Akamai Guardicore Segmentation

Stop Lateral Movement with Granular Visibility and Microsegmentation Controls

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.

USE CASES

- **Prevent Ransomware**
- **Secure Cloud Migration**
- **Achieve Zero Trust**
- **Safeguard Remote Workforce**
- **Accelerate Compliance**
- **Protect Your Endpoints**
- **Ring-fence Critical Applications**
- **Replace Internal Firewalls**

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 and integration with orchestration tools and configuration management databases

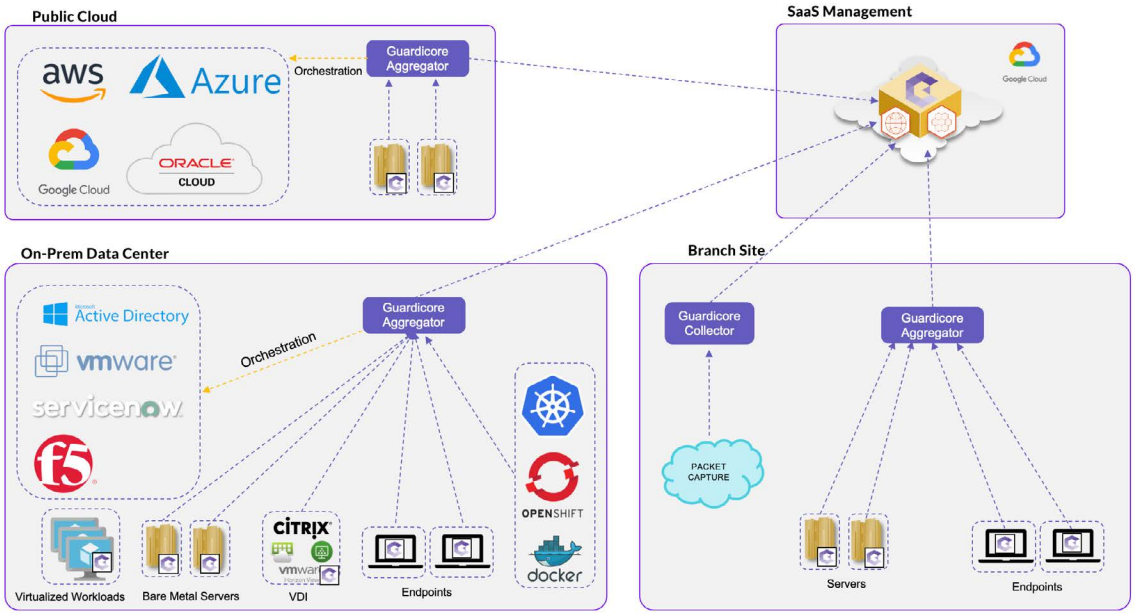
Multiple Protection Methods

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

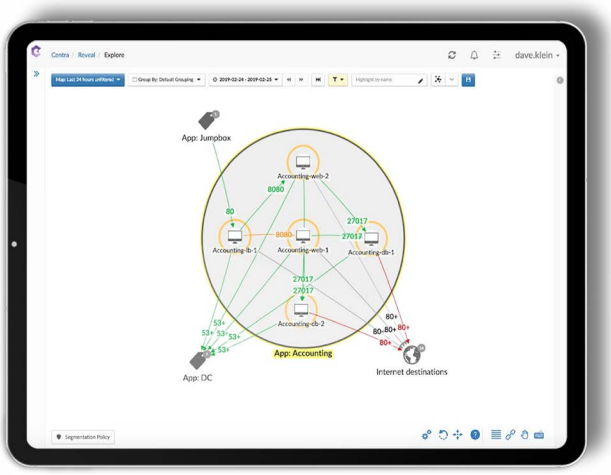
How It Works

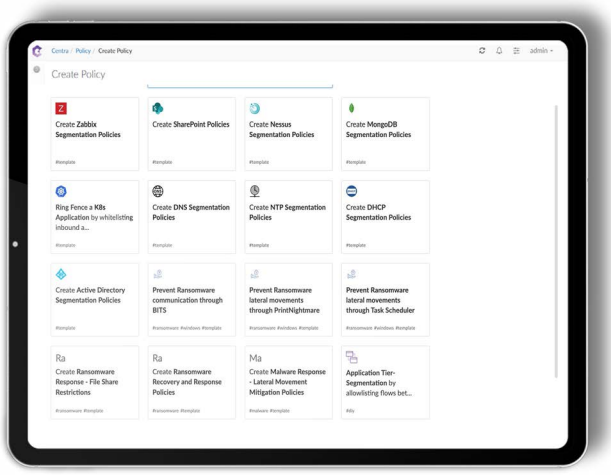
Akamai Guardicore Segmentation collects detailed information about an organization's IT infrastructure through a mix of agent-based sensors, network-based data collectors, virtual private cloud flow logs from cloud providers, and integrations that enable agentless functionality. Relevant context is added 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-premise 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 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

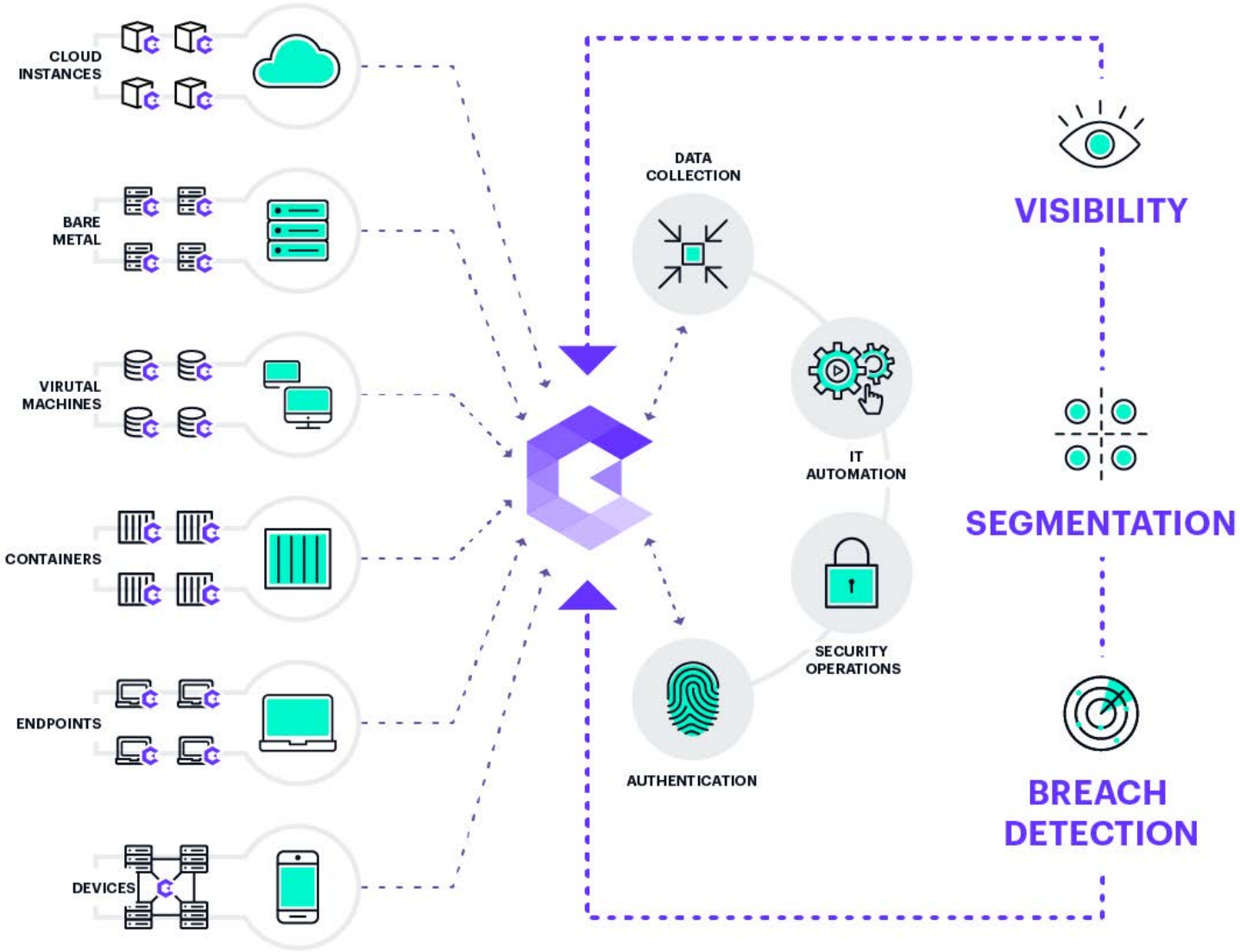
Protect workloads in complex IT environments with a combination of on-premises workloads, virtual machines, legacy systems, containers and orchestration, public/private cloud instances, and IoT/OT

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



Our holistic solution combines key capabilities required for achieving Zero Trust within your IT environment.

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

OPERATING SYSTEMS

Linux

SUSE, CentOS, Red Hat, debian, aws, aws 2, ORACLE LINUX, ubuntu

Apple

Microsoft

Windows Server, Windows

UNIX

AIX, ORACLE SOLARIS, FreeBSD, hp UX

PUBLIC CLOUD PROVIDERS

aws, Microsoft Azure, ORACLE, Google Cloud

HYPERVISORS

KVM, CITRIX XenServer, VMware ESXi, vSphere Hypervisor, NUTANIX, AHV, Hyper-V

HYPERVISOR ORCHESTRATION

vCenter Server, vSphere, NSX, apachecloudstack open source cloud computing, openstack., MIRANTIS, nuagenetworks From Nokia

SECURITY GATEWAYS

cisco, paloalto NETWORKS, CHECK POINT

CONTAINER ORCHESTRATION AND ENGINES

docker, kubernetes, Red Hat OpenShift

BROWSERS FOR WEB CONSOLE

MEMORY AND SYSTEM MINIMUM REQUIREMENTS

Management Server
32 GB RAM, 8 vCPUs, 530 GB

Aggregator
4 GB RAM, 4 vCPUs, 30 GB

Deception Server
32 GB RAM, 8 vCPUs, 100 GB

ESC Collector
2 GB RAM, 2 vCPUs, 30 GB

Protection across any complex environment.
Guardicore.com

INTELLIGENCE-SHARING EXPORT PROTOCOLS

STIX, Syslog, SMTP, CEF, Open REST API