AKAMAI SOLUTION BRIEF

Tenable Vulnerability Management for Akamai Guardicore Segmentation

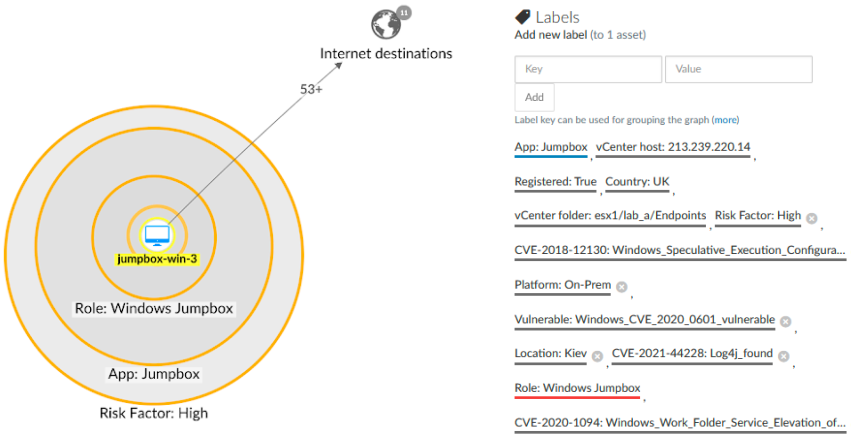
Take action on vulnerabilities in your organization with risk-based segmentation

Tenable provides a risk-based view of the entire attack surface — from IT to the cloud to containers. With this insight, organizations can quickly identify and investigate areas where risk reduction is critical.

This powerful vulnerability management data can now be brought into Akamai Guardicore Segmentation. Using the integrated solution, customers can label assets with relevant Common Vulnerabilities and Exposures (CVE) and risk scores, and then use the data to automatically block unwanted traffic and create more informed segmentation policies.

Identify and remediate risk with Tenable and Akamai

- The integration with Tenable.io and Tenable.sc is bidirectional, which allows tags to be added or removed based on the remediation status in Tenable
- Additionally, asset data discovered by Akamai Guardicore Segmentation (but not yet not configured in Tenable) will be made available for scanning
- Using Akamai Guardicore Segmentation with Tenable.io or Tenable.sc, organizations can identify, prioritize, and quickly address risks, improving their security posture



CVE labels shown on a specific asset in the environment

Using data from Tenable, Akamai Guardicore Segmentation quickly discovers all vulnerable assets in the network, whether it is an on-prem server, an application running in the cloud, a container, or an end-user device. The user can then easily isolate the affected assets from the rest of the environment until the appropriate remediation is completed.

For more information or to see a demo, please contact esg-bd@akamai.com

Key integration benefits

Continuous visibility
Automatically sync and continuously track known and unknown assets with their associated vulnerabilities

Prioritized security activities
Combine vulnerability data from Tenable, threat intelligence, and data science for easy-to-understand risk scores

Risk-based remediation
Create informed segmentation policies based on rich vulnerability data

Technology components

- Tenable.io
- Tenable.sc
- Akamai Guardicore Segmentation

 | Support | Published 02/23