SD microsegmentation – easily deployable security services for companies of all sizes

Akamai Guardicore for the protection of hybrid & multi-cloud architectures against cyber attacks

The more complex the IT services used, the greater the security effort required. The isolation and segregation of applications and their components in the network is necessary to meet compliance requirements and protect enterprise applications and data against cyber attacks. The Guardicore Centra unified microsegmentation solution enables the rapid integration of new applications and minimizes the risk of a cyber attack. The centrally-managed SD microsegmentation service offers many benefits beyond the defense function. For example, application dependen cies can be mapped more comprehensively and policies can be implemented more effectively.

Recognizing and assigning relationships between applications

- Automatically correlate activities at network and process levels
- Identify application behavior based on process-level context

Design, test, and deploy policies quickly

- Design policies using automated rule suggestions based on historical data
- The intuitive workflow helps to continuously refine policies and eliminate errors

Strong security in any environment

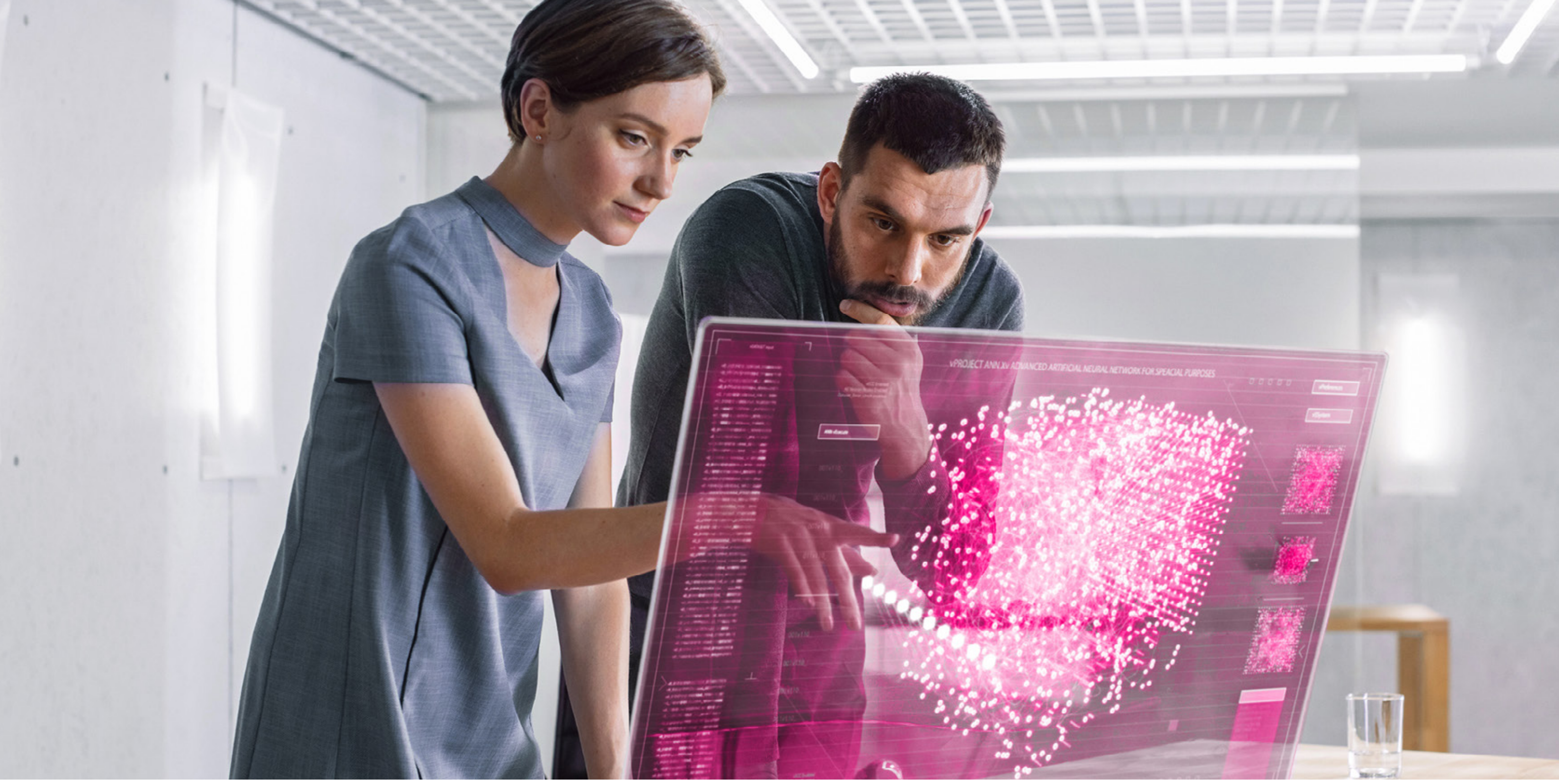
- Control communications at both the network and process level on Windows and Linux
- Investigate policy violations and detect breaches faster with integrated data from multiple attack methods
- Ensure security regardless of potential operating system limitations

Network segmentation has been a staple of IT security for decades. In complex hybrid & multi-cloud architectures, it must be possible to implement security measures at both the workload and process level. Guardicore Centra provides a simple workflow from mapping application dependencies to proposing and setting rules so that any impacts are visible before being applied to traffic.

SD microsegmentation stands for:

- Maximum visibility using a visual map of how applications communicate with each other.
- AI-powered: Prioritization of business-critical applications and implementation of segmentation policies with just a few clicks
- Full visibility into security risks and possibility of intervention by adjusting the segmentation rule
- Faster and easier segmentation using a flexible allow and deny list model that results in timely risk mitigation with few rules
- Broad applicability and protection of critical resources, regardless of where they are deployed or accessed from
- Comprehensive detection of dynamic deception and security breaches and violations, e.g., through reputation analysis and threat intelligence firewall
- Mandatory enforcement of centrally imposed policies and a granular set of rules at the process level
- Faster deployment and management with zero downtime
- Broad usability for many legacy systems, including Windows 2003, CentOS 6, RHEL5, and AS400

T Systems Let's power higher performance


vPROJECT ANN.Xv ADVANCED ARTIFICIAL NEURAL NETWORK FOR SPEACIAL PURPOSES

The solutions at a glance

SD microsegmentation services can be successfully implemented in just three simple steps:

1. Transparency: Identify and map the relationships between applications

2. Concept: Design, test, and deploy policies in record time

3. Implementation: Security in any environment

AI labeling and policy suggestions

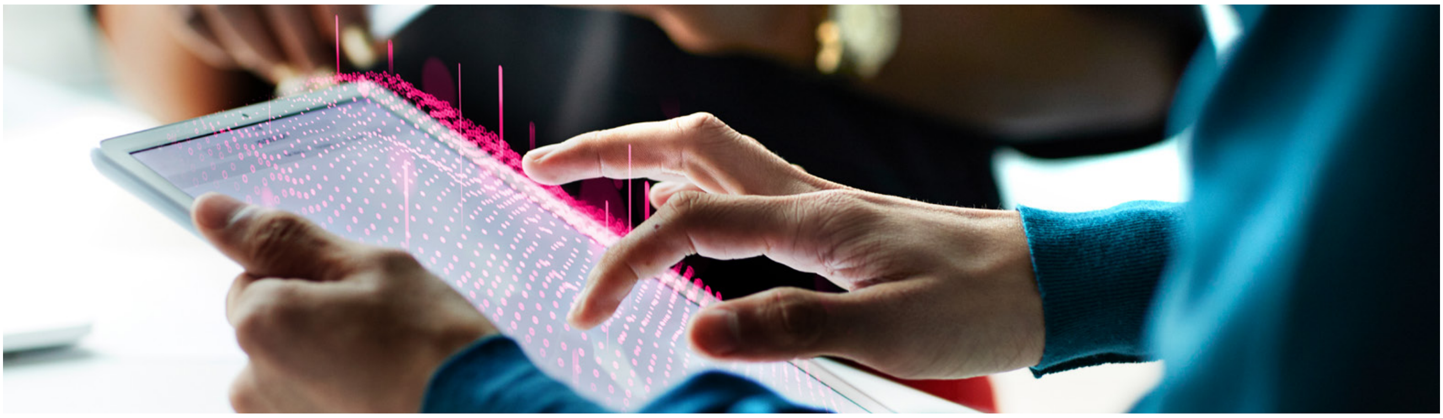
Asset mapping and policy enforcement are two stages of effective segmentation. Automated machine learning technologies can be used to bypass asset mapping, resulting in even faster implementation. This uses detected communication relationships and traffic patterns that have been analyzed as dangerous and/or redundant to generate automated suggestions for the most effective policies.

Introducing SD microsegmentation services into hybrid & multi-cloud environments

The concept of network segmentation has become firmly established. But the security model reaches its limits when it comes to dynamic infrastructures – especially in scalable cloud environments when workloads move between segments and communicate. When cloud services are deployed, there is an increased risk that an attack will not only have been successful at one point in the IT infrastructure before it is detected. It must be possible to combat the attack in real time, and also to limit it to one segment in order to prevent damage to other apps and workloads in the company's own data centers and cloud services. SD microsegmentation services can also be used to increase the security of complex cloud services and control them from a single dashboard for all applications.

Comprehensive protection through complete coverage

SD microsegmentation services can be deployed for any application in any environment – whether it be a public, private, or hybrid cloud service, or an on-premise or hosted service



Vollständige Transparenz als Basis für Segmentierungsregeln

In order to manage the multiple communication relationships involved in application usage, these must be captured and understood. With the SD microsegmentation service, the usage of services that have been used for many years can be made transparent and access rights can be identified that may no longer be desired. Finally, segmentation rules can be created that correspond to user requirements or application dependencies. The central management makes it possible to intervene at any time and to expand any adaptation requirements that arise at short notice.

Control based on granular policies

As the complexity of the infrastructure increases, it must be possible to control data flows in an increasingly granular and detailed manner. The goal of the approach is to securely shield each microsegment from unauthorized data flows. This requires, for example, the definition of access and usage rights for each application. In this way, communication relationships between and within microsegments can be efficiently controlled, according to uniform rules.

With the Guardicore SD microsegmentation service from Akami, policies can be quickly developed and deployed. Users can immediately customize the configuration using the central dashboard. Predefined templates enable a rapid initial implementation, for example in the event of an attack. After the attack has been averted, the configuration can be adapted to meet individual needs.

With the microsegmentation tool, rules can be defined and enforced at the “process level” for the strict control of the processes between the application components. This leads to an optimal level of security.

That’s why you can trust us!

For years, T-Systems has maintained a successful partnership with Akamai, the majority owner of Guardicore. We advise numerous well-known companies on content delivery, web performance, and web security. The importance of Internet-based business processes is growing steadily, and more and more applications are being provided as cloud services. Akamai’s edge services are an excellent fit with T-Systems’ cloud strategy. The services of the delivery platform offer high-performance services worldwide, which are supplemented by leading cloud security services and at the same time relieve customer infrastructures. This creates an outstanding experience for our customers and their users.

DO YOU HAVE QUESTIONS?
0800 33 09030

VISIT US:
www.t-systems.com/de/de

PUBLISHER
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Germany

T Systems Let’s power higher performance