AKAMAI SOLUTION BRIEF

Multi-Method Breach Detection Spotlight: Using Segmentation Policies for Data Center Breach Detection

With data center breaches showing no signs of abating, it's time for security teams to focus more attention on the heart of the data center, where applications are talking to one another and performing mission-critical functions. As more organizations increasingly distribute data center assets across multiple virtualized environments, perimeter defenses are no longer adequate. Security administrators need an efficient means of securing internal east-west traffic from attacks that have already succeeded in breaching perimeter defenses.

Firewalling hits a wall

Firewalls have traditionally been used to secure communications in and out of data centers. However, placing firewalls at the core of the data center is problematic. Unable to adapt to massive amounts of east-west traffic, they become a bottleneck to performance. Firewalling at the server level consumes large amounts of compute resources from the host, which is already highly taxed. It also requires deploying multiple solutions to span the many different types and brands of operating systems in the data center, making management difficult.

Until recently, implementing security policies at the L7 process level has been a challenge as well. That's because it requires having visibility into all applications and processes communicating in your environment. It further demands a holistic understanding of how processes should function together within the application and the data center. Without those insights, implementing process-level security policies can be risky, and the chances of breaking something are greatly elevated.

To protect critical assets in the data center, while simultaneously improving breach detection and response, security teams need the means to:

- Visualize all the applications and processes running in their data centers in real time
- Implement granular security policies without impeding critical processes
- Detect unauthorized communications that may indicate a breach

The best defense is offense: Policy-based detection with Akamai Guardicore Segmentation

Policy-based detection can help security teams more quickly detect, confirm, and contain threats to prevent damage and minimize losses. These granular security controls do double duty, preventing an intruder from gaining malicious access to an application or process while simultaneously alerting administrators to the intruder's presence.

The segmentation policies' capabilities within Akamai Guardicore Segmentation enable security practitioners to:

- Generate a comprehensive visual map of all applications and activity inside the data center, allowing visibility into all workloads and a full understanding of application-layer communications

Multiple detection methods detect breaches faster

Dynamic deception

A redirection architecture and dynamically generated live environments engage attackers and identify their methods without disrupting data center performance

Policy-based detection

Security policies at the Layer 4 network and Layer 7 process levels enable instant recognition of unauthorized communications and noncompliant traffic

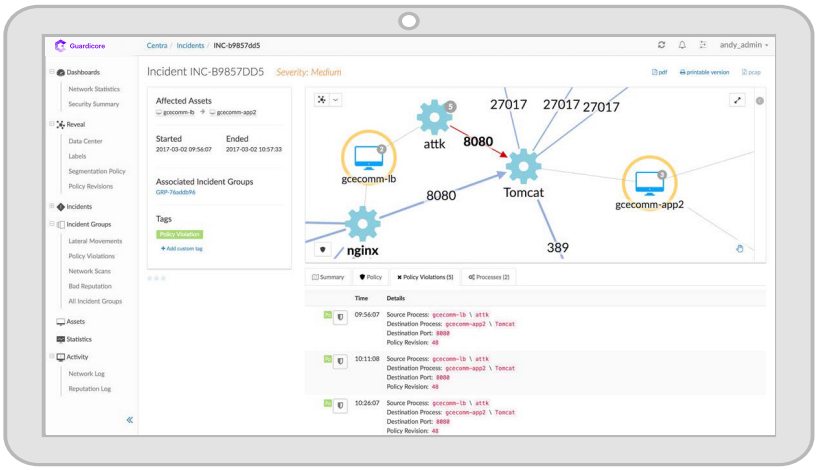
Reputation analysis

Detects suspicious domain names, IP addresses, and file hashes within traffic flows, providing comprehensive breach detection

Akamai

- Filter and organize applications into groups and label them for the purpose of setting common security policies — for example, all applications related to a particular workflow or business function
- Define and create rules governing authorized communications between applications
- Test and refine those rules to ensure they are not disrupting normal authorized traffic

Any noncompliant traffic, unauthorized communication, or other policy violation automatically triggers an alert indicating an intruder may be present. This in turn initiates the investigative process to confirm and contain the threat.



Akamai Guardicore Segmentation detects a potential breach by recognizing and alerting on segmentation policy violations involving unauthorized processes attempting to communicate on authorized ports between two permitted hosts.

Corner your adversaries with multiple detection methods

Policy-based detection is just one of several methods our solution uses to improve real-time breach detection and response. Working in conjunction with one another, these complementary methods also include:

- **Dynamic deception**, which employs real data center servers, IP addresses, operating systems, and services as decoys that actively seek out suspicious activity at the first indication, engage with it, and redirect it to a containment area for threat confirmation and investigation
- **Reputation analysis**, which leverages Akamai's global network of threat sensors and intelligence feeds to identify negative processes and suspicious IP addresses, domain names, or file hashes associated with threats

Deploying these three methods simultaneously forms a strong security net, virtually ensuring that any live breach in the data center is caught, mitigated, and contained for in-depth investigation.

Learn more about Akamai Guardicore Segmentation's comprehensive breach detection capabilities at akamai.com/guardicore.

 | Support | | Published 06/23