PENTERA

Pentera – A Superior Solution for BAS (Breach and Attack Simulation)

The Need for Security Validation

The growing complexity of IT environments and escalating cyber threats are driving security teams to adopt continuous security validation practices. Security validation is vital for identifying real vulnerabilities, assessing their impact, and prioritizing remediation to reduce risk exposure. It offers concrete evidence of an organization's cyber posture, demonstrating whether existing security defenses can withstand actual attacks.

Gartner has recently introduced a new category for products addressing this need - Adversarial Exposure Validation (AEV). AEV is part of the Continuous Threat Exposure Management (CTEM) framework, a transformational approach defined by Gartner to measure and reduce cyber risk proactively. The new AEV category encompasses both Breach and Attack Simulation (BAS) and Automated Penetration Testing and Red Teaming technologies.

Traditional BAS products simulate predefined attack scenarios to validate the effectiveness of security controls. While these tools allow for prescriptive testing of controls against a range of TTPs, they require heavy intervention and effort to use, and do not emulate the real behavior of adversaries running full attacks in an organization's live IT environment. Pentera offers a differentiated approach to BAS, providing more accurate exposure findings while simplifying deployment and operations.

Pentera: A Differentiated Solution

Pentera conducts real attack emulation to find and prioritize exploitable vulnerabilities, misconfigurations, credential exposures and more. Pentera's algorithm-based attack orchestration engine automates full attack sequences and identifies achievable kill-chains, all through an easy-to-deploy, agentless approach.

Pentera's Unique Value Proposition

Real, safe attacks - Pentera safely executes a wide range of attack TTPs and exploits in the production IT environment, all vetted by our Security Research team.

Algorithm-based attack propagation - Pentera's automated attack orchestration engine mimics adversary behavior to uncover full attack kill-chains step-by-step, without any playbooks.

Agentless operation - Pentera reduces operational overhead by eliminating the need for installing and maintaining agents. Attackers don't use agents, and neither does Pentera.

Attack surface coverage - Beyond identifying gaps in security controls, Pentera finds exploitable vulnerabilities, misconfigurations, identity-related exposures, data hygiene issues, and more.

Impact-based prioritization - Pentera prioritizes remediation efforts based on proven exploitable attack paths and their potential business impact.

Pentera Vs. Traditional Breach and Attack Simulation Vendors

Pentera	Legacy BAS Vendors	The Pentera Advantage
Real Attacks - Done Safely Full-vector attacks in production IT environments - delivering realistic emulations with built-in safety.	**Synthetic Attacks** Assuming uniform asset configuration across the network, BAS offers predefined one-shot simulated attacks - configured as individual templates.	Accurate view of full exploitable attack paths to uncover security gaps across all organizational environments.
Algorithm-Based Attack Propagation Attack paths are created dynamically. Pentera's algorithm-based attack orchestration engine mimics adversary behavior by recalculating attack vectors with every new discovery or successful attack step.	**Playbook-Based Prescriptive Testing** Testing is limited to predefined playbook scenarios. It focuses on testing TTPs rather than emulating the adaptive tactics of a real threat actor.	More realistic attack path discovery and thorough assessment of your security posture. Discover "unknown unknowns" that may be exploited by attackers.
Agentless Fast deployment and seamless operations on any target environment.	**Agent-Based** Requires installation and maintenance of agents on target devices.	Frictionless operations and faster roll-out. On demand application of tests over any environment.
Full Attack Surface Validates controls, vulnerabilities, credentials, configurations, and data hygiene across production environments, including endpoints, servers, services, and network devices.	**Limited Scope** Simulates attacks limited to testing controls on compute nodes.	Identification of a broader range of security gaps.
Identity Threat Testing Actively uncovers gaps in identity data hygiene by sniffing networks, enumerating files, and scanning for credentials and other sensitive information. Leverage the discovered data to advance attacks, emulating adversarial tactics like privilege escalation and lateral movement.	**Identity Agnostic** Sniffs for sensitive information but does not connect or advance findings into a more sophisticated attack chain. This results in limited, isolated, and less realistic attack scenarios confined to the host environment where the agent runs.	Validation of credential and data hygiene as well as assessment of identity compromise 'blast radius'.

Pentera	Legacy BAS Vendors	The Pentera Advantage
Dedicated Cracking Engine Utilizes GPU acceleration and dedicated resources for targeted AD attacks, recovering plaintext passwords through brute-force and dictionary methods.	**Local Agent-Based Cracking** Cracks domain/local accounts and hashes, limited by agent capabilities (memory, CPU) or cracked in the cloud.	Harden your credential and identity attack surface while keeping your data private, whether running Pentera on-premises or in the cloud.
Impact-Based Prioritization Tests complete attack kill chains, from root cause to impact, prioritizing exploitable vulnerabilities that pose the greatest business risk.	**TTP-Based Focus** Runs thousands of attack scenarios, creating a flat list of theoretical flaws without full context, focusing on specific tests over real business impact.	Surgical remediation based on proven exploitability and impact.

Summary

Pentera offers a unique combination of BAS capabilities and automated penetration testing technology, delivering a differentiated approach to security validation. Choose Pentera for:

- **Reduced Cyber Risk:** Gain a true understanding of your exposure by seeing what a real attacker could achieve within your environment.
- **Improved Remediation Precision:** Focus on addressing the gaps that cause the highest exposure.
- **Streamlined Operations:** Benefit from an agentless setup, and eliminate the need to manage and select from a multitude of testing templates.

About Pentera

Pentera is the market leader in Automated Security Validation, empowering companies to proactively test all their cybersecurity controls against the latest cyber attacks. Pentera identifies true risk across the entire attack surface, guiding remediation to effectively reduce exposure. The company's security validation capabilities are essential for Continuous Threat Exposure Management (CTEM) operations. Thousands of security professionals around the world trust Pentera to close security gaps before threat actors can exploit them.

For more information, visit: pentera.io