PENTERA

Pentera VS Breach and Attack Simulation Vendors

PENTERA VS BAS (Breach and Attack Simulation) Vendors

Pentera Automated Security Validation Platform

Pentera brings a unique approach to identifying organizations' security threats and improving security readiness. By emulating techniques from the attacker's perspective, the Pentera platform provides the most accurate picture of cybersecurity exposures by safely executing real attacks in the production environment.

Benefits

Accelerate the validation-remediation cycle by focusing first on remediating breachable and risk-bearing weaknesses as they are created.

Reduce third-party reliance and expenses by automatically, independently testing, and validating security as often as needed, at a fixed cost.

Increase security teams' efficiency by focusing your attention only on security gaps proven to be a potential breach-point.

Pentera VS Breach and Attack Simulation Vendors

BAS Vendors	Pentera	The Pentera Advantage
Agent-Based Requires installation and maintenance on target devices.	**Agentless** Fast deployment and frictionless operations on any target environment on-demand.	**Simplified Operations**
Limited Scope Simulates attacks to test controls among compute nodes only.	**Full Attack Surface** Controls, vulnerabilities, credentials, configurations, privileges, and data hygiene validated on production environments, including endpoints, servers, services, and network devices. Covers both external and internal attack surfaces.	**Reduce Risk by Validating the Complete Attack Surface**
Simulated Attacks Findings are not based on the actual production environment, configurations, etc.	**Real Attacks - Done Safely** Full vector attack emulations in real production environments - as close as possible to reality, but safe by design.	**Increase Accuracy of Findings to Optimize Remediation**
Segmentation Limitations Simulations run within the defined network segments only.	**Segmentation Validations** Validates segmentation effectiveness by emulating attacks on the production environment and finding the flaws, enabling it to challenge segmentation.	**Reduce Risk by Unveiling More Exploits**
Playbooks The attack simulations follow predefined paths according to playbooks.	**Dynamic Attack Propagations** Attack vectors are created dynamically, according to the unique properties of the production environment. This results in discovering the "unknown unknowns".	**Increase coverage of all possible attack vectors**
Limited Testing for Other Security Solutions Playbooks cover only the controls assuming their actual behavior	**Validate the Entire Defense Line** Automatically attempt to bypass existing deployed security solutions (i.e., EDR) to highlight security gaps and maximize security readiness.	**Increase Effectiveness of Existing Security Controls**
No Kill Chain Context Playbook results are agnostic to each other, creating a flat list of theoretical flaws.	**Full Kill Chain Context** Compose a full attack vector from the attacker's perspective and provide an optimized remediation plan to eliminate the root cause.	**Root Cause identification and Surgical Remediation**

Conclusion

Security teams choose Pentera as it constantly emulates real attacks, which drastically reduces false positives and simplifies the operational engagement with the platform using a centralized solution.

Real attacks - Emulate the latest tactics, techniques, and procedures.

Ease of Operation - Apply agentless security validation anywhere. Instantly.

Autonomous testing - 1-click to test your complete attack surface: external & internal.

About Pentera

Pentera is the recognized category leader for Automated Security Validation, allowing every organization to easily test the integrity of all cybersecurity layers, unfolding accurate, current security exposures at any moment, at any scale. Thousands of security professionals and service providers worldwide use Pentera to guide remediation and close security gaps before they are exploited.

www.pentera.io