VULNERABILITY MANAGEMENT

SOLUTION BRIEF

PICUS ATTACK SURFACE VALIDATION AND QUALYS VULNERABILITY MANAGEMENT INTEGRATION

JOINT SOLUTION BENEFITS

✔ **Unified Defense Posture**
The integration of Picus ASV with Qualys Vulnerability & Configuration Management creates a unified defense mechanism. This cohesive approach enables organizations to comprehensively manage and mitigate vulnerabilities, enhancing their overall cybersecurity resilience.

✔ **Continuous Asset Visibility**
Stay ahead of evolving IT landscapes and emerging threats with continuous discovery and analysis of assets. This integration empowers organizations to proactively monitor their attack surface, ensuring readiness against cyber risks.

✔ **Efficient Asset Management**
By enriching Picus ASV's Asset Library with data from Qualys Vulnerability & Configuration Management, the integration simplifies the management of diverse asset types and vulnerabilities. This centralized approach enhances efficiency and supports informed decision-making.

✔ **Enhanced Search Capabilities**
Leverage advanced search features within Picus ASV to quickly locate specific assets or vulnerabilities. This capability ensures timely responses to emerging threats in today's dynamic cybersecurity environment.

✔ **Proactive Vulnerability Visibility**
Gain a proactive edge in vulnerability management with comprehensive visibility into potential threats. This integration empowers organizations to act swiftly and effectively.

Enhancing Cybersecurity With Picus Attack Surface Validation and Qualys Vulnerability Management

In today's dynamic cybersecurity landscape, organizations continuously face challenges in identifying and mitigating vulnerabilities across their digital infrastructure. This solution brief highlights the integration of Picus Attack Surface Validation (ASV) with Qualys Vulnerability & Configuration Management, a leading solution in vulnerability assessment and management. This partnership empowers security teams with actionable insights and unparalleled visibility into their security risks, enabling them to proactively protect digital assets.

Qualys Vulnerability & Configuration Management provides comprehensive insights into an organization's security posture. When integrated with Picus ASV, its capabilities are significantly enhanced through advanced attack surface validation and risk prioritization. This powerful combination enables organizations to move beyond simple vulnerability detection, empowering them to address risks with efficiency.



HOW IT WORKS

1. Picus ASV connects to Qualys Vulnerability & Configuration Management via an API, facilitating a direct link that enables the continuous discovery and assessment of assets and vulnerabilities.

2. Collected data is normalized and aggregated within the Picus interface, presenting users with a comprehensive view of their assets and vulnerabilities for effective management.

3. The integrated data enables users to conduct in-depth searches and gain valuable insights, empowering them to make informed decisions about prioritizing and mitigating vulnerabilities.

ABOUT PICUS

At Picus Security, our priority is making it easy for security teams to continuously validate and enhance organizations' cyber resilience.

Our Complete Security Validation Platform simulates real-world threats to automatically measure the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities.

As the pioneer of Breach and Attack Simulation, our people and technology empower customers worldwide to be threat-centric and proactive.

Experience Picus *in Action*

GET A DEMO

Gartner Peer Insights Customers' Choice 2024

Highest Rated Vendor

4.8/5

Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024

GARTNER is a registered trademark and service mark, and the GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge and PEER INSIGHTS are trademarks and service marks, of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

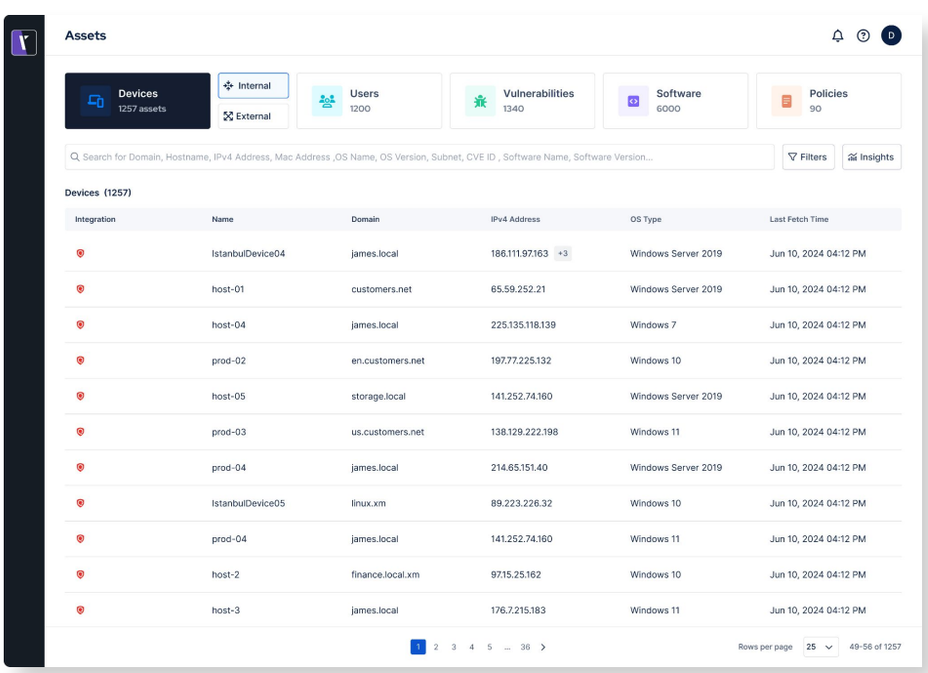
© 2024 Picus Security. All Rights Reserved.

All other product names, logos, and brands are property of their respective owners in the United States and/or other countries.

INTEGRATION OVERVIEW

The Picus Attack Surface Validation (ASV) and Qualys Vulnerability & Configuration Management integration equips organizations with robust tools to navigate the complexities of modern cybersecurity threats. This integration enables the seamless management of vulnerabilities while providing real-time, actionable insights into the organization's environment. By merging real-time vulnerability data with attack surface insights, the integration allows for a deeper understanding of risks, empowering organizations to adopt a more proactive and threat-centric approach.

This integration helps organization to manage their vulnerabilities and mitigation by correlating vulnerability data with operational contexts, organizations can prioritize remediations based on criticality, reducing the time to address high-risk exposures. Furthermore, automated workflows enabled by the integration allow for faster incident response and reduced manual effort, helping security teams focus on strategic initiatives while maintaining a strong security posture.



THE PICUS PLATFORM

Picus Security Validation Platform simulates cyber threats to consistently validate, measure and enhance organizations' cyber resilience. It facilitates a more proactive and threat-centric approach to security by automatically evaluating the effectiveness of security controls, identifying high-risk attack paths, and helping to optimize threat prevention and detection capabilities.

Why is security validation important?

- Controls don't perform out-of-the-box and must be customized.
- New threats mean that security tools can lose their effectiveness.
- Infrastructure drift creates weaknesses that can go unaddressed.
- Pen testing is vulnerability-focused and quickly out of date.
- Boards, auditors & insurers want evidence of security effectiveness.