AKAMAI SOLUTION BRIEF

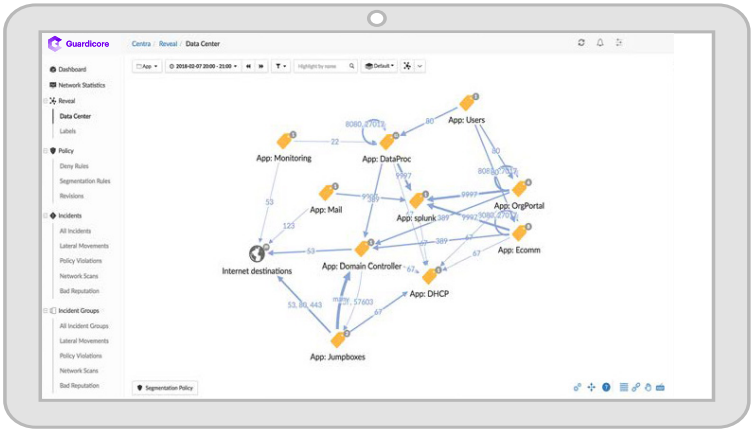
Rapid Microsegmentation in Hybrid Environments with Akamai Guardicore Segmentation

The path to implementing microsegmentation isn't a straight line; there are many twists and turns as you begin to discover, understand, and control the application flows in your IT environment. But without the right approach to navigating the path, you can encounter several challenges along the way. Network blind spots often prevent sufficient discovery and communication mapping of applications, workloads, and underlying processes. Rigid policy engines can force sweeping decisions, which run the risk of breaking applications. Inconsistent policy expression across operating systems can result in dangerous security gaps. Finally, complex — and often manual — integrations of policy violation data with breach detection tools can slow down incident investigation and response. Akamai Guardicore Segmentation helps you successfully navigate the path to microsegmentation in three steps.

Step 1: Reveal

Automatically discover applications and visualize flows

Akamai Guardicore Segmentation features best-in-class visibility that automatically discovers and visualizes all applications, workloads, and communication flows with process-level context, no matter where they reside. You'll have the same view for assets that are on-premises, in the cloud, across multiple clouds, and more. This visualization, coupled with automatic importation of orchestration metadata, enables your security teams to quickly and easily label and group all assets and applications, streamlining policy development.



Secure critical applications wherever they reside

Platform agnostic

Akamai Guardicore Segmentation can visualize assets and enforce security policy across infrastructures: on-premise, in the cloud, and across multiple clouds

Quick time to policy

Automated rule suggestions, a flexible policy engine, and an intuitive user interface all make policy creation and enforcement less time-consuming

Integrated breach detection and response

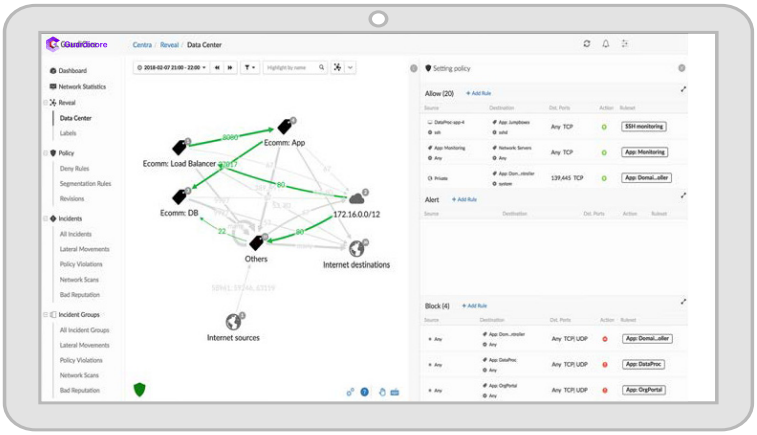
Visualize policy violations and quickly respond to active threats, protecting your most critical assets no matter where they reside

Akamai

Step 2: Build

Quickly design, test, and deploy policies

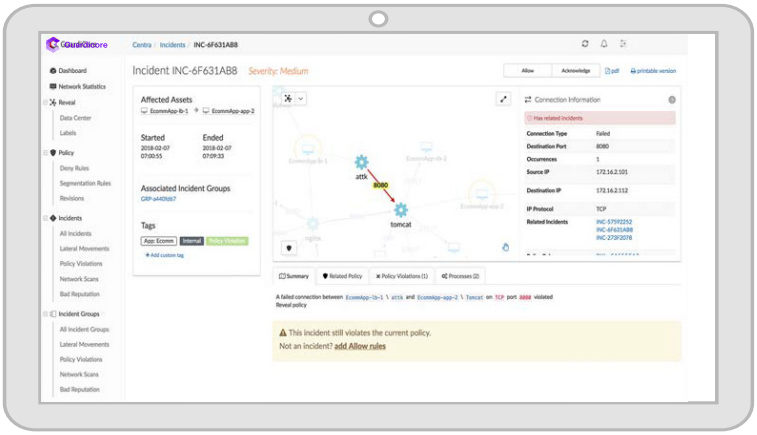
Akamai Guardicore Segmentation simplifies microsegmentation policy development and management. A single click on a communication flow in the Reveal map generates automated rule suggestions based on historical observations, enabling you to quickly build a strong policy. An intuitive workflow and a flexible policy engine supports continuous policy refinement and reduces costly errors.



Step 3: Enforce

Provide strong security in any environment

With the ability to enforce communication policy at the network and process level across systems, Akamai Guardicore Segmentation maintains security regardless of operating system enforcement limitations. Also, integrated breach detection and response capabilities enable you to see policy violations in the context of an active breach, enabling you to quickly identify the method of attack and remediate it.



Please visit akamai.com/guardicore for more information.

 | Support | | Published 06/23