



## Tenable.io Vulnerability Management for Guardicore Centra

Take action on vulnerabilities in your organization with a risk-based approach for segmentation.

Tenable.io provides security stakeholders with a risk-based view of their organization's 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 the Guardicore Centra Security Platform seamlessly via a plug-in. Using the integrated solution, organizations can label assets in Guardicore with relevant Common Vulnerabilities and Exposures (CVE) and risk scores.

Then, security teams can use the new risk-based data to quickly create informed segmentation policies that block traffic or generate an alert.



Continuously track known and unknown assets and their vulnerabilities, so you can identify threats and unexpected network changes before they become breaches.



### Key Benefits

- Continuous visibility**  
 Automatically and continuously track known and unknown assets and their vulnerabilities.
- Prioritize security activities**  
 Combine vulnerability data, threat intelligence, and data science for easy to understand risk scores.
- Risk-based remediation**  
 Create informed segmentation policies based on rich vulnerability data.

The screenshot shows the 'Policy Rules' configuration page in Guardicore Centra. The interface includes a search bar, filters, and a table of rules. A tooltip is displayed over the 'Labels' column of the first rule, showing 'Risk Factor: High & Compliance: PCI' and 'High PCI'.

| Section | Source              | Destination         | Ruleset  | Hits | Author  | Comments | Created          | Modified         | ID           | Enabled   |
|---------|---------------------|---------------------|----------|------|---------|----------|------------------|------------------|--------------|-----------|
| Alert   | C:\Windows\stsc.exe | Any                 | Risk_Hon | 0    | sharonb |          | 2021-02-10 15:09 | 2021-02-11 15:09 | RUL-704CD857 | Unchanged |
| Block   | * Any               | C:\Windows\ntfs.exe | Risk_Hon | 0    | sharonb |          | 2021-02-10 14:57 | 2021-02-11 15:09 | RUL-4D390D96 | Unchanged |
| Block   | CVE-2021-24078      | * Any               | Risk_Hon | 5K   | sharonb |          | 2021-02-10 14:55 | 2021-02-11 15:09 | RUL-65D34972 | Unchanged |

Create and manage segmentation policies based on risk factor.

