EXCLUSIVE NETWORKS

PICUS SECURITY

“Maximize the Security Potential”

Picus “Continuous Security Validation and Remediation” Solution

If you have one bullet to fire:

Picus Security offer a unique approach for enterprises to **measure their cyber-threat readiness** and **strengthen defence measures** in hours and minutes. Deployed in production networks, Picus virtual appliances mimic both the attacker and the victim. Attacking each other, Picus Peers simulate attack scenarios and fool security defences as if a real attack is taking place. Peers deployed in hours and start providing results in minutes! Picus is completely safe to run.

Customer's Pain

- Security solutions (IPS, NGFW, WAF, DLP, AntiMalware Sandbox, SWG...) are getting more and more complex to manage. **Operational cost and burden** are increasing to maintain this long list of devices.
- After investing in well-known security solutions, many enterprises think they are safe from cyber-attacks. But without metrics, it's impossible to know how well a solution is contributing to the security posture. Based on field findings, security success rate they get is generally 20-50 %. Less than half of what they paid for. **High capex, low return.**

Did you Know?

- **Security logs show the incidents security devices could detect only.** What about the ones that were undetected/missed?
- **Most security teams are afraid of making changes** due to lack of visibility and fear of false positives. Many security devices work with default configurations.
- In an average large enterprise, security teams manage approximately **30 different security solution.** Impossible to keep up without automation.

Market Insight

- **Most cyber threats exploit known and old vulnerabilities and still cannot be prevented. In 2015,** ten vulnerabilities accounted for 85% of successful exploit traffic. The other 15% consisted of over 900 CVEs and they were also active (source: Verizon 2016 Data Breach Report).
- **96% of breaches are avoidable through security controls** (source: Verizon 2012 Data Breach Report).
- **Cyber-security market size increased to $81 Billion in 2016 with 8% CAGR.** Yet, there is no sign of decline in security incidents.
- **Security assessment is a huge opportunity.** While cyber security market grows 8% CAGR, security testing markets grow 18%. The market size expected to be 7.6B in 2021 (Markets& Markets).

Questions to Ask?

- How do you measure the success and miss rate of your security defence systems (NGFW, NIPS, WAF, Sandbox, DLP, Web Gateway, Proxy). What are your metrics or KPIs (key performance indicators) on “prevention success rate”?
- What is your security success rate from Internet to LAN (or choose another path) segment as we speak now? Can you give me an exact percentage?
- How long does it take to define the remediation actions and apply them on your security devices?
- How many of your network segments are most critical to cyber threats?
- What if you had a tool that could continuously help you identify your security control gaps and provide to remediate them in minutes?

Top Benefits

- Allows security teams to challenge their security controls with real attacks, before the attacks are executed by hackers. **Self-challenge.**
- Identifies the security gaps in real time and helps take the remediation actions in minutes and hours. **Protection ahead of the real attacks take place.**
- Picus provides vendor specific and open source remediation options for each cyber threat. This helps companies increase the security success rate 30 to 40% in weeks and sustain it high. **Full utilisation of security infrastructure.**
- **Increased security level – better cyber protection.**
- Real time identification – quick fixing of security gaps. **Operational efficiency.**

Target Customers

- Enterprises with 2,000 users and above seats: On premise or cloud management options. As a product or service.
- Mid Market Companies with 500-2,000 seats. Cloud management. As a service.
- All sectors.
- All companies with NGFW, IPS, WAF, Sandbox, SWG/EGW, DLP... technologies in place or in preparation to invest.

Solution Overview

- Picus' lightweight agents installed on both ends of the network that will be tested. (i.e. Company Extranet and Local Area Network or Cloud and DMZ).
- Agents mimics the attacker and the vulnerable systems and attack each other to fool the defence systems.
- Picus peers are linux based and can be installed on Microsoft Hyper V or VMWare ESX virtual platforms.
- Management Console **can be hosted in Cloud or On Premise.**
- Example of the information Picus provides: This NGFW can protect 74% of the Vulnerability Exploitation attacks at this moment in time. Among the 9 sub categories under this attack category, success rate is 100% for exploit kits, 60% for memory corruption attacks, 30% for Input manipulation attacks, etc. Picus details the attacks specifically and provides remediation recommendation and rules, specific to the vendors and open-source.

Key Differentiators

- Existing security services (i.e. pen-test) and tools (i.e. vulnerability management, policy management, etc.) focus on finding vulnerabilities on servers, computers, applications etc. Often no immediate actions can be taken on these findings and they do not help have better cyber security controls.
- Existing security services and tools give only point-in-time view. No continuous insight, whereas cyberthreats are relentless and never stops.
- **Picus is a continuous attack simulation tool. Picus can work at the background 7/24 basis and identify missed cyber-attacks real time.**
- **Picus has specific focus to remediation. It does not only identify the problems but also assist to solve them in minutes.**
- **It has a wide attack coverage: 150 to 200 attacks added each month.**
- **Picus simulates not only the attacker but also the victim. Therefore, it is precise and totally safe.**

Competition

1. **Vulnerability Scanning and Penetration Testing Tools** (Rapid7, Nessus, Qualys) focus on identifying vulnerabilities on assets whereas Picus' focus is on the efficiency of the security devices. These solutions are complementary.
2. **Security Device Configuration Solutions** (i.e.Algosec/Firemon/Tufin) focus on analysing configurations of firewalls and has limited offerings for application layer security devices such as IPS, WAF, Sandboxing tools and proxies. Picus complements this field with its application layer security focus.
3. **Security Device Testing Appliances** (i.e. Ixia Breakingpoint/Spirent) focus on stress and effectiveness testing of security devices in lab environments. Picus' value proposition lay in working in production environments, with full security focus and being easy to use.

Independent Accolades

- One of the top ten start-up companies selected by PWC in 2016.
- McAfee SIA partner.