telefonicatech.com

Telefónica Tech

CYBER SECURITY SERVICES AND SOLUTIONS DOSSIER

We support you on the journey to business *resiliencie*

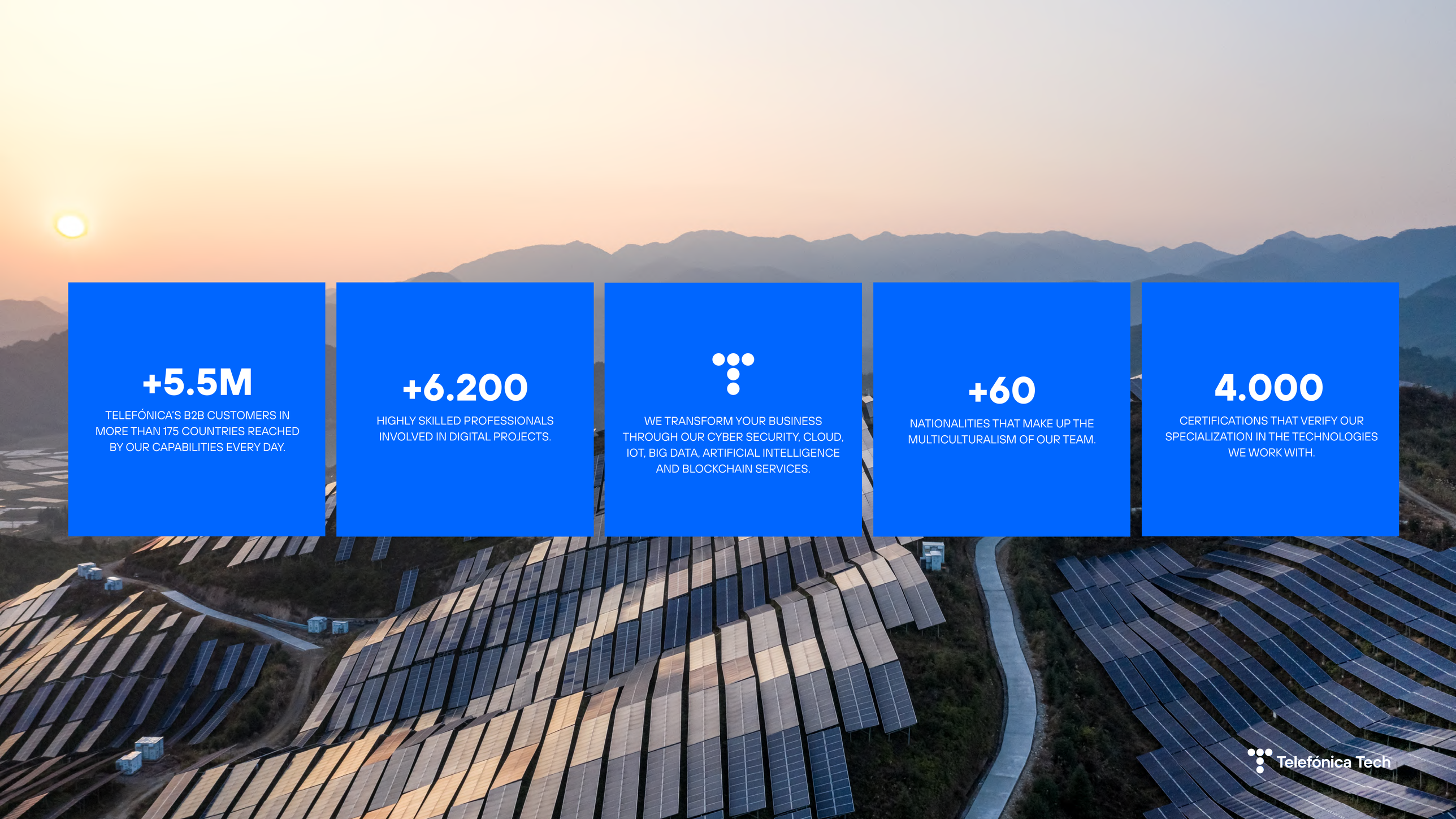
Telefónica Tech

A place called **Telefónica Tech**

Telefónica Tech, with a highly diversified team of more than **6,200 exceptionally skilled professionals from over 60 nationalities**, believes that technology can do great things: from extracting the full value of data to make the best business decisions, to ensuring the resilience of every organization to build a more sustainable future.

Telefónica Tech is a leading NextGen Tech solutions provider that has built a **differentiated customer** journey based on the migration from traditional Communications and IT services to NextGen IT solutions. **Our strong sustainable portfolio,** combined with high-value professional and managed services, enables Telefónica Tech to accompany our customers on their traditional journey of transformation of communications and IT, towards achieving fully cyber-secure and cloud-based communications and IT and optimizing their business processes thanks to Artificial Intelligence and IoT Solutions.

TELEFONICATECH.COM



+5.5M

TELEFÓNICA'S B2B CUSTOMERS IN MORE THAN 175 COUNTRIES REACHED BY OUR CAPABILITIES EVERY DAY.

+6.200

HIGHLY SKILLED PROFESSIONALS INVOLVED IN DIGITAL PROJECTS.

WE TRANSFORM YOUR BUSINESS THROUGH OUR CYBER SECURITY, CLOUD, IOT, BIG DATA, ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN SERVICES.

+60

NATIONALITIES THAT MAKE UP THE MULTICULTURALISM OF OUR TEAM.

4.000

CERTIFICATIONS THAT VERIFY OUR SPECIALIZATION IN THE TECHNOLOGIES WE WORK WITH.

Telefónica Tech

Who is Telefónica Tech in cyber security?

A global provider of managed security services with a comprehensive portfolio of cyber security capabilities.

15
YEARS
OF CYBER SECURITY PRACTICE

~2.000
EXPERTS
CYBER SECURITY EXPERTS GLOBALLY

~1.700
CUSTORMERS
CYBER SECURITY CUSTOMERS GLOBALLY

>50
TECHNOLOGIES
AND MORE THAN 30 MANAGED CYBER SECURITY SERVICES

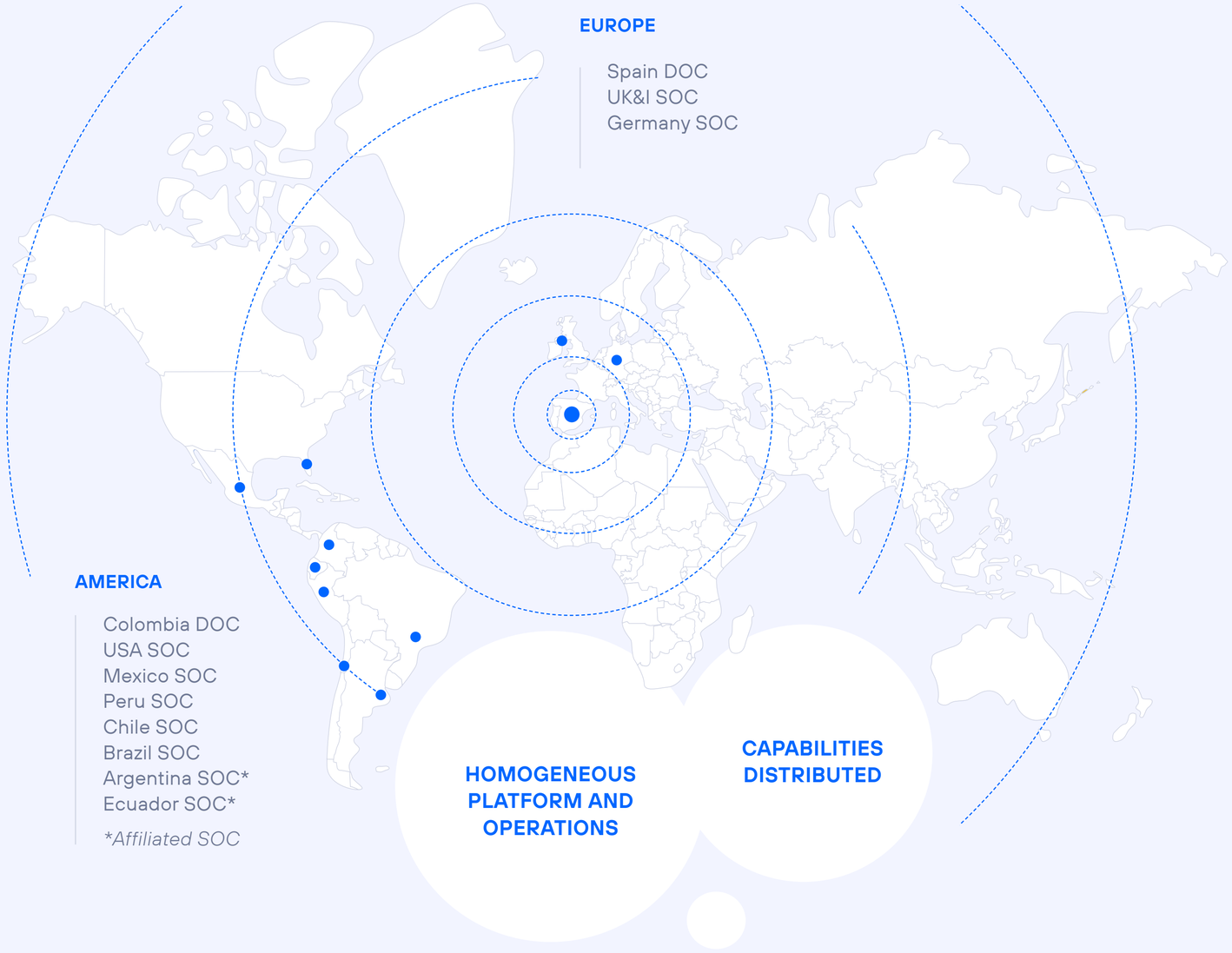
- **350k** TICKETS MANAGED PER YEAR
- **>6k** CUSTOMER SECURITY REPORTS
- **500k** ALERTS MANAGED PER YEAR
- **>10k** FRAUDULENT SITES CLOSED PER YEAR
- **15k** MANAGED SECURITY DEVICES
- **114** INTEGRATED CYBER INTELLIGENCE FEEDS
- **600** SECURITY MIGRATIONS PER YEAR
- **20M** IOC AND ROTATING ASSESSMENTS ON OUR DATA
- **120k** DIGITAL CUSTOMER NOTIFICATIONS

Telefónica Tech

One Digital Operations Center (DOC) with two geographic locations and 11 SOCs and 11 SOCs worldwide

Developing the best end-to-end capabilities in cyber security and cloud operations.

- GLOBAL **SCOPE** AND LOCALPRESENCE
- **24/7/365** ALWAYS-ON SECURITY PROFESSIONALS
- **MULTIDISCIPLINARY** TEAM
- SYNERGIES FOR A BETTER **CUSTOMER EXPERIENCE**
- THE BEST **PLATFORMS AND INFRASTRUCTURE**
- **INTEGRATED VISION** WITH A SINGLE POINT OF CONTACT



Telefónica Tech

NextDefense | Core cyber security services

EXTENDED DETECTION & RESPONSE	• Managed Detection & Response • SIEM Management	• Digital Forensics & Incident Response • Cloud Security
NEXTDEFENSE PLATFORM	• Platform • Security Analytics	• Security Assessment & Automation
CYBER THREAT INTELLIGENCE	• Digital Risk Protection • Threat Intelligence	• Third-Party Risks
VULNERABILITY RISK MANAGEMENT	• Vulnerability Scanning • Pentesting & Security Assessment	• Red Team Assessment
NETWORK SECURITY	• Security Edge • Secure Internet Access • Security Device Management • Clean Email	• DDoS Protection • Secure Internet Access Branch • Secure Internet Access Essentials • Web Application Defense
MISSION CRITICAL SOC	• OT Security • Industrial perimeter Protection	• Industrial Cyber Security Assessment • OT&IoT Security Monitoring
SECURE MICROSOFT	• Secure Microsoft 365	
DATA & IDENTITY PROTECTION	• Information Rights Management • Digital Certificates • Access & Authentication	• Electronic and Biometric Signature • Priviledge Access Management

FlexSuite | Cloud and secure connectivity

SASE	• SASE
SD-WAN	• FlexWAN
SD-LAN CLOUD WIFI	• FlexSITE
SD-BRANCH	• Secure SD-Branch

Your 360° digitalization | Service for SMEs

YOUR DIGITAL BUSINESS	• Your Secure Enterprise • Secure Business Connection

Consulting and Professional Services | Tailor-made services

CONSULTING AND PROFESSIONAL SERVICES	• Cyber Security Consulting • Cyber Security Professional Services

Navigation Menu (Portfolio Index).

Telefónica Tech

NextDefense

Core cyber security services

We make your journey to the cloud secure and help you develop a cyber-resilient business with our NextDefense Cyber Security solutions.

Telefónica Tech

Managed Detection & Response

MORE INFORMATION

Our Managed Detection and Response (MDR) helps modern organizations stay secure and respond to advanced threats.

ABOUT THE SERVICE

This service aims to help security teams **accelerate the deployment of advanced and mature detection and response capabilities** by reducing the time it takes to deploy detection and response capabilities by eliminating the complex processes of purchasing, operating, and maintaining a 24-hour security toolset.

We have the **best market-leading technologies, security experts and automated processes** to ensure complete protection.

WHAT DOES IT ALLOW?

- Adopt the **best Endpoint Detection and Response (EDR) technology managed by teams of analysts who have been in a large number of incidents.**
- Increase your own **security capacity, reduce mean response time, and anticipate threats.**
- **Gain an effective**, fast, and comprehensive response capability to cyber breaches including DFIR capabilities (optional).

BENEFITS

Delivery, deployment, configuration, and support
Our team is responsible for the delivery and configuration of EDR technology, providing personalized guidance and implementation support.

24/7 monitoring and response
Including triage, analysis, contextualization and validation of threat alerts, plus remote containment and escalation of confirmed security breaches enriched with our intelligence platform.

Proactive Threat Hunting
Our threat hunters leverage threat intelligence to conduct proactive searches for undetected TTP-based threats that have evaded security systems.

Expanded response capability
Early detection and blocking of critical threats, automatic mitigations and DFIR capability (optional) for a comprehensive response.

SIEM Management

MORE INFORMATION

Our managed SIEM solution enables continuous threat monitoring and detection across your organization.

ABOUT THE SERVICE

This service aims to expand **detection and response capabilities** through continuous monitoring and correlation of events, logs and alerts in the customer's IT environment, providing **visibility of the security status, as well as support to the security teams in case of any threat detected** or need for security monitoring evolution. and support to the security teams in case of any detected threat or monitoring evolution needs.

The goal is to provide a **service with high automation in the detection of security anomalies and cyber threats**, eliminating the need to have a team and / or SIEM technology itself, obtaining orchestration capabilities and response "As A Service".

WHAT DOES IT ALLOW?

- Adopt the **latest generation** SIEM technology from the most relevant partners in the market.
- **Expand security capacity** over all technological environments (on-premises and cloud) obtaining a global monitoring vision and reducing security risks.
- **Increase detection capabilities and response times** efficiently and continuously through 24/7 expert analyst teams and enriched intelligence.

BENEFITS

End-to-end management
Our teams are responsible for SIEM delivery, configuration, deployment and installation, providing guidance and support throughout the process to the customer's IT teams.

24/7 monitoring and detection
Including triage, analysis and discarding of false positives, as well as remote escalation of any confirmed threats under orchestrated procedures.

Threat Search
Our analysts leverage the latest information from TTPs, vulnerabilities and IoCs to search for threats that have gone undetected.

Detection and customization
Extensive correlation and aggregation catalog with implementation tailored to customer assets and processes, supported by experts who maintain an up-to-date environment with customized information.

Digital Forensics & Incident Response

MORE INFORMATION

Digital forensics and incident response service helps organizations respond effectively to cyber incidents.

ABOUT THE SERVICE

Building a skilled and experienced incident response team is a challenge for even the most mature organizations. **Telefónica Tech incorporates this capability through the Digital Forensics and Incident Response** (DFIR) service.

Our main objective is to **provide help, support and guidance** to IT and security teams on **security breaches, with capabilities designed to address threats** such as: ransomware, email compromise, denials of service, data leaks, insider attackers or APTs.

WHAT DOES IT ALLOW?

- **Ensure coordination, containment, investigation, and mitigation after a security incident** with the support of an expert team based on a solid methodology.
- **Enhance your cybers ecurity** through advanced malware analysis and forensic capabilities.
- **Obtain a fast, effective, and comprehensive respons**e to cyber-crisis to reduce response and recovery times.

BENEFITS

End-to-end support and back-up
Full response during and after the incident, providing close guidance on actions to be taken.

Dedicated Incident Manager
Provides end-to-end support and coordination to your teams throughout the entire incident lifecycle.

Threat Intelligence Based
We adopt a multi-source intelligence-driven approach for effective investigation responses, validating compromise alerts and serving as the basis for in-depth threat searches.

Elite team
Specialized team composed of forensic and malware analysts, threat hunters, incident managers, network experts, threat intelligence analysts and legal specialists.

Cloud Security – Cloud MSS

MORE INFORMATION

Our goal is to help your security areas take back control of their security in the cloud, introducing and integrating it into the design and operation processes as a transversal component of all of them.

ABOUT THE SERVICE

Our **Cloud Security solution is designed to identify, assess, and manage the challenges and threats of the cloud** thanks to a set of capabilities that support your business, helping you to adopt the cloud with confidence.

Telefónica Tech's Cloud MSS service focuses on comprehensive **public and private** cloud security, both in terms of **governance** and **protection, throughout the lifecycle** of the cloud infrastructure and applications.

WHAT DOES IT ALLOW?

- Having **visibility and governance of the assets deployed in the cloud** independently of the CSP (Cloud Solution Provider).
- Continuous **assessment and compliance** of the cloud infrastructure according to different regulatory frameworks and best practices.
- **Protection** of workloads throughout their lifecycle and **threat detection.**
- **Identity** management in the cloud.
- Implementation of **security policies customized** to the customer's environment.
- **Service delivery** based on dashboards and **KPIs**, which allow the customer to have a vision of security and monitor it, in order to have a continuous improvement.

BENEFITS

Regulatory compliance
Regulatory (GDPR) and standards (PCI-DSS) compliance support.

Protection and detection
Implementation of workload protection measures for any cloud environment and detection of threats and attacks. Including **24/7** for critical alerts.

Bastioning
Bastioning of cloud assets based on Telefónica Tech's recommendations and best practices.

CI/CD pipeline integration
CODE and CI/CD securitization.

Expertise
Our specialized groups of DOCs and SOCs bring together cloud and security expertise and best-of-breed cloud-native security platforms (CNAPP).

Reporting and KPI tracking
Dynamic deliverables and KPIs to ensure continuous security insight and improvement.

Platform

Our NextDefense Platform is the enabler that orchestrates technology, processes and people so that all our managed services are integrated and kept up to date based on industry best practices allowing the customers a comprehensive protection of their business.

ABOUT THE SERVICE

The digitalization of all business processes has brought with it new cyber security risks arising from the high integration between systems and networks managed from cloud environments. A siloed view of the different security domains is therefore no longer enough to protect the business. A breach in any of these domains can be exploited by cybercriminals and spread to any critical system.

Our managed services have been integrated into our NextDefense platform to provide our customers with an end-to-end view of their security status, rapid response to attacks and continuous improvement.

The platform allows customers to access a service management portal with a single view of the status of their services, security analytics and threat intelligence dashboards, and to communicate in an agile way with Telefónica Tech, among other functionalities.

WHAT DOES IT ALLOW?

LThe NextDefense platform brings together end-to-end capabilities that enable a customer's CISO or cyber security manager to:

1. Holistically **measure** your **security posture.**
2. **Maximize their breach response** and reduce response time.
3. **Understand and prioritize your initiatives** based on the real impact on your company's security.
4. Manage your relationship with Telefónica Tech and **use our managed services in an agile way**.

Customers can use the platform through our service management portal. The platform also allows customization of all dashboards and reports.

BENEFITS

Telefónica Tech's managed services management in one place unified
View of all relevant KPIs for each service and a one-stop shop for incident, change, and document management.

Integration with our customers' processes and channels
From opening incidents in their Teams channels or via Whatsapp, to integration with their ITSM systems or tools via API.

End-to-end visibility of the state of cyber security
Enables a holistic understanding of our customers' security posture, taking into account all their critical services and assets.

Integrated security intelligence
The platform integrates our Threat Intelligence Platform so that threats are communicated to the customer and all our services constantly evolve based on new threats.

Security Analytics

Managed service that transforms the data generated by the customer's cyber security solutions into useful information for governance and decision making, security posture improvement and operation (detection and response).

ABOUT THE SERVICE

Exploiting the data generated by the multiple security solutions that make up the customer's security architecture is critical to the protection of the enterprise's and for the continuous improvement of the security posture and operation.

The Security Analytics service helps customers manage the lifecycle of their security data and build dashboards with relevant information tailored to each user involved in the company's security, CISOs, SOC Managers and Analysts and to each use case. In addition, it includes advisory services provided by our experts to extract the maximum value from the service.

WHAT DOES IT ALLOW?

- **Expert advice from Telefónica Tech** based on industry best practices to prioritize the analytics use cases that best fit the customer's objectives and baseline situation.
- **Integration, normalization, and storage of multiple data sources,** both proprietary, external or Telefónica Tech's, and development of dashboards with the use cases chosen by the customer.
- **Flexible deployment model** both in the customer's on-premises or cloud infrastructure or in Telefónica Tech's cloud.
- After the implementation of the dashboards, the service includes the **periodic review of the security metrics** by one of our expert Security Managers. After each review, the Security Manager generates a **detailed report** on the status of the KPIs with recommendations for improvement.

BENEFITS

Increased Return on Investment (ROI) in security
Measuring both the risks and the effect of improvement initiatives helps CISOs and other security managers justify the business case for cyber security, justify new investments, and invest in the projects that have the greatest impact

Improved security posture
End-to-end visibility of the security measures and policies that protect all company assets and their evaluation based on industry best practices, allow to know the real protection of the company and the level of risk to define improvement plans.

Improving the quality of security operations
The capacity of the analytics solution to visualize in real time all security events in a consolidated manner and classify them, allows the SOC teams to focus on those of greater severity and subsequently execute forensic exercises to improve the response to similar events.

Personalized attention
Our technical and commercial team provides a personalized experience from commercial advice and selection of the use cases that best suit each scenario, to technical support in case of changes or incidents.

Security Assessment & Automation

Detection and Response process automation service based on a catalog of multi-technology automations and in continuous evolution complemented with professional services to adapt the automations to the specific needs of each customer.

ABOUT THE SERVICE

The number of cyberattacks and their complexity is growing exponentially. In this situation, the SOCs of the companies must place the automation of the Detection and Response processes at the center of their activity.

Otherwise, they will not be able to effectively address threats resulting in increased risk and potential business impact.

Developing automation, however, is a costly process that requires extensive knowledge of multiple technologies, industry processes and best practices, and a high degree of customization. This poses a barrier to entry for many companies.

We launched "Security Assessment & Automation" to democratize the automation of Detection and Response processes, a service that offers an approach by offering a catalog of automations in continuous development and a package of professional services. All this is delivered in an aaS consumption model.

WHAT DOES IT ALLOW?

- The Security Assessment & Automation service provides our customers with a **complete catalog of Detection and Response** playbooks for the main technologies on the market and their use cases, under a subscription model.
- Subscribed customers gain access to a **growing catalog of generic automation that they can use to protect their critical business assets**, either on a standalone basis or by delegating their integration and implementation to Telefónica Tech.
- The service offering includes the **maintenance of existing playbooks, and the addition of playbooks created both for global security breaches and for other Telefónica Tech customers.**
- In addition, included in the service is the **initial assessment of the customer's security posture and risks** to align the automation roadmap with their business need.

BENEFITS

Based on industry best practices
Our customers have access to a catalog that brings together the best practices that Telefónica Tech recommends based on its expert knowledge and in its daily operations with other customers.

Keeping security up to date
The service approach allows our customers to focus on their business, while Telefónica Tech takes care of the maintenance and creation of new automation for each security breach that may arise.

Lower cost of automation
Accessible to any company, regardless of its ability to maintain the costs and resources involved in the creation and maintenance of playbooks and automation.

Facilitate the onboarding of playbooks in production.
The service includes professional adaptation and integration services with our customers' tools, as well as a playbook catalog for all the main tools and technologies in the sector.

Digital Risk Protection

MORE INFORMATION

We monitor and protect your brand, reputation and business against threats directed against your organization on the public web, as well as the deep and dark web.

ABOUT THE SERVICE

This service helps customers to be aware of their exposure in the digital world and to **identify threats and risks associated to their reputation and brand, business continuity and online fraud**, based on real evidence (Threat Intelligence).

We monitor the open web, deep web, and dark web, as well as specialized feeds, looking for references to your organization's assets to detect elements that can negatively affect your business. **We analyze the mentions** and add recommendations to help control your digital risks. Finally, **we implement the necessary measures** to curb fraudulent activity, eliminating the associated risk.

WHAT DOES IT ALLOW?

- **Track activities** that may damage your company's reputation or brand image.
- **Detect threats** that target business processes in an attempt to stop your normal activity.
- **Track activities that are likely to result in fraudulent action** against your company's interests.
- **Have a complete and up-to-date view of the risks** facing your entire mobile channel.
- **Shut down resources used to commit fraud against your company or your customers** and impersonate their identity and remove unauthorized content.

BENEFITS

Updated awareness status
We help you gain knowledge of your digital footprint and help the organization understand the business impact of the digital risks to which your company is exposed.

Prevent successful attacks
We report on exposed assets (shadow IT, public leaks, hacktivism...) that help to decrease successful attacks by reducing the attack surface.

Cost reduction
Early identification and prevention of potential attacks contributes to the reduction of costs associated with the potential financial and reputational impact.

Focus on what matters
We detect elements that may negatively affect your business, analyze and contextualize them, reducing noise and reporting only what may pose a threat.

Threat Intelligence

We transform information into intelligence at different levels (tactical, operational and strategic) to help you take a proactive stance against threats.

ABOUT THE SERVICE

Our holistic approach allows us to provide **intelligence tailored to different profiles within the same organization.**

This intelligence answers the lowest level details of specific attacks (IoCs), the details of campaigns and actors (TTPs) and the highest-level details of attack trends and the threat landscape. In addition, shared with the various functional teams established within the organization, it has the potential to help identify, communicate, and reduce risk across the organization identify, communicate, and reduce risk across the organization.

WHAT DOES IT ALLOW?

- **Tactical intelligence:** ensure preparedness and implementation of security controls and processes.
- **Operational intelligence:** better understand the threat landscape and defend the organization against specific threats.
- **Strategic intelligence:** allocate the necessary resources to mitigate risks and defend the organization against generic threats.

BENEFITS

Prevention
Allows to increase the number of preventive blocks and the number and impact of patched vulnerabilities.

Detection
Increases the number of detections and positive alerts, also reducing false positives, while the context allows reducing the time spent on each alert.

Response
Reduces mean time to detection (MTTD), facilitating the discovery of a greater number of incidents, and mean time to remediation (MTTR).

CYBER THREAT INTELLIGENCE

It helps you understand digital risks, providing you with a strategic advantage for better identification and anticipation against threats.

Third-Party Risks

MORE INFORMATION

Identify, quantify, and reduce your security risks with the only security ratings solution with proven correlation to business results.

ABOUT THE SERVICE

Organizations are often unaware of their own organization's actual security performance, let alone that of their vendors and partners.

This is due to a **lack of objective statistics and tools** that help measure and mitigate dynamic risk across their business ecosystem.

With this in mind, we have partnered with BitSight to offer the **Third-Party Risks service, to help you gain standardized visibility into the risks present across your entire ecosystem,** prioritizing your investments and actions in the most critical areas that generate the greatest measurable impact over time.

WHAT DOES IT ALLOW?

- **Continuously monitor and benchmark your organization**, either internally or with third parties, through Security Performance Management.
- Expose your risk within the supply chain thanks to Third-Party Risks, helping you to focus your resources on working together with your suppliers to achieve **significant and measurable risk reduction.**

BENEFITS

Security Benchmarking
Measure the impact of security processes and tools, calculating the ROI of your cyber security budget and benchmarking your performance against your industry and specific competitors.

Risk reduction
Reduce exposure to data leaks by making security decisions quickly and effectively.

Objective communication
Facilitate data-driven conversations about cyber security with any of your organization's stakeholders.

Vulnerability Scanning

MORE INFORMATION

Go beyond traditional scanning with risk-based remediation.

ABOUT THE SERVICE

This service addresses the challenge of the increasing number of **new vulnerabilities emerging every day in network devices, servers, and web applications.**

By continuously monitoring and automatically analyzing the security of your network infrastructure and web applications to provide a **global view of your organization's weaknesses,** helping to identify vulnerabilities in your network, servers, and web applications. your organization, helping to identify vulnerabilities in your assets and enabling **prioritized management of their remediation.**

A customer-facing portal and our DOCs and SOCs complete the value proposition of the service.

WHAT DOES IT ALLOW?

- **End-to-end vulnerability management** through an Online Portal that allows tracking of a vulnerability from detection to resolution.
- Provide a **trusted communication channel** through the role of a local analyst who understands the customer's needs and requirements.
- Having a t**eam of experts** who review the results obtained by the tools to **determine their severity and support the customer in defining a remediation plan.**

BENEFITS

Complete and continuously updated coverage
Our scanning technology provides visibility into assets beyond a company's control and implements the latest attack techniques with continuous analysis of IT network infrastructure and web applications. This reduces exposure time to security breaches and provides real-time risk awareness across the entire attack surface.

All your vulnerabilities in a single point
Our Online Portal provides a single point for vulnerability management based on security standards. Our platform includes dashboards with detailed metrics, technical recommendations, and remediation projects for effective prioritization.

Time and cost savings
associated with vulnerability prioritization and remediation processes.

Pentesting & Security Assessment

MORE INFORMATION

We help you discover vulnerabilities that an attacker could exploit to gain access to your environment and systems.

ABOUT THE SERVICE

We provide an independent and objective assessment of infrastructure, software and employee security, clearly highlighting the **security risk to corporate and customer data** from both external and internal vulnerabilities.

Only by emulating real-life threat actors, such as disgruntled employees, external hackers and cyberattackers, can the **true technical risks inherent in IT systems** be identified and then inherent in IT systems and then **facilitate the identification of the necessary mitigating controls to be implemented.**

WHAT DOES IT ALLOW?

- **Actionable information and reporting:** we improve the security posture of customers by identifying potential risk areas that need to be remediated.
- **Post-testing support:** we advise on the remediation process and support decision making. We certify vulnerability remediation to verify risk elimination.

BENEFITS

Comprehensive and independent assessment
We provide an independent and objective security assessment of your infrastructure, software, and employees, clearly highlighting the security risks associated with internal and external vulnerabilities.

Vulnerability prioritization
We help discover critical vulnerabilities, understand their risk and prioritize based on their exploitability and impact. This service enables compliance with regulations and industry standards and keeps executive management informed about the overall risk level of the organization.

Time and Cost Savings
Reduces system downtime and saves remediation costs.

Ensures compliance
We help you comply with security regulations and preserve your company's reputation.

Red Team Assessment

MORE INFORMATION

We run attack simulations with real scenarios adapted to the reality of your business, allowing you to validate your resilience, train and evolve your defenses.

ABOUT THE SERVICE

Our **Red Team** service is designed to **test and continuously improve the effectiveness and detection and response capability of companies' information security defenses** by simulating attack scenarios using the Techniques, Tactics and Procedures (TTPs) of real adversaries.

We provide companies with an **independent assessment that provides a deep dive into the risks and vulnerabilities** of the enterprise and serves as a benchmark against which to measure future security improvements.

WHAT DOES IT ALLOW?

- Have a comprehensive, independent assessment of your security **strengths and weaknesses.**
- Get clear and concise guidance on **how to protect your information** from today's sophisticated attacks.
- Increase your level of **protection and expertise against new generation threats** and unknown vulnerabilities without real risk.

BENEFITS

See the real impact of a targeted attack
Understand the real consequences of a targeted attack and justify the allocation of security resources and whether they are being used effectively to mitigate and prevent threats.

A complete analysis of your security strengths and weaknesses
Receive the essential distilled information your business needs and convey it in a way that is valuable to both non-technical executives and the technical security team.

Gain persistent expertise
In the face of next-generation threats and unknown vulnerabilities with no real risk. Increase your security team's awareness, motivation, and readiness, as defenses are constantly tested and adapted to the evolving environment.

Security Edge

MORE INFORMATION

We provide secure access, from any place and device, to websites, SaaS applications and private applications deployed in CPD or IaaS environment.

ABOUT THE SERVICE

It is a **network security service** managed by Telefónica Tech's DOCs and SOCs. **The service platform is deployed in the cloud, on an extensive network of nodes that adapts to the customer's footprint** to offer the best experience.

It offers multiple security capabilities that guarantee the company **secure access to the Internet and corporate applications**, whether they are deployed as Software as a Service (SaaS), in the infrastructure of a cloud provider (IaaS), or in the company's Data Processing Centers (DPC). In addition, for any device regardless of its location, inside or outside the corporate network.

WHAT DOES IT ALLOW?

- **Block access to malicious sites, botnets or malware downloading** on users' browsing from any location and device.
- **Implement browsing policies** based on web categories.
- **Protect** against unknown or zero-day malware.
- Maintain control and visibility **over SaaS application usage.**
- **Provide secure access to private applications**, through a Zero Trust model, to users from any location and device.
- **Security management is delegated to a team of experts from our DOC.**

BENEFITS

Activation and deployment
No infrastructure deployment required at the customer's premises.

High availability and maximum network efficiency
The service's international footprint of nodes guarantees close to 100% availability, with geographic redundancy.

Maximum network efficiency
Direct connection to the main Internet interconnection points and cloud service providers guarantees the best user experience.

24/7 DOC
The customer has 24/7 access to the DOC and SOCs for the management of their requests and incidents. In addition, our experts are available to help you define, transfer, and implement your security policy requirements.

OPEX Model
Avoid the need to invest, deploy and maintain your own security infrastructure by adopting an OPEX model.

Secure Internet Access (SIA)

MORE INFORMATION

Telefónica's network offers a convergent Internet connection and security solution to protect users' browsing.

ABOUT THE SERVICE

It is a managed security service provided from our network and fully integrated with Telefónica's Data Internet connectivity.

It does not require any deployment or configuration of equipment at the customer's home. **The only requirement to enjoy the service is to request activation.**

The customer has a service portal that gives access to reports, configured policies and ticket management.

The security technology provider is a market leader.

WHAT DOES IT ALLOW?

- **Block access** to malicious sites and botnets.
- **Inspect traffic** and block malware downloads.
- Detect intrusion attempts.
- **Implement browsing policies** based on web categories.

Security management is delegated to a team of highly skilled experts from our DOC.

The service scales with connectivity, the customer does not need to worry about upgrading hardware and software as their connectivity needs change.

BENEFITS

Activation and deployment
Activation is automatic and our DOC and SOC teams take care of security policy configuration, providing guidance and support throughout the policy definition and deployment process.

Service availability close to 100%
The service is redundant in different network service centers, so that any of them can take over in case of failure, this confers an availability close to 100%.

Maximum network efficiency
As it is a platform deployed on our network, the impact in terms of delay is minimal and the network experience is optimal.

24/7 DOC
The customer has 24/7 access to our DOCs and SOCs for request and incident management. The customer has experts to help them define and translate their requirements into security policies and implement them.

Security Device Management

Managed service and professional services that ensure the proper functioning and evolution of the customer's security infrastructures.

ABOUT THE SERVICE

Security Appliance Management is the management of security appliances such as firewalls, intrusion detection systems and anti-virus software to ensure that they are properly configured, updated, and monitored to provide effective protection against cyber threats.

Companies require not only a **managed service** to ensure the proper functioning of their security infrastructure, but also **professional services** to help them understand the needs for improvement or evolution of their infrastructure.

WHAT DOES IT ALLOW?

Helps the company to:

- Respond to constantly evolving **threats**.
- **Evolve** its security infrastructure.
- Address **talent shortages**.
- Overcome **budget** constraints.
- Ensure **regulatory compliance.**
- Successfully address **technology changes.**
- Manage the **complexity and diversity** of manufacturer dialogue.

Our DOC and SOC professionals carry out installation and/or migration projects, as well as provide maintenance, support, monitoring, administration, and technical consulting services 24 hours a day, 7 days a week, with certified and experienced personnel in a wide range of technologies with market-leading platforms.

BENEFITS

Supply and installation
Security equipment from leading manufacturers.

Maintenance
Management of maintenance contracts and processes for security equipment.

Specialized support
Advice on the management of safety equipment following best practices.

Health monitoring
Automated monitoring of the status of safety devices.

Administration
Complete operation of security devices, ensuring their correct performance and your security policies.

Consulting and technical architecture
Full range of professional services, guaranteeing the best practices, regulations, and market standards.

Clean Email

MORE INFORMATION

We offer you a managed protection service against your company's main threat vector: email.

ABOUT THE SERVICE

Clean Email provides **advanced email protection** that prevents information leakage, ransomware and other types of malware, phishing and spam.

It is a **managed, comprehensive, and modular service** that combines the capabilities of Telefónica Tech's **Digital Operations Centers (DOC)** with leading technology to protect your company and users.

The service is tailored to the needs of the digital enterprise in terms of **achieving reliability, protection, and security.**

WHAT DOES IT ALLOW?

This service allows you to increase the reliability, effectiveness, and efficiency of your email platform thanks to:

- **Proactive prevention, detection and blocking of threats** before they reach their targets.
- Visibility of threats, with **forensic analysis.**
- **Visibility of the risk** posed by current users to implement preventive measures.
- Shared t**hreat intelligence.**
- Automation of events and remediation to **reduce threat exposure time.**
- **Customer security portal,** where they will be able to fully track business KPI reporting and ticket resolution.

BENEFITS

Risk mitigation
By protecting the main attack vector (e-mail), from which malicious activities are triggered.

Visibility
Thanks to continuous monitoring and reports generated by our DOC experts, it is possible to identify the most targeted users, the main sources of fraudulent emails, etc.

Impact reduction
Being a preventive and proactive service, managed from our DOC and SOCs, it increases efficiency by reducing tasks, time, and possible operational impact.

Threat Intelligence
Unbeatable reliability with enormous detection capabilities of fraudulent elements, thanks to the daily analysis of more than 1 billion messages.

DDoS Protection

MORE INFORMATION

We secure your digital environments and maintain the continuity of your business with a leading and advanced solution in protection against DDoS attacks.

ABOUT THE SERVICE

It is a **managed protection service against DDoS attacks from the network** to the customer's dedicated links. No equipment installation is required thanks to the collaboration of Telefónica de España S.A.U. in its role as ISP.

Traffic destined for the customer's network is monitored and attacks are mitigated before they reach the customer's link, either on the international or national transit network, depending on the specific case.

WHAT DOES IT ALLOW?

This service allows protecting the customer's network assets against DDoS activity in two phases:

- **Detection**: continuous monitoring of traffic directed towards the customer's links, **allowing to obtain statistical usage data and being able to detect massive volume attacks** that saturate these links (volumetric attacks).
- **Mitigation:** traffic from customers under attack is **diverted to a series of mitigation "farms"**. **A mitigation process is carried** out there where a distinction is made between malicious and legitimate traffic, allowing only the latter to progress to the final destination (the customer's network) and blocking the attack, without the need to inspect the traffic.

BENEFITS

Managed service
This solution is provided in service mode, with no investment required from the customer.

24/7 monitoring and response
Permanent monitoring and 24/7 attention from our DOC experts, who analyze the alerts detected and proceed with mitigation in case the attack is confirmed. Our customers benefit from our defined SLA for incidents.

Traffic is not inspected
Statistical information (netflow) is analyzed, guaranteeing the security and secrecy of communications.

Non-intrusive solution
Activated on the customer's dedicated links, it does not involve modifications to the customer's equipment.

Secure Internet Access Branch (SIA Branch)

MORE INFORMATION

Provides advanced security for the company's local network: malware protection, application control, intrusion detection, browsing control and remote access for mobile employees. Managed by our Digital Operation Centers.

ABOUT THE SERVICE

We protect users' Internet browsing and Internet access to resources on the customer's LAN, through a **managed service based on the installation of security equipment at the customer's premises.**

T**elefónica Tech's SIA Branch** (Secure Internet Access) or Managed UTM (Unified Threat Management) **service is based on the deployment, configuration, and remote management of a Fortinet new generation firewall** by our team of experts. **The customer will be able to strengthen the security and visibility of the traffic flowing through their network with a monthly payment system.**

WHAT DOES IT ALLOW?

The service allows the **creation of a border or perimeter between the Internet and the customer's internal network,** monitoring the flow of information between both networks, being able to apply:

- Visibility and reporting.
- Antivirus filtering.
- Protection against attacks.
- Application detection and control.
- Internal user navigation control.
- Antimalware protection.

BENEFITS

Activation and deployment
The service includes provisioning, on-site installation, and policy configuration. Our team of DOC experts provides close guidance and support throughout the deployment process.

24/7 DOC
The customer has 24/7 access to our DOCs and SOCs for request and incident management. The customer has experts to help them define and translate their requirements into security policies and implement them.

Secure Internet Access Essentials (SIA Essentials)

MORE INFORMATION

A service that offers protection for users' browsing by preventing access to malicious and malware domains.
It also allows to control navigation destinations, improving productivity and protection of the company's users.

ABOUT THE SERVICE

We provide you with **a solution that allows you to offer security features by default from the operators' networks.**

Telefónica Tech's **SIA Essentials** (Secure Internet Access Essentials) service **leverages the network's DNS servers to check whether the sites being accessed by network users are legitimate** or, on the contrary, are infected by malware, phishing or are related to a botnet.

Additionally, we offer the possibility of acquiring a package in which you can add web **filtering by categories and Internet disconnection according to schedule.**

WHAT DOES IT ALLOW?

- **Differentiate the operator's communications network** by providing a default security layer.
- **Provide web security based on DNS and web filtering** to keep you up and running quickly and reliably.
- **Have maximum protection** against botnets, web phishing and malware.
- **Temporarily disable your Internet connection.**

BENEFITS

Delivery and deployment / installation
Our team will advise you on the way and requirements to integrate the solution into the network with the least possible impact in order to make it a complete success.

Level 2 and Level 3 Support
Our service-associated security experts can be engaged to support customers by minimizing the need for locally trained assets.

End customer supply processes
Additionally, provisioning mechanisms are provided to integrate with your systems and automate service activation for end customers.

Web Application Defense (WAD)

MORE INFORMATION

The Web Application Defense service offers a comprehensive range of solutions to protect web applications and APIs against specialized threats.

ABOUT THE SERVICE

WAD (Web Application Defense) is a **comprehensive service that offers a wide variety of solutions to protect web applications and APIs from the most common and specialized cyber threats in this asset class**, such as DDoS attacks, automated attacks, information leakage, malicious code injection and more.

This service also provides actionable intelligence so that organizations can **anticipate emerging threats and take preventative measures to ensure the security of their critical applications and data.**

WHAT DOES IT ALLOW?

The service allows us to provide our customers:

- **Market-leading technology** with full understanding of the needs of both traditional and cloud-native applications.
- **Scalability and easy deployment** regardless of where applications are hosted, with secure and efficient handling of increased request traffic, including APIs.
- **Simplified and centralized policy management and monitoring** to avoid vulnerabilities due to misconfigurations and scattered and inconsistent policies.

BENEFITS

Higher level of security
Improves security posture by providing enterprises with comprehensive protection against traditional and modern cyber threats.

Compliance
Enables compliance with standards and requirements of regulatory agencies.

Trust
Improve customer confidence by reducing reputational damage from security issues.

Spending efficiency
Cost savings by improving the level of protection by avoiding the costs associated with security incidents and related legal expenses.

Specialized support
Customer service and management by Security and Cloud specialists.

OT Security

MORE INFORMATION

Cyber security solutions for industry, critical infrastructure, and healthcare environments.

ABOUT THE SERVICE

The digitalization process in which we are immersed in recent years is transforming infrastructures and sectors that until now remained partially isolated and perform critical functions for society. This is the case of hospitals, energy generation, transport and distribution infrastructures, and the manufacturing sector in general.

Telefónica Tech has a range of **products and services and a team specialized** in this specific field of cyber security.

WHAT DOES IT ALLOW?

Our value proposition is composed of different products and services that allow us to adapt to the customer's needs:

- **Industrial Cyber Security Assessments:** Industrial cyber security assessments to survey existing assets and identify and analyze risks.
- **OT&IoT Perimeter Protection:** IT/OT segregation and OT network segmentation projects to define and implement secure network architectures and secure remote access solutions.
- **OT&IoT Security Monitoring:** Managed industrial monitoring service to maintain an up-to-date view of assets and have incident detection and response capabilities.

BENEFITS

Facilitates digital transformation
Our goal is to help you in your digital transformation, to make it secure and resilient.

Know your environment
Gain maximum visibility into your infrastructure and the cyber security risks to which it is exposed.

Tailor-made protection
We have specific security solutions for each sector such as energy, medicine or robotics.

Focus on your business
Our managed services take care of everything so you can focus on what matters most: your business.

Industrial Perimeter Protection

A set of solutions for perimeter protection of infrastructures that host cyber-physical systems where operational technologies and IoT in general are highly relevant.

ABOUT THE SERVICE

It is a modular service proposal with different cyber security functions and a depth of service adaptable to the customer's needs to **provide perimeter protection of infrastructures.**

The service is a natural follow-up to an industrial cyber security assessment, which provides an understanding of the infrastructure that is the basis for a **secure network architecture design.**

The design is then implemented by deploying IT/OT segregation, OT network segmentation and OT remote access solutions.

WHAT DOES IT ALLOW?

It meets the needs in terms of **infrastructure protection** and the establishment of a formal access control mechanism.

The functions that can be offered are typical recommendations arising from the cyber security assessment:

- Segregation of IT and OT networks.
- OT network segmentation.
- Remote access for OT environment.
- The service is tailored to the customer's needs and may include.
- Supply of the technological solution.
- Solution implementation.
- Exploitation of the industrial solution.

BENEFITS

Laying the foundations of the cyber security strategy
The fundamentals of cyber security policy start with knowing the infrastructure, considering a secure design, and implementing a protection solution on which to build other solutions.

Modular proposal adaptable to your particular needs
The service has been structured in modules to meet the needs in terms of concrete solutions and depth of service.

Guarantee of an experienced team
The service is provided by a multidisciplinary team composed of experts in industrial cyber security and in the implementation and operation of the supported technologies.

Industrial Cyber Security Assessment

A service consisting of the cyber security assessment of environments where operational technologies and, in general, devices and systems for monitoring and control of operational activities, such as factories, energy generation and transportation systems or healthcare environments, are the most important.

ABOUT THE SERVICE

The service consists of the **collection and analysis of information on the infrastructure** under analysis by a team of professionals certified in the reference standard for industrial environments (IEC 62443).

The capture of traffic from the environment is added to the documentation provided by the customer, which is analyzed with different tools in order to obtain information on the assets and the risks to which they are exposed to finally determine a series of recommendations.

A report is delivered as part of the service.

WHAT DOES IT ALLOW?

- **Identify assets, their communication relationships**, and a high-level view of the network architecture.
- **Identify the main risks** to which the infrastructure under assessment is exposed.
- To have a series of security r**ecommendations with which to establish a plan** to prioritize the implementation of countermeasures to improve the level of security.

BENEFITS

Visibility of the environment and identification of risks
The report delivered provides a clear picture of the operational environment at the time the information was captured, allowing the CISO and other stakeholders to be aware of the environment and the most relevant risks.

Establish the basis for a Security Master Plan.
The detailed information together with the recommendations to solve the vulnerabilities detected, provide the starting information to be able to elaborate a Security Master Plan that we can also offer as a continuation of the service.

OT&IoT Security Monitoring

MORE INFORMATION

Managed service based on our MSSP capabilities based on leading monitoring technology for security monitoring of environments where operational technologies and IoT devices are key players, such as industrial plants and hospitals.

ABOUT THE SERVICE

The service provides the **ability to detect incidents and anomalies in industrial and healthcare environments.**

A series of probes are deployed in the infrastructure being monitored, capable of inspecting traffic and generating events that are received by our DOC, as part of the service. We have implemented a series of detection procedures on this basis, which are additionally fed from our internal and external sources of cyber threat intelligence with the aim of minimizing false positives and enriching the alerts that are generated to notify incidents.

WHAT DOES IT ALLOW?

Main characteristics of the service:

- **To have a service for monitoring the security** of environments and detecting incidents and anomalies that may affect operations.
- Be aware of **changes in the operating environment** in the form of new assets and/or vulnerabilities.
- To be **aware of the incidents detected** and the treatment given to them.

BENEFITS

Continuous visibility of the environment
Thanks to continuous monitoring, there is an up-to-date knowledge of the productive environments in terms of assets and communication relationships between them.

Detection of threats affecting the environment
Continuous monitoring and periodic updating of the threat database provides an incident detection system for the monitored infrastructure.

Saves costs by outsourcing the monitoring function
Although it is possible to acquire the technology and build a service on our own, the shortage of professionals with specialized knowledge in industrial cyber security and the pace at which technologies are updated make it difficult to maintain the quality of the service over time. With this service we make it possible to outsource this function to our customers.

SECURE MICROSOFT • A complete cloud security services solution carefully designed to strengthen your Microsoft 365 environment. Security consulting, implementation and management organized in four modules: Identity, Devices, Information and Threats.

Secure Microsoft 365

MORE INFORMATION

We secure your Microsoft 365 environment thanks to our consulting, implementation and security management services tailored to your needs.

ABOUT THE SERVICE

We offer a **customized solution** based on the current state of your company. We implement the necessary tools, configure the relevant policies and thus achieve the **highest possible level of security.**

We carry out a **diagnosis and establish customized goals**, adapted to your organization's priorities, with **consulting services**.

We implement the **appropriate tools according to a roadmap aligned** with your concerns and pain points. We finally perform a **management that allows a continuous improvement of security.**

WHAT DOES IT ALLOW?

- **Know the security status** of the Microsoft 365 environment.
- Identity **management and protection**
- **Improve the bastioning of the organization's devices** and manage the use of BYOD.
- **Protect information in line** with the needs of your organization.
- **Monitor threats in your environment** to improve the security of the devices.

BENEFITS

Applied safety
You have the tools, we provide the services to ensure that your security is at the optimum level for your organization.

Certified specialists
Specialists knowledgeable in multiple security technologies and Microsoft certified at your disposal.

Cost reduction
Know in advance the cost of the service and how much you can afford to pay for it.

Flexibility
You can address all areas at once or start with the one that most concerns your organization.

DATA & IDENTITY PROTECTION

- Provide your employees with efficient and secure access to your organization's corporate resources and prevent unauthorized access or loss of sensitive company data in modern, hybrid and remote user architectures.

Information Rights Management

MORE INFORMATION

It allows companies to have their sensitive information under control and protected, limiting access to documents to those who must have it, with the minimum permissions necessary to carry out their function, following the principle of least privilege.

ABOUT THE SERVICE

We offer you an intelligent service for the protection and control of your information, whatever and wherever it is.

Telefónica Tech's Information Rights Management is an intelligent, data-centric, corporate document security service that combines the capabilities of our DOC and SOCs with leading technology to protect and control corporate information, whatever and wherever it is, based on the principle of least privilege.

The protection travels with the information, and it is the protection that determines who can do what with the information.

WHAT DOES IT ALLOW?

- **Secure your documentation and sensitive information** in corporate repositories, and beyond.
- **Take quick action on certain events** (ex-employees, change of roles, partners, loss of devices).
- Enhance your **reputation and credibility** with non-intrusive protection measures that promote change management.
- **Reduce costs** by simplifying the tasks of security administrators and areas with critical information.
- Comply with the **rules and regulations** regarding **security, privacy and data protection.**
- **Dedicate yourself to your business**, delegating the implementation, monitoring and support to our experts.

BENEFITS

Dynamic data protection
It doesn't matter where the data is (where it is and whether it is at rest, in transit or in use) and it doesn't matter what kind of data it is or what type it is. Protection always travels with it (embedded at rest) as if it were just another component of the document.

Monitoring, control, auditing and tracking of data
Thanks to the technological power and the service provided by Telefónica Tech's DOC and SOC experts, you always have visibility over your protected documents, knowing what is happening with them (who is trying to access them, permissions, etc.).

Data loss prevention
The document always travels with its corresponding protection, which cannot be removed, the two being inseparable. It is possible to control who has access and for how long, or even revoke access to the document, remotely.

Normative compliance
You avoid non-compliance with data protection regulations (GDPR, PCI, ISO 27001), legal liabilities and financial losses by encrypting, controlling access and not storing documents (but rather permission relationships over them).

DATA & IDENTITY PROTECTION

Provide your employees with efficient and secure access to your organization's corporate resources and prevent unauthorized access or loss of sensitive company data in modern, hybrid and remote user architectures.

Digital Certificates

MORE INFORMATION

We guarantee the security of your website by issuing TLS/SSL certificates through our own platform, carrying out an exhaustive follow-up of our customers and controlling the entire life cycle of the certificates.

ABOUT THE SERVICE

Telefónica Tech **guarantees the security of your website by issuing TLS/SSL Digital Certificates** through our own platform, carrying out an exhaustive follow-up of our customers and controlling the entire life cycle of the certificates.

We manage DigiCert's SSL and MPKI certification services for the most important IBEX35 companies, including the main national and international banks present in Spain for the issuance of SSL secure server digital certificates, users and document signatures.

We offer different types of certificates: SSL (single domain, multi-domain, wildcard, EV, customer, private CA), code signing, document signing, and document signature.

WHAT DOES IT ALLOW?

- Show your **website secure and reliable** in all browsers.
- Protect sensitive information.
- Ensure **GDPR compliance.**
- To have all the **guarantees of Telefónica Tech**, DigiCert Platinum Partner.

BENEFITS

Agility in issuance deadlines
We manage the issuance of certificates through our own CertCentral® platform in the manufacturer's PKI structure, which allows us to guarantee faster issuance times.

Personalized attention
We have a highly qualified technical and commercial team that provides our customers with personalized attention and real knowledge of the casuistry of the national market.

Cost reduction
We provide specific offers with volume discounts and special offers thanks to strategic agreements.

Confidence and security guaranteed
We manage the issuance of certificates with a prestigious certification authority, providing the necessary confidence to ensure the identity of the certificate holder customer.

Access & Authentication

MORE INFORMATION

Centralizes access management to corporate resources and incorporates multi-factor authentication and single sign-on.

ABOUT THE SERVICE

Access & Authentication is a complete access management solution, which allows organizations to **centralize the administration and management of access control systems and control access to any corporate resource**, including network elements such as VPNs and applications such as Office 365. In addition, among other functionalities, it incorporates **multi-factor authentication (MFA) and single sign-on (SSO),** thereby improving safety and productivity.

Access & Authentication offers all this at a much **lower price** than the competition and also includes an **end-to-end service** where we carry out the implementation and configuration of the service as well as support, monitoring and administration.

WHAT DOES IT ALLOW?

- **Improve security,** including multi-factor authentication (MFA) by forcing users to use an additional factor before authenticating.
- **Centralize identity management** and application **access** in one place thanks to administration and user portals.
- **Improve productivity** by freeing up most tasks for IT and HR teams and across the entire workforce with Single Sign-On (SSO) functionality.
- **Control employee access** to corporate resources through configurable access policies while ensuring the principle of least privilege.

BENEFITS

Deployment, implementation, and configuration
Our team is in charge of the entire service provision, performing the deployment and implementation of the solution and supporting the configuration of the final systems.

Monitoring, support, and administration
The service license itself includes by default the monitoring and support in 8x5.
In addition, this support can be extended to 24/7 and we can even perform all the administration of the service.

Low Price
The service has the main functionalities for a lower price than the competition and including support.

Control Roadmap
As the solution is owned by Telefónica Tech Ventures, we control the roadmap so we have the flexibility to incorporate new functionalities as required.

Electronic and Biometric Signature

MORE INFORMATION

SealSign is a scalable, modular, and complete enterprise platform for signing electronic documents, compatible with digital certificates, OTP codes and biometric signatures. It generates electronic documents with full legal validity.

ABOUT THE SERVICE

SealSign is the platform on which we offer the Electronic and Biometric Signature service that **allows the electronic signature or handwritten signature of electronic documents** made with a stylus or touch pen on a screen with the capture of the graphic trace and the data that make up and validate the signer's biometric pattern, with full legal guarantees.

It also allows signing by OTP (sent by email or SMS) and certificates (SealSign Central Key Control - CKC). Possibility of offering the service in cloud or on-premises model according to customer needs.

WHAT DOES IT ALLOW?

- **Define an electronic or biometric signature** flow to sign from any location and device and receive all documents to be signed in a way similar to an email inbox and protect against information leakage.
- **Sign any document electronically:** delivery notes, contracts, purchasing signature process, review signatures, policies, customer identification and patents.
- **Sign electronically any other type of documents:** informed consents, identification of medical personnel, among others.
- **Control and store certificates in a centralized, controlled and secure** manner in encrypted databases or HSM devices that allow only authorized users to perform authentication, signature or encryption processes.

BENEFITS

Agility and security
Increases the agility and security of document signing while maintaining an optimal user experience.

Productivity and efficiency
Improved productivity and efficiency of the processes associated with the business.

Time and cost savings
Reduces turnaround time in daily operations and costs associated with paper document management (printing, scanning, transferring, archiving).

Validity and legal protection
Generation of electronic documents with full legal validity. Facilitates regulatory and legislative compliance associated with the business activity, maintaining confidentiality and legal certainty.

Control
Mantiene el control sobre quién o quiénes pueden realizar operaciones sobre los certificados mediante políticas de uso y trazabilidad de las operaciones realizadas.

Priviledge Access Management (PAM)

MORE INFORMATION

Our solution establishes a control barrier by separating the nominal accounts of privileged users from the generic access accounts, thus allowing to establish an intermediate and independent control element over access.

ABOUT THE SERVICE

We protect your organization's critical infrastructure and sensitive information from credential theft and privilege misuse.

Privileged access enables organizations to protect their infrastructure and applications, manage their business efficiently and maintain the confidentiality of sensitive data and critical infrastructure.

Telefónica Tech offers the **Privilege Access Management (PAM) service to help our customers protect all privileged accounts** by guarding their passwords, isolating their sessions, and proactively monitoring their accesses.

WHAT DOES IT ALLOW?

- **Custody and storage of credentials:** centralization of the storage of privileged passwords, in order to easily and efficiently apply corporate security policies.
- **Isolation and session control:** protect systems by isolating privileged user sessions to identify who is using them and ensure that they have the required authorization.
- **Threat monitoring and detection:** monitor privileged access activity to detect anomalous behavior on critical systems and be able to perform audits both in real time and a posteriori.
- **Real-time response:** automatically intervene to suspend or terminate sessions based on user actions during the session, as well as facilitate the action of specialized threat teams.

BENEFITS

Offered in SaaS mode
This modality allows an easy and simple deployment and integration with minimal impact on the daily operation of the organization.

Centralized access management system
We make employees' day-to-day work easier by providing them with single sign-on and self-service portals to manage their password and access to corporate applications.

Flexible platform
Based on a leading technology that facilitates the use and operation of the solution.
The isolation process and session control are transparent to the users of the service, which results in greater use of the solution.

Scalability and integration
The PAM service is designed to evolve as needs grow and also to adapt to other IAM solutions.

FlexSuite

Cloud and secure connectivity

We offer you a comprehensive service of connectivity to and from your cloud with the flexibility and speed of cloud-native deployment and operation.

Telefónica Tech

SASE

MORE INFORMATION

Cloud-based security to adapt to all new challenges and ensure that your network is protected at all levels.

ABOUT THE SERVICE

This is a service in **which security and network functions converge,** forming a SASE architecture where **SDWAN, Security Edge and Zero Trust concepts are integrated and interconnected to form a more efficient solution, with comprehensive visibility and more use cases.**

You decide how traffic is managed with SDWAN to make your network agile, dynamic and ready for acceleration to the cloud and ready for cloud acceleration, and Security Edge protects users, data and applications, wherever they are. All managed from our Digital Operations Center and SOCs.

WHAT DOES IT ALLOW?

Our SASE service combines the advantages of D-WAN and Edge security in a single product.

- The convergence of security and networking improves our service by **making it simpler, reducing vulnerabilities and improving threat response.**

BENEFITS

Security applied from the cloud
Consolidates security functions and applies in a cross-cutting and coordinated manner homogeneous policies inside and outside the office.

Safe navigation
Protects employees when surfing the Internet. Adapted to a mobile environment and from any device.

Secure and controlled access to applications
Access control adapted to hybrid environments under Zero Trust model that provides granular access policies based on identity, application, and risk assessment of each access.

Specialized support
Continuous advice from our experts on service management and best practices.

Efficiency and agility
Continuous monitoring and rapid resolution of security events.

FlexWAN

MORE INFORMATION

Our FlexWAN converged network and security service, managed by our experts, protects your company from the threats of the future.

ABOUT THE SERVICE

We offer a comprehensive **FlexWAN network and security solution** with market-leading technologies to **centralize management and gain visibility and control over the most complex network and security scenarios.**

We support companies from the equipment to the commercial, provisioning and operation processes. **It includes integration with the network, installation and provision of the device, operation, support, and proactive evolution** of the service based on market analysis and customer needs.

WHAT DOES IT ALLOW?

- Adopt **market-leading** WAN and security technology, **advanced functionalities and complete portfolio.**
- Increase your own **ability to protect** your company and employees from persistent **cyber threats.**
- **To have a network and security provision advised by specialists** who design a customized solution, operate the service and help you to evolve it.

BENEFITS

Simple and modular business model
We offer a customized monthly payment model without prior investment in HW, licenses and platforms. Includes activation of all service elements and security features.

Transparent service delivery
The technical team will be responsible for setting up the service and the platform will be managed by us in the cloud to ensure data privacy.

Real-time management portal
We support early detection and resolution of incidents through real-time service monitoring. We generate customized reports and graphs of the status of your network and security services.

Customer service and management by specialists
We have 24/7/365 customer service teams for the identification and resolution of incidents, as well as the management of configuration changes.

FlexSITE

MORE INFORMATION

Connect, optimize, and secure your end-to-end enterprise network with the simplicity of our solution.

ABOUT THE SERVICE

This solution i**ntegrates SD-Branch services** (WiFi & LAN, secure SD-WAN) f**or the end-to-end of your enterprise network.**

Our specialists will help you accelerate time to market by choosing the technology that best fits your business strategy and IT requirements, designing and installing each site and proactively managing incidents and service evolution.

WiFi and LAN technologies have evolved to become part of Secure SD-Branch technologies. **We use the best platforms on the market to offer you centralized management from the cloud and transversal network security.**

WHAT DOES IT ALLOW?

- **Deliver an improved user experience**, with higher throughput, lower latency, and increased bandwidth to support new hosted business applications on-premises or in the cloud.
- **Scale as your business grows, streamline changes** to your network and reduce deployment time.
- Visualize relevant network data and **anticipate possible anomalies** through analytics and Artificial Intelligence.
- **Enable WiFi and LAN service integration** with other network and security services.
- Access a **customer portal with network visibility** and shared management option and customizable captive guest portal.

BENEFITS

Simple and modular business model
Monthly fee without prior investment in hardware and licenses. Flexible blocks adjustable to your network refreshment needs. Easy license activation and integration with security.

Prompt service delivery
Architectural design, planning, and complete installation of CPEs, switches and access points and cabling. Service on the managed cloud platform.

Customer service and management by specialists
We have 24/7/365 customer service teams for the identification and resolution of incidents, as well as the management of configuration changes.

End-to-end service convergence
Analysis of configuration changes to ensure consistency between the services of the suite. Correlation between WiFi & LAN issues with SD-WAN and security issues.

Secure SD-Branch

MORE INFORMATION

Telefónica Tech's Secure SD-Branch managed service is the end-to-end managed service that brings together WiFi & LAN, SD-WAN and cyber security services for headquarters and teleworkers. In addition, it does so in an integrated manner with all of Telefónica's fixed and mobile connectivity offerings.

ABOUT THE SERVICE

An **SD-Branch solution** is one that combines in a single platform and SDN (Software-Defined Networking) architecture at least 4 solutions that traditionally existed as separate products: Cloud WiFi and LAN, SD-WAN and connectivity (MPLS, Internet or mobile).

You can easily automate the deployment, management and operation of wired, wireless, and WAN infrastructure from the central platform.

Our Secure SD-Branch service adds integration with network components, security elements such as NAC, ZTNA or integration with cloud security solutions such as SSE, coining the term "Secure SD-Branch" and providing headquarters and remote workers with a secure network perimeter.

WHAT DOES IT ALLOW?

- **Centralized and remote management:** the control and management of the lifecycle of each device is centralized in a single cloud platform. Therefore, onboarding, configuration and monitoring can be performed in a simple and massive way.
- **Dynamic traffic balancing between accesses:** the SD-WAN router provides the network with high availability and QoS. By configuring granular network policies, administrators can choose which access should use which type of traffic. Internet for SaaS, MPLS, corporate applications or mobile network as a back-up in case of fixed access failure.
- **High-performance WiFi and LAN:** extensive hardware portfolio for indoor and outdoor deployments that can serve high traffic or device density environments.

BENEFITS

Rapid project execution
As all modules are integrated and have a central platform from which all configuration is done, once the project is designed, deployment and start-up can be done as soon as the hardware is available.

Easy onboarding of new devices
Zero Touch Provisioning (ZTP) capabilities mean that device onboarding can be done in a matter of minutes.

Reduction of management costs
Network administrators can transform the information available in the management platforms into dashboards and customized reports that allow them to increase their knowledge of the state of their network. They can then take improvement actions to reduce the number of incidents and improve the user experience.

Reduction of vulnerabilities
By applying cyber security policies in a centralized and integrated manner across modules, you can ensure that these policies function correctly across the entire device plant.

Your 360° Digitalization

Service for SMEs

Find out more about how we can help your digital business by protecting your company with our cyber security services.

Telefónica Tech

Your Secure Enterprise

MORE INFORMATION

The digital security and 24/7 support your SME needs.

ABOUT THE SERVICE

Telefónica Tech wants to help you so that your business is always safe through a managed security service.

Tu Empresa Segura is a cyber security solution fully adapted to your needs so that you can rest **assured that your business is always protected.**

We will be by your side during the whole process: giving you support and solving your doubts and incidents, speaking your language, and with a customized attention from our personalized security support center (SOC Pyme).

You will have a group of experts that will accompany you from the very first moment, making safety a simple matter.

WHAT DOES IT INCLUDE?

We provide a managed cyber security service that includes **support and maintenance, management** with definition of policies and rules and configuration of tools and access to service reports.

WHAT DOES IT ALLOW YOU TO DO?

We offer **3 different packages** adapted to the protection needs of your company, the type of data it handles, the use of email or the navigation it performs so that your organization has, depending on the package chosen, the following services.

- Safe navigation.
- Antivirus / Antiransomware.
- Clean Mail.
- Secure Remote Work.
- Sede Segura.
- Awareness.
- Protection of Cloud services.

BENEFITS

Risk reduction
Acting early by determining the possible threats and what the prevention and reaction measures will be in case of attack, will allow you to be prepared. It is about being ahead of those who intend to attack your business information.

Business continuity
React quickly to ensure business continuity while maintaining a minimum level of service to avoid business interruption.

Earn trust and reputation
By protecting your business, you not only protect your company's data, but also your customers' data, with the peace of mind that we protect the privacy of that information.

Secure Business Connection

MORE INFORMATION

Surf the Internet without fear of viruses and malware.

ABOUT THE SERVICE

A **secure connectivity** service for your company, exclusively for all organizations that have Fusión Empresas.

Protects Internet browsing traffic, cleaning it from Telefónica's network.

¿QUÉ PERMITE?

Web filtering by web categories and URLs filters and blocks all http and https traffic from your company. Allows you to include pages in a "blacklist", configure specific browsing schedules, block/unblock policies, etc.

- **Antiphishing:** protection against phishing scams on the Internet (detection and blocking).
- **Antivirus:** protection against viruses, spyware, trojans and worms that could potentially infect computers while surfing the Internet.
- **Dashboard:** service self-management portal with customized reports: deleted viruses, blocked categories, most visited websites, etc.
- **High visibility of the service:** icon/Mosca during navigation (http).

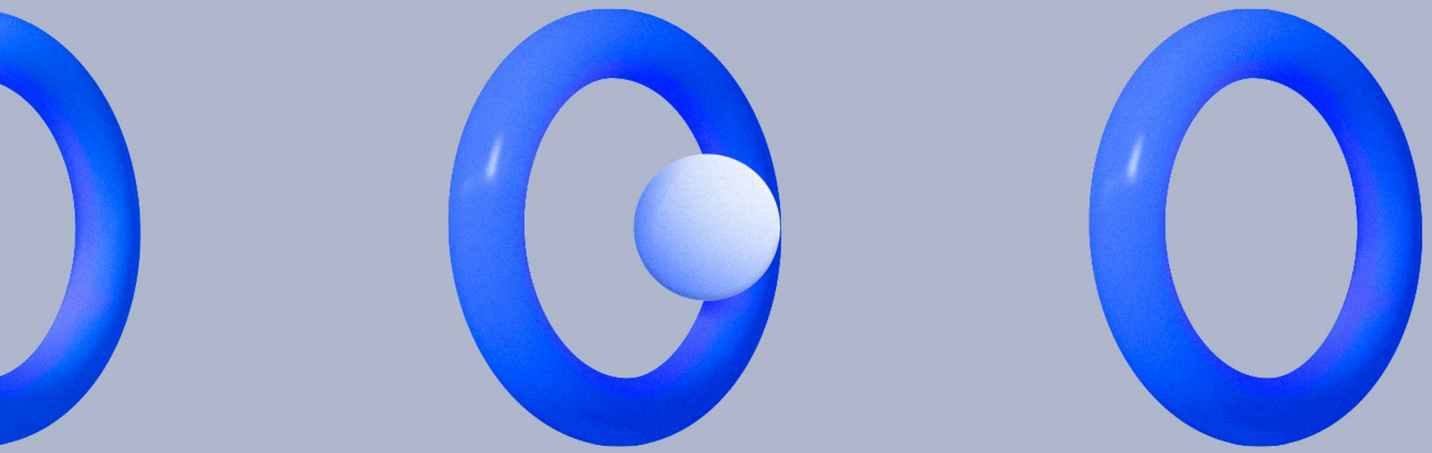
BENEFITS

Reliable
Surf peacefully free of viruses and phishing. With the Antiphishing service you will protect your employees from possible fraud on the Internet by identity theft and with the Antivirus you will protect your computers from viruses, spyware, trojans, and worms that could infect them while your employees surf the Internet.

Productive
Controls where and at what time employees surf. The service prevents access to unwanted Internet content and the downloading of potentially harmful files.

Adaptable
No investment in equipment, as security is provided from the Telefónica network and at a monthly cost per site.

Intuitive
Manage the service intuitively from a simple web portal with customized reports.



Consulting and Professional Services

Tailor-made services

We support you throughout the entire lifecycle of identification, implementation and management of the solution that best suits your business objectives with our consulting and professional services capabilities.

Telefónica Tech

CONSULTING AND PROFESSIONAL SERVICES

We support you throughout the entire lifecycle of identification, implementation and management of the solution that best suits your business objectives.

Cyber Security Consulting

MORE INFORMATION

We help you with the cyber security and resilience of your processes to make your digital transformation: fast, simple, and secure.

ABOUT THE SERVICE

We offer a **comprehensive cyber security consulting and advisory service.**

We provide you with the best expert consultants, with more than 10 years of experience in cyber security, resilience, and regulatory compliance projects, who will be able to design a customized plan and provide the subsequent support your business needs to make your digital transformation a success.

We can also **train your employees** so that they stay at the forefront of technology and acquire all the necessary skills

CAPABILITIES

We train your employees to develop and strengthen their cyber security skills.

- **Awareness: we reinforce the behavior and safety habits of employees**, preparing them for the increase of cyber-attacks, providing them with a greater perception of risk and reducing security incidents and information leaks.
- **Training:** we accelerate the level of knowledge in information security of employees through the design and implementation of a **training program to promote skills** and respond to the high demand for professionals in this market.
- **Simulation:** we have tools and professionals to **simulate possible attacks and/or vulnerabilities** and teach you how to improve your security by offering you practice in real environments.

COMPREHENSIVE LEARNING SERVICE

- **Cyber security:** We offer services to align your organization's cyber security initiatives with your business objectives. Including Security Master Plans based on best practices, as well as external CISO support services.
- **Privacy:** We provide the best expert advice on privacy matters, including audits and defense against claims. We have a team of certified DPDs who provide external support to the DPD or assume its outsourcing.
- **Resilience:** We contribute to the improvement of Business Continuity and Disaster Recovery and Cyber Security Incidents. We contribute to the analysis of the context, determination of the impact, development of plans and strategies and periodic testing to improve the resilience of the most critical infrastructures.

Cyber Security Professional Services

MORE INFORMATION

We help you with the cyber security and resilience of your processes to make your digital transformation: fast, simple, and secure.

ABOUT THE SERVICE

We support you throughout the entire lifecycle of identifying, implementing, and **managing the solution that best suits your business objectives with our consulting and professional services capabilities.**

Starting with our strategic and technological consulting that helps you identify the cyber security risks of your business and design a strategic security plan, to the implementation and integration, management and response that will allow you not only **to be cyber-resilient but also to comply with the Security Regulations that apply to your business.**

All this, added to the i**ntelligence, orchestration, and detection platforms, as well as our numerous certifications, alliances and partnerships** make Telefónica Tech the best choice for your business.

CAPABILITIES

- **Managed services:** we manage security by adding an extra layer of intelligence. With our capabilities you can improve visibility into corporate security and strengthen your defense while gaining information to make decisions. We have experts distributed in our DOCs and SOCs who work combining knowledge and best practices, as well as the most advanced intelligence platforms.
- **Security implementation and integration:** delegate the complexity of the implementation and integration of your business security to our professional cyber security consultants. When the chosen solution meets the expectations defined by the business, a correct design is key, as well as the adaptation of the implementation, integrating it with the customer's systems.
- **Security consulting services:** we provide you with the capabilities to define the best security strategy and address your transformation with a risk approach always defined from solution design. Our consulting helps you identify the most important technological risks, achieve complete visibility of threats and design, and implement solutions to minimize exposure to attacks.

Telefónica Tech

Telefónica Tech is the leading company in digital transformation. It offers a wide range of services and integrated technology solutions for Cyber Security, Cloud, IoT, Big Data, Artificial Intelligence, and Blockchain.

telefonicatech.com