APPLICATION RESILIENCY

Akamai Guardicore Microsegmentation

HOW CAN TELEFÓNICA TECH HELP?

Akamai Guardicore is beyond traditional security, offering advanced visibility, east-west and north-south traffic control with effective malware containment, reducing the attack surface

Relying on perimeter security alone is no longer sufficient in a scenario where corporate networks are increasingly dynamic and distributed. Modern threats adapt quickly and seek to expand laterally, taking advantage of poor internal segmentation. **Organizations require a clear vision, granular control, and real incident response capabilities to cope with this landscape.**

The Akamai Guardicore-based microsegmentation solution allows the establishment of clear boundaries between critical systems, applications, and services, without the need to redesign the existing infrastructure.

It is possible to define segmentation policies adapted to the actual operation of the business through a precise visualization of the traffic. This enables minimizing the attack surface and slowing down the advance of possible internal and external threats.

Our specialized team supports each phase of the project, from the initial analysis to implementation and monitoring, ensuring an agile and effective adoption. It is a key solution to strengthen security in on-premises, hybrid and multicloud environments, without compromising the operability and agility of the business.

WHO IS THIS SERVICE FOR?

Organizations of any size **seeking to contain threats through microsegmentation, without the need to redesign their network,** and to reduce costs associated with complex solutions or traditional infrastructures that are ineffective against lateral movement.

Large organizations with established cyber security capabilities that need **to segment complex environments, reduce the attack surface,** and outsource the ongoing operation so that their internal teams can focus on higher value strategic initiatives.

Entities and administrations that need to segment critical environments **to comply with regulations** such as PCI DSS, GDPR or sectorial frameworks, protecting sensitive systems and reducing the attack surface to ensure solid and sustainable compliance over time.

OUR VALUE PROPOSITION

Our service

The **Akamai Guardicore** microsegmentation service **protects complex environments from advanced threats,** such as malware that moves laterally to compromise multiple systems. It identifies interdependencies between assets and applies controls without impacting operations with detailed traffic visibility and precise segmentation policies.

Thanks to its logical segmentation approach, it limits the propagation of attacks and reduces their impact. The dynamic segmentation platform and our 24/7 SOC complete a value proposition focused on effective risk containment and mitigation.

What does it allow you to do?

The service enables the implementation of **granular and adaptive microsegmentation that provides control over traffic between applications, servers and users, preventing lateral movement and containing threats, offering both north-south and east-west protection.** Unlike traditional approaches, it offers complete visibility into communications, enables accurate policies based on real context, and integrates easily into hybrid and multi-cloud environments, without the need to redesign existing infrastructure. This flexibility enables progressive adoption aligned with business priorities.

› **Visualize and map** interdependencies between assets in real time to design effective segmentation.

› Having a specialized team that **identifies risks and assists in the definition of containment policies.**

› **Reduce attack surface and prevent threat propagation** through smart segmentation and detection of anomalous behavior within the network.

Benefits

Deep and continuous visibility of internal traffic

Our microsegmentation solution provides detailed mapping of communications between assets, applications, and services, allowing you to detect unnecessary relationships and establish accurate segmentation policies. This continuous visibility facilitates risk identification and strengthens security in real time.

Resource optimization

Organizations reduce the costs associated with traditional infrastructures and free internal teams to focus on more analytical, planning or continuous improvement tasks.

Centralized management from a single console

Akamai Guardicore provides a unified console that allows you to view internal traffic in real time, manage segmentation policies intuitively and apply precise controls from a single point of operation.

Telefónica Tech's differential value

We offer you the best microsegmentation technology through our strategic partnership with Akamai Guardicore, recognized for its innovation in application protection, environments, and smart segmentation.

Each defined policy is based on an in-depth analysis of traffic flows, allowing us to apply precise controls that limit unnecessary connections and strengthen security in real time.

Our certified team has experience in complex segmentation deployments, which allows us to adapt this solution to any environment ensuring efficient integration without affecting operational performance.

TEAMS AND ACHIEVEMENTS

Our teams

- **+2.500 cyber security professionals**
- **Global presence** through Security Operations Centers (SOC) and Digital Operations Center (DOC).
- **Ability to implement and operate** microsegmentation solutions in complex environments.

Achievements

- Microsegmentation projects implemented in **highly regulated critical sectors** such as infrastructure, healthcare, and public sector.
- **Significant reduction** of attack surface in hybrid and multi-cloud infrastructures.
- **Improved incident response times** thanks to dynamic segmentation and real-time visibility.

BUSINESS MODEL

The Akamai Guardicore microsegmentation service is aimed at strengthening the internal security of complex infrastructures, limiting unauthorized communications between systems. Its managed model requires a minimum duration of 12 months and is priced according to the number of assets, environments or segments to be protected, including technological provision, policy design and continuous operation of the environment.

- Segmentation project: number of servers or environments.
- Managed operation: defined coverage and scope.

RELATED PARTNERS

Akamai

Discover all our solutions

We believe in the transformative power of technology to improve processes, optimize resources and open new business opportunities.

Contact us to start the digital transformation of your organization.