DATASHEET

SECURITY CONTROL VALIDATION FOR PREVENTION CONTROLS

Maintaining prevention controls to ensure that they block cyber-attacks is an essential responsibility of every security team. However, the time and effort required to update tools on an ongoing basis can be seriously resource-intensive and an inability to make swift configuration changes can easily lead to data breaches. In some cases, tools may also fail to provide the level of protection expected.

By simulating real-world cyber threats, **Picus Security Control Validation** validates the effectiveness of your organization's network, endpoint and email controls on a continuous basis.
Supplying actionable mitigation recommendations, the platform also helps to alleviate the pressure of keeping them optimized **24/7.**

With **Picus SCV**, **automatically validate** the effectiveness of:

- ✓ Firewalls and Next-Gen Firewalls (NGFW)
- ✓ Secure Web Gateways (SWG)
- ✓ Data Loss Prevention (DLP)
- ✓ Endpoint Protection Platforms (EPP)
- ✓ Email (ES) and Network Sandboxes (NS)
- ✓ Web Application Firewalls (WAF)
- ✓ Secure Email Gateways (SEG)
- ✓ Intrusion Prevention Systems (IPS)
- ✓ Antivirus (AV)
- ✓ URL Isolation (URL)

HOW PICUS SCV OPTIMIZES THREAT PREVENTION

Continuously identifies policy weaknesses

Picus identifies attacks that are missed by your prevention controls, enabling you to identify threats which could pose a risk and take action to mitigate them.

Identifies environmental drift

As your IT infrastructure grows, validate that your security controls are providing sufficient protection and not leaving assets exposed.

Facilitates swiftlier mitigation of gaps

To reduce the time and effort required to tune your security controls, Picus supplies vendor-specific prevention signatures.

Provides a holistic view

To help measure security effectiveness, Picus generates security scores for controls on both an individual and collective basis.

Maps results to frameworks

Picus maps assessment results to the MITRE ATT&CK Framework, enabling you to visualize threat coverage and prioritize the mitigation of gaps.

Integrates with the latest tools

For a deeper level of validation, Picus integrates with the latest toolsets and streamlines workflows by automating the application of mitigation content.

VALIDATE YOUR DEFENCES AGAINST THE LATEST THREATS

To ensure that your prevention controls are effective at blocking the latest threats, The Picus Platform's Threat Library of over **3,800 threats and 19,000 actions*** is updated daily by a team of experts.

New threats are added to the library within 24 hours of disclosure and are mapped to MITRE ATT&CK, OWASP, CVE and CWE references, as well as target applications and operating systems.

The types of threats Picus Security Control Validation can simulate includes:

→ Malware Attacks
Determine the readiness of your organization's controls to prevent the latest malware and ransomware.

→ Email Attacks
Validate the effectiveness of your controls to block malicious links and attachments.

→ Endpoint Attacks
Validate that scenario attacks from threat groups, including APTs, are prevented by endpoint security controls.

→ Vulnerability Exploitation Attacks
Understand how effective your security controls are at blocking local and remote code exploitation.

→ Web Application Attacks
Gauge if your defenses are capable of blocking code injection, denial of service and brute force attacks.

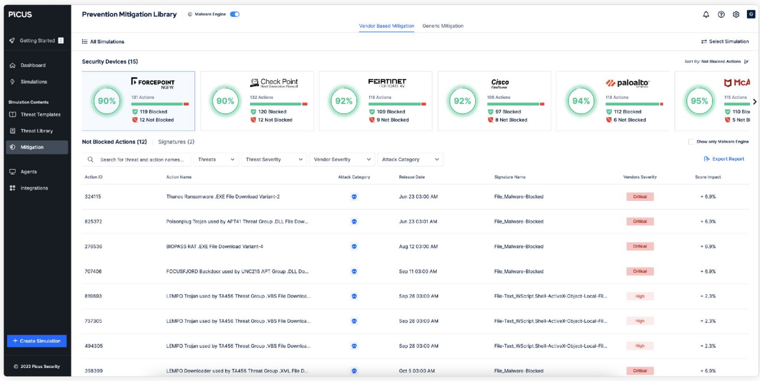
→ Data Exfiltration Attacks
Assess whether your defenses can prevent the exfiltration of sensitive personal and financial information over HTTP/S.

→ Cloud Attacks
Proactively identify and address security threats specific to your cloud infrastructure by simulating real world attacks.

*Each threat consists of one or multiple actions. An action corresponds to a specific procedure required for a threat to achieve an objective.

THE INSIGHTS YOU NEED TO QUICKLY CLOSE GAPS AND DEMONSTRATE ASSURANCE

To enable the effectiveness of your prevention capabilities to be benchmarked and measured on an ongoing basis, Picus Security Control Validation provides individual and collective performance metrics for each of your controls.



Prevention Mitigation Library

Security Devices (15)

FORCEPOINT NGFW	Check Point Next Generation Firewall	FORTINET FORTIGATE AV	Cisco FirePower	paloalto	McA
90%	90%	92%	92%	94%	95%
131 Actions	132 Actions	118 Actions	105 Actions	118 Actions	115 Actions
119 Blocked	120 Blocked	109 Blocked	97 Blocked	112 Blocked	110 Blo
12 Not Blocked	12 Not Blocked	9 Not Blocked	8 Not Blocked	6 Not Blocked	5 Not Bl

Not Blocked Actions (12) | Signatures (2)

Search for threat and action names... | Threats | Threat Severity | Vendor Severity | Attack Category

Action ID	Action Name	Attack Category	Release Date	Signature Name	Vendors Severity	Score Impact
324115	Thanos Ransomware .EXE File Download Variant-2	●	Jun 23 03:00 AM	File_Malware-Blocked	Critical	+ 6.9%
825372	Poisonplug Trojan used by APT41 Threat Group .DLL File Dow...	●	Jun 23 03:01 AM	File_Malware-Blocked	Critical	+ 6.9%
276536	BIOPASS RAT .EXE File Download Variant-4	●	Aug 12 03:00 AM	File_Malware-Blocked	Critical	+ 6.9%
707406	FOCUSFJORD Backdoor used by UNC215 APT Group .DLL Do...	●	Sep 11 03:00 AM	File_Malware-Blocked	Critical	+ 6.9%
819693	LEMPO Trojan used by TA456 Threat Group .VBS File Downloa...	●	Sep 28 03:00 AM	File-Text_WScript.Shell-ActiveX-Object-Local-Fil...	High	+ 2.3%
737305	LEMPO Trojan used by TA456 Threat Group .VBS File Downloa...	●	Sep 28 03:00 AM	File-Text_WScript.Shell-ActiveX-Object-Local-Fil...	High	+ 2.3%
494305	LEMPO Trojan used by TA456 Threat Group .VBS File Downloa...	●	Sep 28 03:00 AM	File-Text_WScript.Shell-ActiveX-Object-Local-Fil...	High	+ 2.3%
358399	LEMPO Downloader used by TA456 Threat Group .XML File D...	●	Oct 5 03:00 AM	File_Malware-Blocked	Critical	+ 6.9%

View performance metrics for each of your security controls and generate executive reports to share results

For threats that are not blocked, the platform provides vendor-specific and generic signatures - grouping all threats that can be blocked by each signature. All signatures are fully tested by Picus Labs prior to release.

To facilitate swiftlier mitigation, The Picus Platform's ability to integrate with a wide range of network and endpoint security tools enable signatures to be applied via automation.

KEY FEATURES

✓ Supplies **holistic visibility** of threat detection and response capabilities.

✓ Provides **insights** on the Fixing Items, Improvement Points, and Positive Points over detection rule baseline.

✓ **Continuously** detects improvement points in the rule baseline by the correlations of the insights given for the rule.

✓ **Prioritizes** rules that need improvement with filtering options on the assessment result.

✓ Reveals the effect of a **newly developed rule** on SIEM.

✓ Maps results to **MITRE ATT&CK** Framework.

✓ Measures the **threat coverage** of rules and analyze deficiencies with **an extensive Picus Threat Library** of 3,700+ threats consisting of 19K+ actions, **updated daily.**

Test Your Defenses Against the Latest Threats

START FREE TRIAL

Gartner
peerinsights™
4.9 / 5*

*average score at time of press in January 2023

www.picussecurity.com

picussecurity