PICUS

KEY BENEFITS

Challenge Your Security Technologies

Allow your security teams to challenge their security controls with real attacks before cybercriminals do.

Identify Security Gaps

Identify security gaps in real-time and take action in minutes with Picus mitigation guidance.

Utilize Your Security Infrastructure to its Maximum

Picus helps companies double their threat stopping success rate in just weeks and sustain it.

Operational Efficiency

Real-time identification – quick fixing of security gaps.

PICUS CONTINUOUS SECURITY VALIDATION SOFTWARE FOR "AUTOMATED CYBER-THREAT SIMULATION AND MITIGATION"

Using emerging threat samples, Picus continuously challenges your readiness to emerging threats, identifies strong and weak points of your security measures in real-time and helps you get the most of your security investments.

Hackers Use Known Methods to Bypass

The security market is currently projected to reach $9.6 billion USD by the end of 2018[1]. Despite this growth, security breaches are still on the rise. The likelihood of a recurring data breach over the next two years is 27.7%[2]. The evident question is: "Why aren't the new, advanced technologies and deliberate operational efforts slowing this trend?"

Underutilized Security Investments

Enterprises underutilize their security investments due to limited resources and the expertise required to fine-tune complex security technologies. Operational costs continually increase to maintain a growing list of devices and eventually become a burden.

A False Sense of Safety

After investing in well-known security solutions, many enterprises think they are immune to cyber-attacks. But without metrics, it's impossible to know how well a solution is contributing to your security posture.

SIEM Integration

ArcSight, McAfee nitrosecurity, IBM Radar, splunk>, LogRhythm, And other SIEM Providers

Technology Alliances

Check Point, McAfee, Cisco Solution Partner, paloalto, TREND MICRO, CITRIX, FORTINET, F5 NETWORKS, SNORT

Go Beyond Traditional Tools and Services

Enterprises need to go beyond point-in-time security tools and services to measure their readiness to cyber-attacks. Keeping a security posture robust should be an ongoing process. A Continuous Security Validation Solution is now possible with the Picus platform.

HOW DOES PICUS WORK?

Picus is designed to identify gaps in security controls and offer mitigation options. To deliver on these promises, Picus takes a four-step approach:

DEPLOY

Install and configure off-the-shelf Picus software solution in hours. After the deployment, our users start getting results within just minutes.

ASSESS

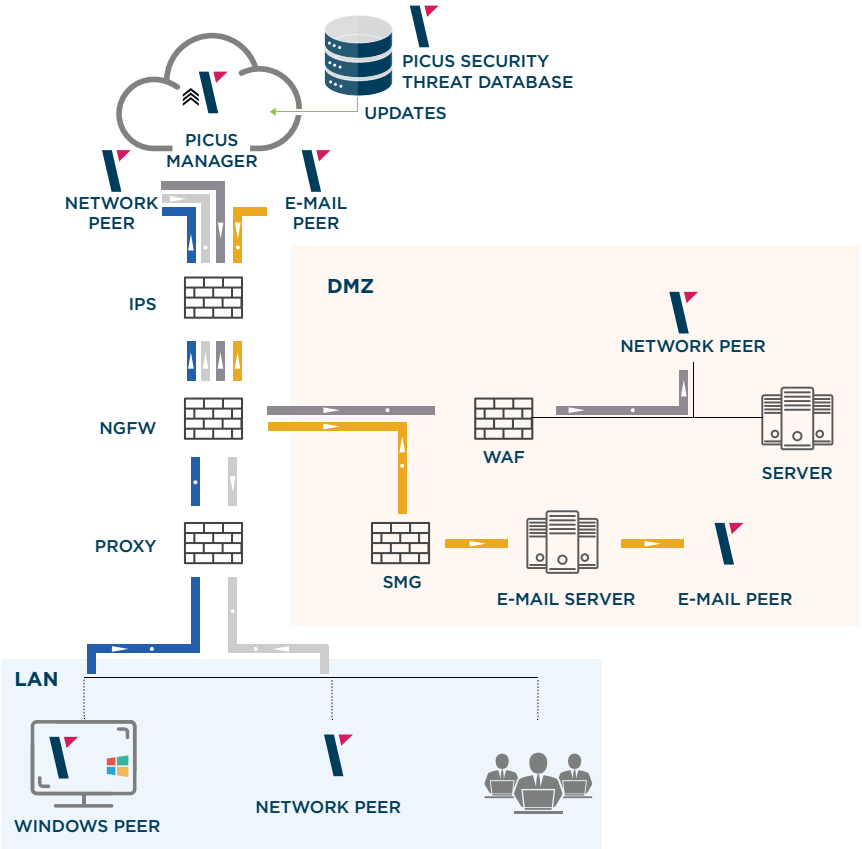
Identify security gaps in real-time and take action in minutes with Picus mitigation guidance.

MEASURE

Interactive dashboards capture the overall picture with objective metrics and list the gaps revealed.

MITIGATE

For gaps revealed during our assessments, Picus provides vendor-specific remediation signatures and creates an actionable prioritization list.



Picus Security Labs

Picus Labs not only identify emerging threats and provide immediate responses, but also bridge the gap between offensive and defensive security teams. As Red Teams analyze, classify, and validate emerging threats, Blue Teams identify how security technologies perform against emerging threats.

The Picus threat database consists of real world threat samples with a specific focus on following attack categories:

- Vulnerability exploitation
- Malware
- Web application attacks
- Data exfiltration

Why Choose Picus?

Focus on Security Controls

Traditional services and tools focus on identifying vulnerabilities, whereas Picus focuses on the efficiency of security devices.

Good for All Prevention Solutions

Standard security device configuration testing solutions have limited offerings for application layer security devices such as IPS, WAF, Sandboxing tools and proxies.

Risk-Free Assessment in Production Environment

Large security device testing appliances focus on stress and effectiveness testing of security devices in lab environments. In contrast, the easily deployable and usable Picus solution is designed to work in the Production Environment.

[1] Gartner Inc., Press Release, 2017
[2] Ponemon Institute, Cost of Data Breach Study, 2017

415 Jackson St., Suite B,
San Francisco, CA 94111 USA
info@picussecurity.com
www.picussecurity.com