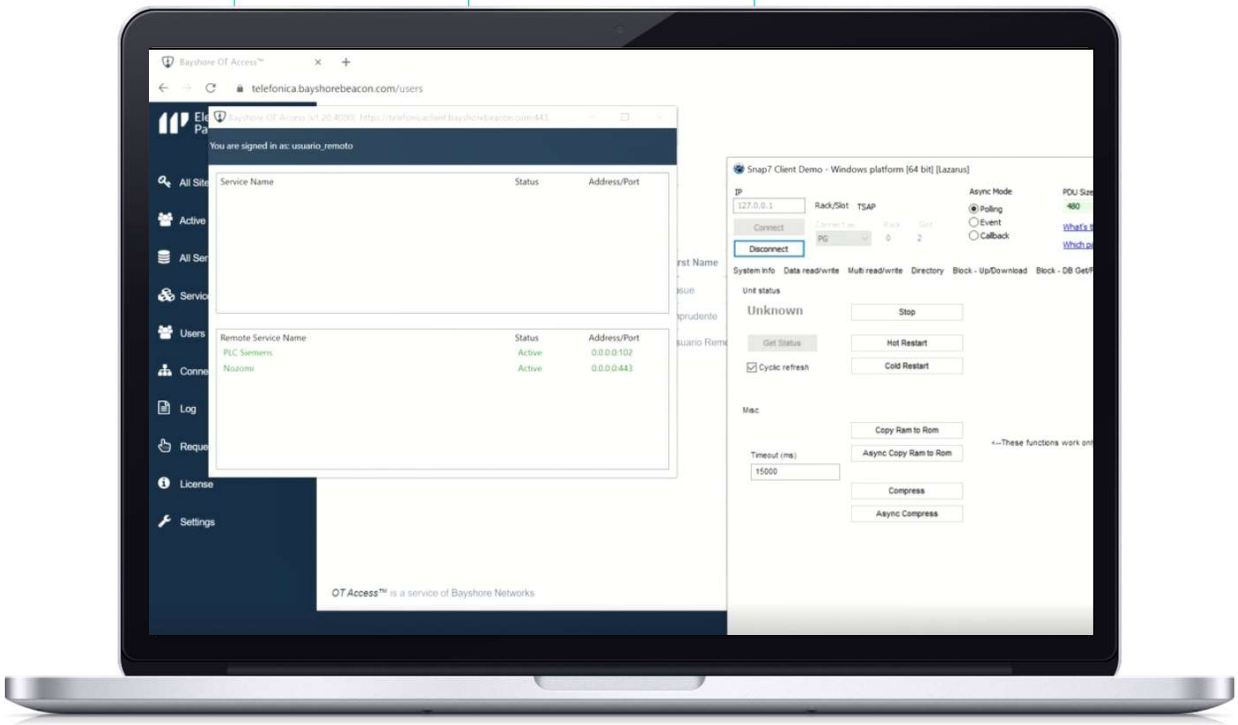
Telefónica CYBER SECURITY COMPANY

OT Remote Access

Industrial granularity

Remote access client

IP hiding, Straight to device



What and Where?

Connectivity with the outside world is fundamental to modern industrial Networks. Several activities such as remote maintenance, remote control and monitoring, or data acquisition depend on robust remote Access to the network. A secure remote access is mandatory

Features

Secure encrypted access
Centralized connection control and policies
Authentication mechanisms
Simplicity

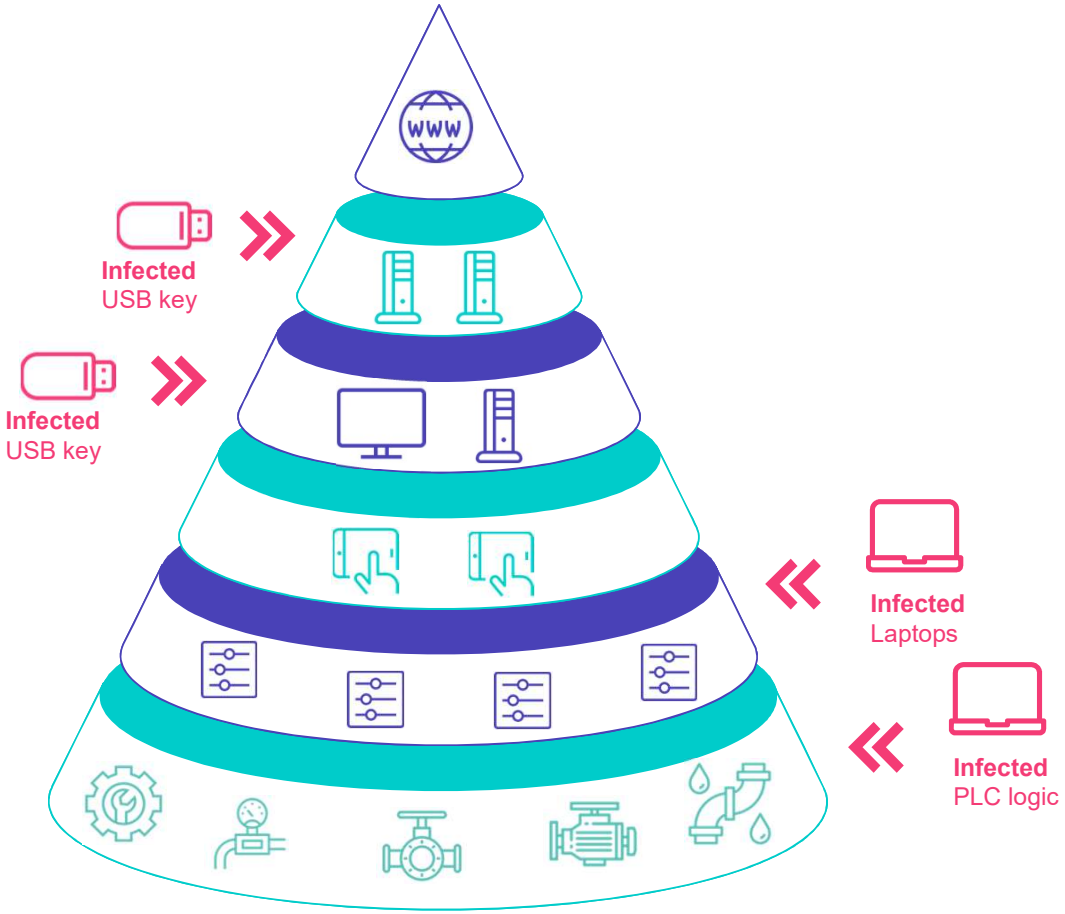
Benefits

Full control over devices and protocols access
Integrate with your existing identity platform
Extensive log generation for later auditory
Implement best security practices and architectures
Ease of use for remote users
Robust encryption
Reduce cybersecurity risks

ElevenPaths

Telefónica CYBER SECURITY COMPANY

USB Protection



What and Where?

One of the most common attack vectors comes from USB devices, Telefónica provides various solutions that respond to SW (virus), HW (keyboard simulators) and electrical (port protection) threats in various formats that adapt to the industrial environment.

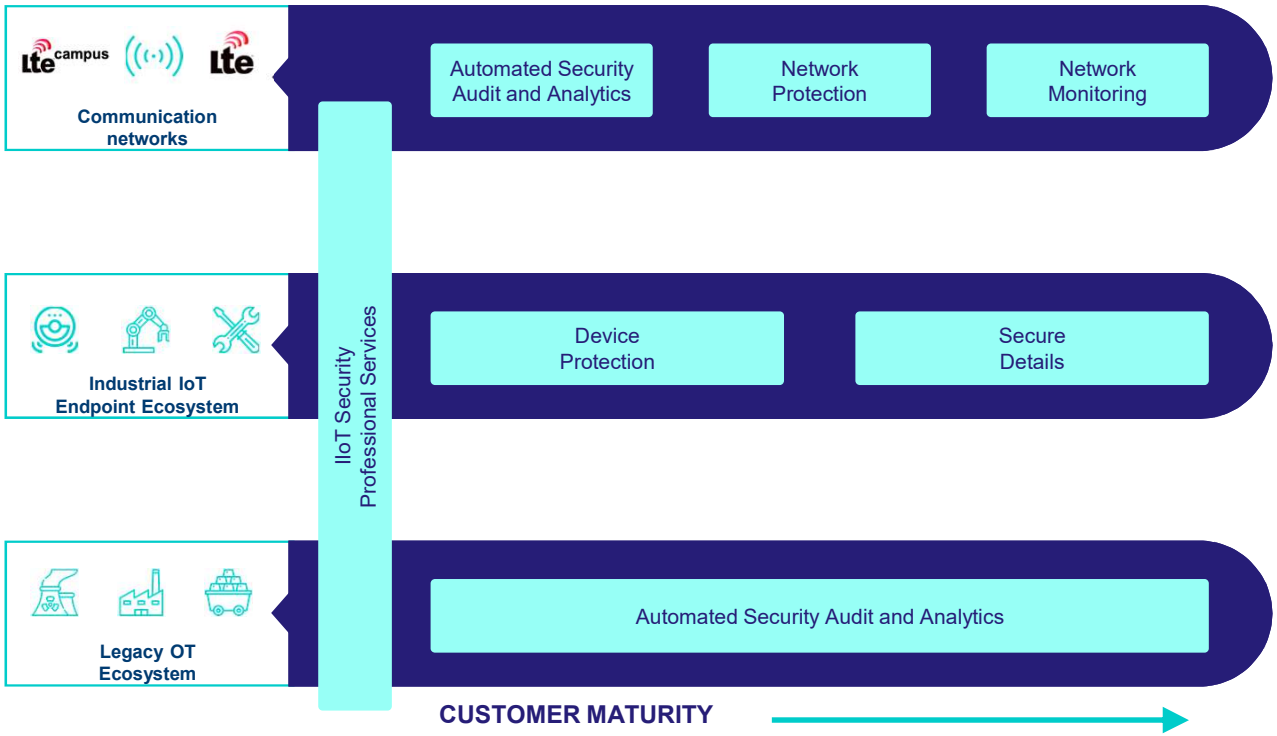
Features

Portable Security. To use a USB as an easy portable antivirus for entire environment
USB Sanitization. To neutralize and control de USB access to your environment against the SW threats.
Advance USB Sanitization. In addition to protect against the SW threats, it adds electric and HW protection for your environment.

Benefits

Centralized Management.
Easy Operation.
No Installation Required.
USB Scanning Station for secure information transfer with Rugged design and multiple anti-malware technologies
HW Protection against BadUSB
Electric protection against USBKiller

Secure Factory of the Future



What and Where?

Customers integrating such technologies often face the need of changing their networks and connectivity solutions to support new use cases. This solution is entitled to accompany the customer along this journey and help him identify, detect and mitigate the emerging threats that appear.

Features

Automated Security Audit
Network Protection
IIoT Monitoring over P-LTE

Benefits

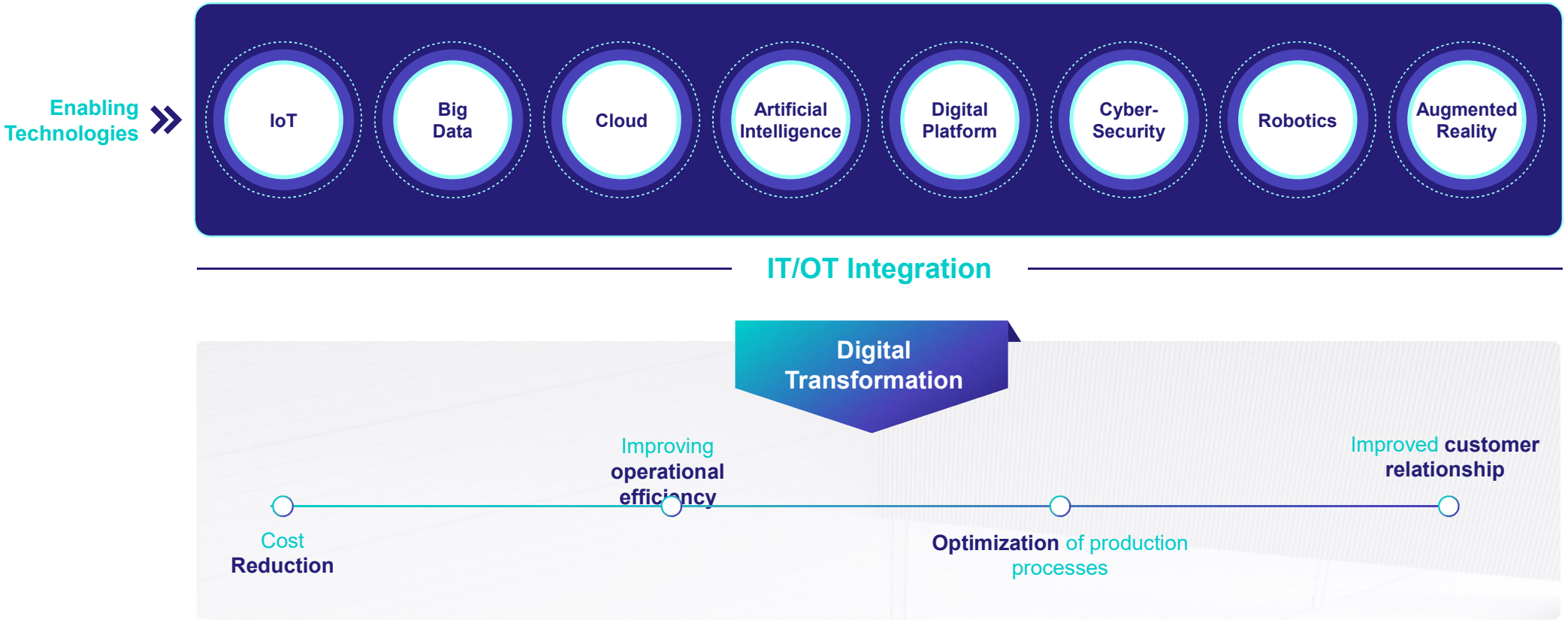
Ensure security compliance against recognized standards and identify possible emerging threats due to misconfiguration
Separate device traffic according to the device type and service
Analyze all device traffic to identify possible sources of threats and
Seamless integration with SOC teams

ElevenPaths

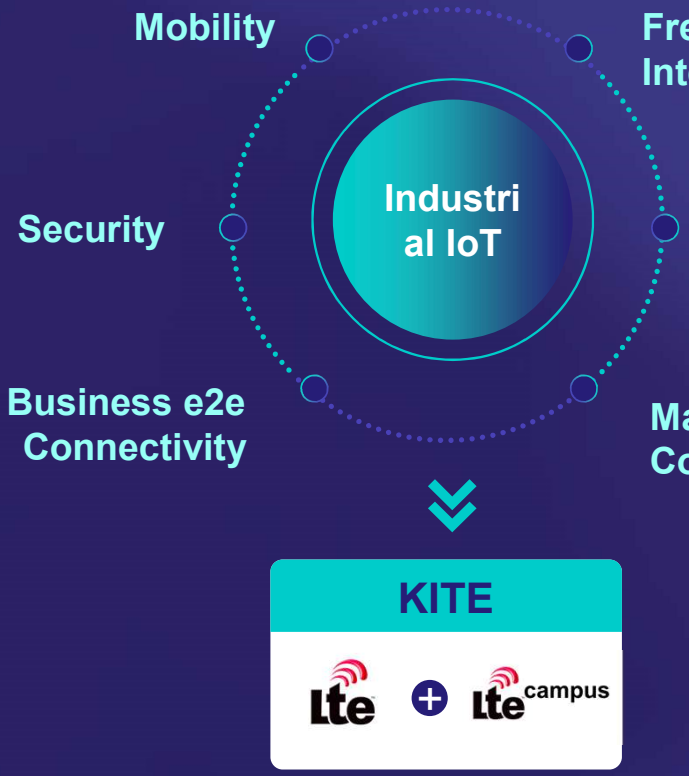
Telefónica CYBER SECURITY COMPANY

Secure Factory of the Future

Digital Transformation



Industrial IoT



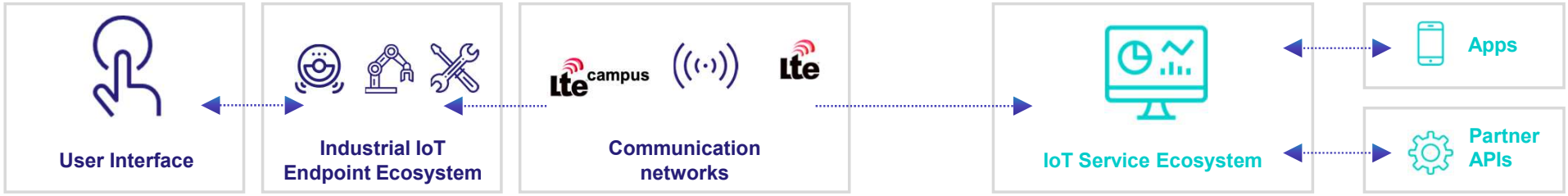
Current technologies

Digital Transformation

IoT specific security challenges
Must address the IoT scale and limitations

New IoT Protocols

Traditional IT security
Known field although requires doing properly



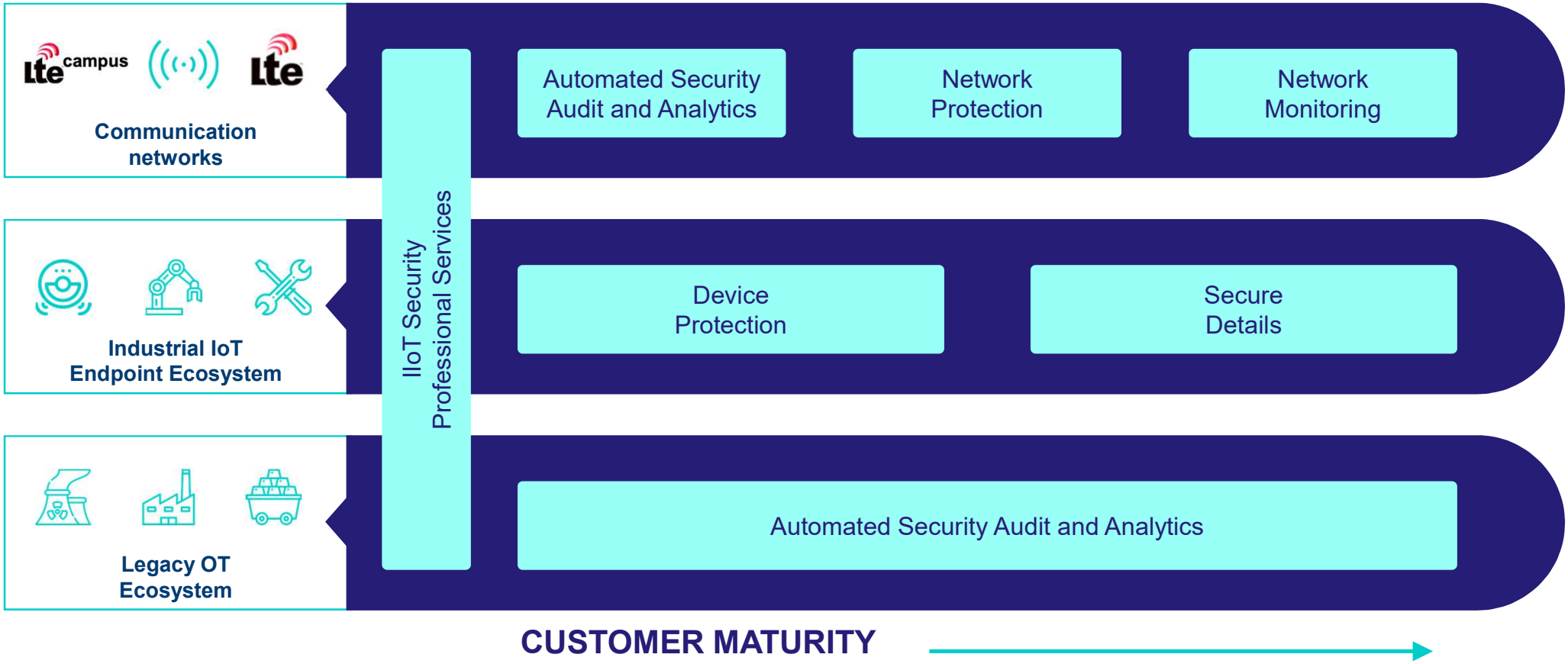
Secure connectivity with Value Added Services

Reinforce IIoT endpoints

Protect Legacy OT Ecosystem

Legacy OT Ecosystem
Physically isolated industrial domains are now exposed to the Internet

Value Proposition



Secure Factory of the Future

Secure Factory of the Future

Different enabling technologies, such as IoT, big data or augmented reality, are driving the digital transformation of industrial environments with the aim of reducing costs, improving operational efficiency, optimising production processes and enhancing customer relations.

Customers integrating such technologies often face the need of changing their networks and connectivity solutions to support new use cases. This solution is entitled to walk with the customer along this journey and help him identify, detect and mitigate the emerging threats that appear.

Target Segments

Companies that are transitioning towards the use of private networks based on LTE or 5G in a wide variety of industry sectors such as those of the energy, manufacturing, retail, utilities, water management, food & beverage, chemical, pharmaceutical, building automation, railways, oil & gas, transportation, mining, automotive, healthcare sectors.

Benefits

Ensure security compliance against recognized standards and identify possible emerging threats due to misconfiguration

Separate device traffic according to the device type and service

Analyze all device traffic to identify possible sources of threats and

Seamless integration with SOC teams

Features

Automated Security Audit: a security audit tool that periodically checks configuration compliance against recognized security frameworks and raises an alarm in case that a possible misconfiguration or change is detected

Network Protection: a combination of network security equipment that enables IIoT Service Segmentation, IIoT / IT Segregation.

IIoT Monitoring over P-LTE: a tool that profiles IIoT devices based on their network activity and defines targeted baselines per device type. Identifies risks related to device type and notifes in case that the device traffic patterns change

Service Offering

Industrial IoT Networks based on Private LTE are complex and personalized, and so its security architecuture. Telefónica works alongside its partners to provide the best fit for the customer's deployment

Secure Factory of the Future

Automated Security Audit and Analytics

Private LTE and 5G networks are key enabling technologies to address the new challenges that digital transformation bring to our customer's industrial environments. The most ambitious environments of this technology require complex hardware to be deployed within the premises of the Customer. Automated Security Audit and Analytics is a tool that periodically checks security configuration of on-premise deployed hardware against well recognized standards to ensure that this has not suffered from any accidental misconfiguration at any time.

Target Segments

Companies that make use of private LTE and 5G networks to deliver digital services in industrial sectors, such as manufacturing, mining, logistics and ports

Benefits

Ensure security compliance against recognized standards and identify possible emerging threats due to misconfiguration

Automate security management for private networks

End to end Security for complex use cases in private LTE and 5G networks

Features

Security audit: Tool that periodically checks configuration compliance against recognized security frameworks

Baseline automation: Automate on-demand system reconfiguration to meet security standard requirements

Anomaly: Realtime security event monitoring for instant intrusion **detection in all network assets**

Service Offering

Tailored solution only for the use cases 4 and 5 of Industrial IoT Networks based on private LTE or 5G

ElevenPaths

Telefónica CYBER SECURITY COMPANY

Secure Factory of the Future

Network Protection

Industrial IoT Networks interconnect a wide set of Industrial assets and services. To control the environment more granularly, the industrial processes and devices connectivity must be separated and protected within the IIoT context following the best recommendations. This is a tailored solution for Private LTE and 5G networks, the equipment of which is tightly integrated to the private network.

Target Segments

Companies that make use of private LTE and 5G networks to deliver digital services in industrial sectors, such as manufacturing, mining, logistics and ports

Benefits

Separate device traffic according to the device type and service

Analyze all device traffic to identify possible sources of threats and

Seamless integration with SOC teams

Features

IIoT/IT Segregation and IIoT Service segmentation to guarantee that each IoT device connects only where it must connect

Application level security with app control and IDS / IPS capabilities with special focus for Industrial Threat Intelligence

Tightly coupled to the Private LTE or 5G offerings

Service Offering

Tailored solution for each specific use case of Industrial IoT Networks based on private LTE or 5G

Secure Factory of the Future

Network Monitoring

Industrial IoT Networks interconnect a wide set of Industrial assets to IoT and IT services. This poses new security challenges. The first of the challenges is that customers need to be aware of all the devices that are using IIoT connectivity and to detect when anomalous and suspicious behavior takes place. Being able to identify suspicious changes in the communication patterns will help the customer in predicting potential malicious activity at an early stage

Target Segments

Companies that make use of private LTE and 5G networks to deliver digital services in industrial sectors, such as manufacturing, mining, logistics and ports

Benefits

Confidently Use Solution Designed Specifically for OT and IoT

Quickly Monitor ICS and other Networks and Processes with Real-time Insights

Easy Provide Exceptional Forensics and Troubleshooting Services

Rapidly Detect & Hunt Cyber Threats using a best-in-class solution

Behavior based anomaly detection

Rules and signature-based detection

Advanced correlation for detailed insights

Features

Device profiling and visibility: defining a communication baseline for connected devices brings visibilty to the IIoT end to end.

Threat detection: any slight change in the device profile is identified as an anomaly. Anomalies are often the precursor of malicious activity

Easy integration for mitigation: easy integraton with network equipment, as well as with event correlators and event triggers to provide automated response

Service Offering

Tailored solution for each specific use case of Industrial IoT Networks based on private LTE or 5G

ElevenPaths

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

Telefónica CYBER SECURITY COMPANY