

Software Defined Network Segmentation

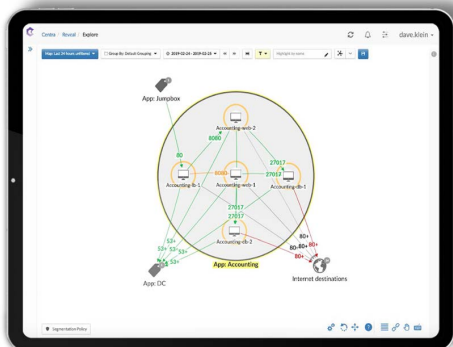
Enterprise IT infrastructure is still evolving from traditional on-premises data centers to cloud and hybrid cloud architectures, with a blend of platforms and application deployment models. Although this digital transformation is helping many organizations achieve greater business agility, reduce infrastructure costs, and enable remote work, it is also creating a larger and more complex attack surface that does not have a well-defined perimeter.

Each individual server, virtual machine, cloud instance, and endpoint is now a possible point of exposure; and with the prevalence of threats like ransomware and zero-day vulnerabilities, attackers are becoming more adept at moving laterally toward high-value targets when—not if—they find a way in.

Akamai Guardicore Segmentation provides the simplest, fastest, and most intuitive way to enforce Zero Trust principles within your network. We stop lateral movement by visualizing activity within your IT environments, implementing precise microsegmentation policies, and detecting possible breaches quickly.

Adaptive Security That Self-Tunes

Akamai Guardicore Segmentation collects detailed information about an organization’s IT infrastructure through a mix of agent-based sensors, network-based data collectors, virtual private cloud flow logs from cloud providers, and integrations that enable agentless functionality. Relevant context is added to this information through a flexible and highly automated labeling process that includes integration with existing data sources, such as orchestration systems and configuration management databases.



BENEFITS FOR YOUR BUSINESS

Granular, AI Powered Segmentation

Protect all your websites, applications, and APIs from a broad range of threats, including volumetric DDoS, automated botnets, and injection and API-based attacks, among others, from a single WAAP solution.

Real-Time and Historical Visibility

Maintain strong security with automatic updates and alleviate alert fatigue with automatic self-tuning to help security teams focus on investigating real attacks and not chasing false alerts.

Broad Platform Support

Maximize your security investment with a solution that includes web application and API protections, bot visibility and mitigation, DDoS protection, SIEM connectors, web optimization, edge compute, API acceleration, and more.

Flexible Asset Labeling

Add rich context with a customizable labeling hierarchy and integration with orchestration tools and configuration management databases.

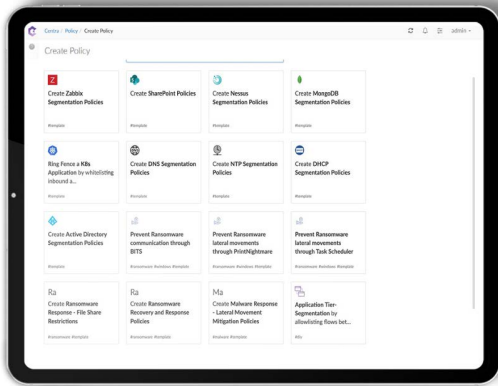
Multiple Protection Methods

Integrate threat intelligence, defense and breach detection capabilities to reduce incident response time.



Network Map

The output is a dynamic map of the entire IT infrastructure that allows security teams to view activity with user- and process-level granularity on a real-time or historical basis. These detailed insights, combined with AI-powered policy workflows, make the creation of segmentation policies fast, intuitive, and based on real workload context.



Templates

Policy creation is made easy with prebuilt templates for the most common use cases. Policy enforcement is completely decoupled from the underlying infrastructure, so security policies can be created or altered without complex network changes or downtime. In addition, policies follow the workload no matter where it resides — in on-premises data centers or public cloud environments. Our segmentation capabilities are complemented by a sophisticated set of threat defense and breach detection capabilities, as well as threat hunting services provided by Akamai Threat Labs.

Comprehensive Protection at Scale

Any Environment

Protect workloads in complex IT environments with a combination of on-premises workloads, virtual machines, legacy systems, containers and orchestration, public/private cloud instances, and IoT/OT

Simplify Security

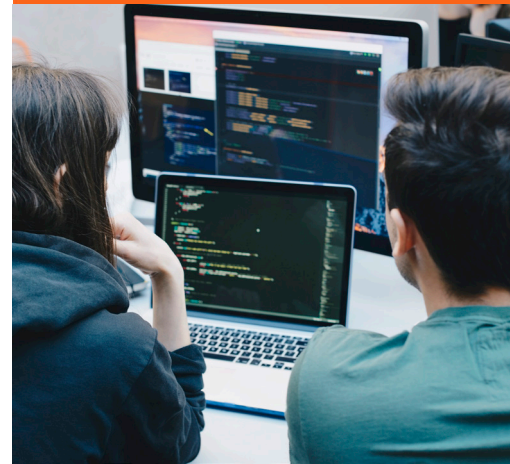
Simplify security management with one platform that provides network visualization, segmentation, threat defense, breach detection capabilities, and guided policy enforcement for Zero Trust initiatives

Enterprise Scalability and Performance

Start with focused protection of your most critical digital assets and scale up to protect your full enterprise without complexity, infrastructure changes, or performance bottlenecks

Supported Platforms and Technologies

- » We are designed to integrate with your existing infrastructure
- » Our OS support expands continuously with our customers' needs
- » Click here for a complete list of our integrations and technology partners



Akamai Select Partnership

Akamai's portfolio of advanced security and video delivery solutions is backed by Evolane's unparalleled customer service, analytics and 24/7 monitoring. Founder Kristof Haeck worked together with Akamai throughout his career and got to know the platform in all its facets. As someone who only chooses who and what he believes in, it didn't take long for Kristof to become an Akamai Select Partner to continue the successes.

This title is reserved for partners who continue to invest to provide the right product knowledge and product configuration! With more than 15 years of experience with Akamai's solutions, our engineers are now as certified as can be and we got to do some great projects for amazing companies. This is how Evolane combines the benefits of a trusted local partner with the ingenious technology of an international company.

To learn more, [click here](#) and visit our Akamai partnerpage on the Evolane website.



info@evolane.eu