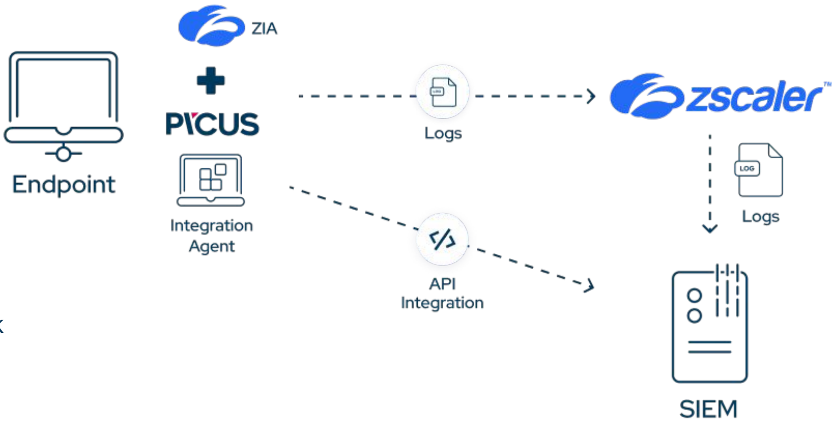
SOLUTION BRIEF

THE PICUS COMPLETE SECURITY VALIDATION PLATFORM AND ZSCALER ZIA INTEGRATION

CONTINUOUSLY VALIDATE YOUR SECURITY EFFICACY

Ensuring a security stack is configured correctly can be challenging. Traditional security stacks leveraging different point solutions creates complexity and potential gaps. Zscaler's Zero Trust Exchange delivers a complete security stack through a Secure Services Edge (SSE) architecture, delivered as a service from the cloud.

The Picus Complete Security Validation Platform integrates with Zscaler by analyzing activity logs to continuously test, validate and report on security efficacy. Attacks such as data exfiltration, network infiltration and endpoint attacks are performed safely and checked against Zscaler's detection and prevention capabilities.



Integration Benefits

✔ Improve Attack Readiness
The Picus Platform continuously challenges Zscaler ZIA against over 3,500 threats (comprising 18k+ actions). The platform provides visibility of Zscaler ZIA's network and cloud readiness, and furthermore, identifies detection gaps and answers questions on readiness for users with an intuitive UI.

✔ Achieve Better Detection Rates and Faster Response Time
The integration aligns offense and defense teams, enables proactive SecOps and SOC practices. By this, the joint integration optimizes prevention and detection abilities of ZIA and continuously improves alerting accuracy and detection rule drifts.

✔ Operationalize MITRE ATT&CK Matrix to Achieve Metrics-Driven Operations
By automatically mapping threat coverage findings for both security events and detections to the MITRE ATT&CK, The Picus Platform enables Zscaler customers to measure gaps and prioritize the mitigation of adversary techniques.

How It Works

To validate your existing Zscaler ZIA setup, follow these simple steps:

1. Install the Picus simulation agent on an endpoint protected by Zscaler ZIA.
2. Install the Picus integration agent and configure the SIEM integration to validate Zscaler ZIA logs.
3. Simulate the threats you want to test your defenses against.
4. Analyse the insights about the level of protection and detection provided by your Zscaler ZIA.
5. Mitigate the critical gaps based on the findings.

ABOUT PICUS

At Picus Security, we help organizations to continuously validate, measure and enhance the effectiveness of their security controls so that they can more accurately assess risks and strengthen cyber resilience.

As the pioneer of Breach and Attack Simulation (BAS), our Complete Security Control Validation Platform is used by security teams worldwide to proactively identify security gaps and obtain actionable insights to address Them.

Picus has offices in North America, Europe and APAC and is supported by a global network of channel and alliance partners.

ABOUT zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest in-line cloud security platform.

Test Your Defenses Against the Latest Threats

START FREE TRIAL

www.picussecurity.com

picussecurity

KEY USE CASES

Zscaler ZIA Policy Validation

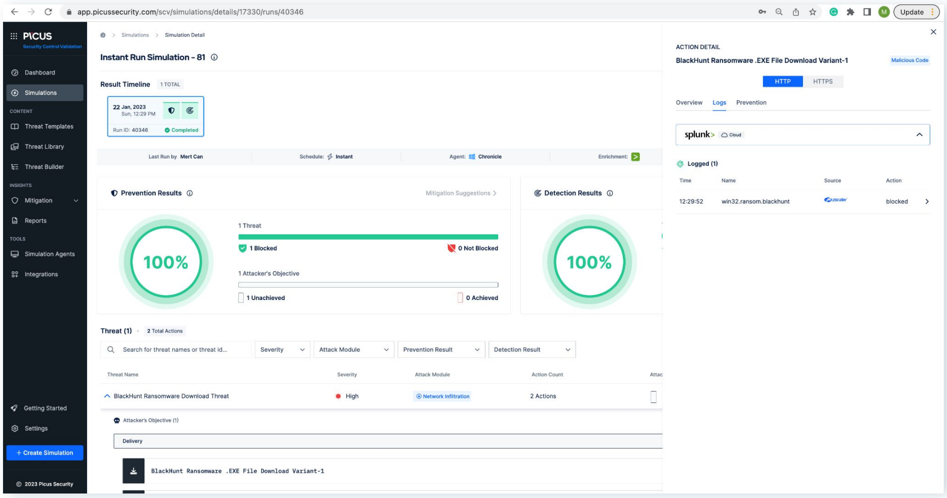
The Picus Platform enables organizations to test and measure the ability of their Zscaler ZIA policies to defend against the latest threats. When weaknesses or gaps are identified, the platform helps to gauge their impact and optimize existing toolsets to address them.

Enhancing Detection Efficacy

The Picus platform identifies weaknesses and misconfigurations in Security Event and Event Management (SIEM) to verify if there is a failure to generate alerts and retrieve correct logs for analysis. The Picus Platform correlates results with corresponding SIEM alerts and events to ensure they are properly tracked on the SIEM, thereby measuring the effectiveness of your Zscaler security control.

Security Posture Management

The Picus Platform enables security leaders to obtain a clearer picture of their security posture by assessing and quantifying the effectiveness of security controls to prevent, detect and respond to attacks across the cyber kill chain.



app.picussecurity.com/scv/simulations/details/17330/runs/40346

Instant Run Simulation - 81

Result Timeline 1 TOTAL

22 Jan, 2023
Sun, 12:29 PM
Run ID: 40346 Completed

Last Run by Mert Can | Schedule: Instant | Agent: Chronicle | Enrichment:

Prevention Results

1 Threat
1 Blocked | 0 Not Blocked
1 Attacker's Objective
1 Unachieved | 0 Achieved

Detection Results

Threat (1) · 2 Total Actions

Search for threat names or threat id... | Severity | Attack Module | Prevention Result | Detection Result

Threat Name	Severity	Attack Module	Action Count	Attac
BlackHunt Ransomware Download Threat	High	Network Infiltration	2 Actions	

Attacker's Objective (1)

Delivery

`BlackHunt Ransomware .EXE File Download Variant-1`

ACTION DETAIL

BlackHunt Ransomware .EXE File Download Variant-1 Malicious Code

Logged (1)

Time	Name	Source	Action
12:29:52	win32.ransom.blackhunt	zscaler	blocked

PICUS PLATFORM

Picus Security Validation Platform simulates real-world threats to continuously validate, measure and enhance the effectiveness of organizations' cyber defenses. The platform bolsters cyber resilience by identifying threat prevention and detection gaps, supplying actionable mitigation recommendations, and by facilitating a more proactive and threat-centric approach to security.

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.