Enterprise IT infrastructure continues to evolve 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. It is designed to stop lateral movement by visualizing activity within your IT environments, implementing precise microsegmentation policies, and detecting possible breaches quickly.

Key solution capabilities

**Granular, AI-powered segmentation**
Implement policies in a few clicks using AI recommendations, templates for remediating ransomware and other common use cases, and precise workload attributes like processes, users, and domain names

**Real-time and historical visibility**
Map application dependencies and flows down to the user and process levels on a real-time or historical basis

**Broad platform support**
Cover modern and legacy operating systems across bare-metal servers, virtual machines, containers, IoT, and cloud instances

**Flexible asset labeling**
Add rich context with a customizable labeling hierarchy for visibility and enforcement, and integration with orchestration tools and configuration management databases for automated labeling

**Multiple protection methods**
Integrate threat intelligence, defense, and breach detection capabilities to reduce incident response time

**BENEFITS TO YOUR BUSINESS**

- Prevent ransomware
- Achieve Zero Trust
- Accelerate compliance
- Ringfence critical applications
- Secure cloud migrations
- Safeguard remote workforce
- Protect endpoints
- Move beyond internal firewalls
How it works

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.

**Infrastructure topology**

Most customers utilize SaaS management, but on-premises management options are also available.

**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 pre-built 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 by Akamai Hunt, our managed threat hunting service.
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

Simplified 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

- Akamai Guardicore Segmentation is designed to integrate with your existing infrastructure.
- Our OS support expands continuously with our customers’ needs.
- Check out our technology partners page for a complete list of our integrations.

Operating systems

- Linux
  - SUSE
  - CentOS
  - Red Hat
  - Debian
  - Amazon Linux
  - Oracle Linux
  - Ubuntu

- Unix
  - AIX
  - Oracle Solaris
  - FreeBSD
  - HP-UX

Public cloud providers

- AWS
- Microsoft Azure
- Google Cloud

Hypervision orchestration

- VMware vCenter
- VMware vsphere
- VMware ESXi
- VMware App枯燥
- Citrix XenServer
- OpenStack
- Mirantis
- Docker

Security gateways

- Cisco
- Palo Alto
- Check Point

Container orchestration and engines

- Docker
- Kubernetes
- Red Hat OpenShift

Memory and system minimum requirements

<table>
<thead>
<tr>
<th></th>
<th>Management Server</th>
<th>Aggregator</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 GB RAM, 8 vCPUs, 530 GB</td>
<td>4 GB RAM, 4 vCPUs, 30 GB</td>
<td></td>
</tr>
<tr>
<td>32 GB RAM, 8 vCPUs, 100 GB</td>
<td>ESC Collector</td>
<td></td>
</tr>
<tr>
<td>2 GB RAM, 2 vCPUs, 30 GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API

For more information about Akamai Guardicore Segmentation, or to request a personalized product demo, visit akamai.com/guardicore.