SOLUTION BRIEF

Fortinet and Picus Security Solution

Enhanced Cyber Resilience and Streamlined Security Operations

Executive Summary

To help organizations validate the effectiveness of their security controls and enhance their cyber resilience, Fortinet and Picus Security, the pioneer of Breach and Attack Simulation (BAS), have partnered to develop a joint solution. The solution enables security teams to proactively identify security gaps and obtain actionable insights while ensuring consistent data flow, lower alert noise, and agile response capabilities.

The Challenge

With cyberattacks increasing in number and severity, security operations center (SOC) teams face more significant challenges detecting and responding to them. Visibility blind spots and alert fatigue are common problems, often caused by misconfigured and underutilized security controls. With well-deployed and always adjusted systems, SOC teams can identify security events early enough to prevent serious breaches.

Joint Solution

Together, Fortinet and Picus Security are committed to delivering a cutting-edge security solution that empower organizations to defend against sophisticated cyberattacks. With this integration, security teams can optimize their security operations and build a robust security framework that safeguards their digital assets.

Bringing the Fortinet FortiSIEM and Picus Security Platform together in an integrated solution empowers organizations to strengthen their security controls and bolster their cyber resilience by validating the effectiveness of their security measures.

The integration enables security teams to continuously assess the effectiveness of their prevention and detection controls against simulated attacks by using the Picus Threat Library, which includes over 90% of the MITRE ATT&CK techniques and thousands of malware, vulnerability exploits, web application attacks, and data exfiltration attack samples.

Picus simulates attacks in a safe and controlled environment to provide security teams with a real-world understanding of their security posture and enable them to prioritize and optimize their security investments.

Solution Components

The Picus Complete Security Validation Platform simulates cyberthreats to continuously 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.

Solution Components

- Fortinet FortiSIEM
- Picus Security Validation Platform

Solution Benefits

- Preparedness against current and emerging cyberthreats
- Complete visibility and cross-correlation of SOC and network operations center (NOC) analytics and network analytics
- Effective incident response and digital forensics
- Actionable guidance on policies and Sigma rules for security control gaps
- Measure the organization's resilience with risk scoring and modeling against MITRE ATT&CK and adversary kill chains
- Establish an agile CI/CD pipeline for detection-as-code and automate threat detection life cycle

FORTINET FABRIC-READY

Fortinet FortiSIEM combines visibility, correlation, automated response, and remediation in a scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and prevent breaches.

Joint Solution Integration

How does the joint integration work?

1. Picus simulates attacks in a safe environment to test security controls.
2. Logs from FortiSIEM are sent to Picus.
3. Picus pulls the logs from FortiSIEM using API queries and then validates the logs.
4. The results are displayed on the dashboard, allowing security teams to take action and improve their security posture.

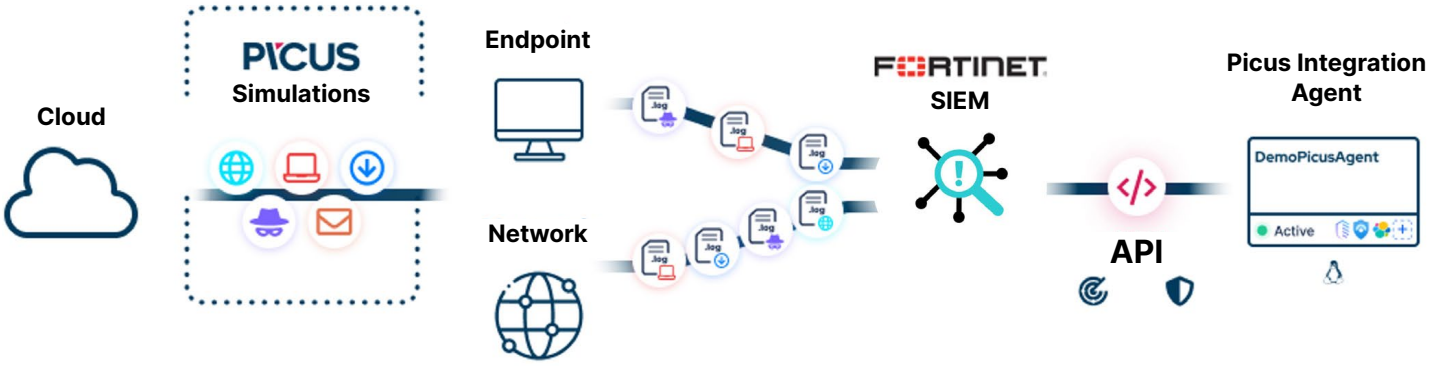

Figure 1: Picus Complete Security Validation Platform and FortiSIEM integration diagram

Joint Use Case

Log Validation

Without the correct data, it's impossible to identify threat activity in your networks. By simulating real-world threats and analyzing the security logs captured by FortiSIEM, Picus:

- Determines if logs from relevant sources are being ingested (and in a timely fashion)
- Understands and prioritize new data sources required to address logging gaps
- Ensures that logs contain the requisite level of data granularity

About Picus Security

Picus Security's 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, Picus empowers customers worldwide to be threat-centric and proactive.

August 7, 2023 8:28 AM
2285021-0-0-EN