PENTERA | DATA SHEET

PENTERA

Continuous Security Validation Of Your Internal Network

Automate the discovery of real security exposures in your IT environment with Pentera. Continuously validate your security at scale by safely emulating the actions of an attacker in your network.

Key Product Pillars

Identify True Risk
By safely emulating attacks, Pentera discovers the exploitable attack surface and uncovers security gaps in real-time, in the context of the specific IT environment.

Fully Autonomous
Pentera performs reconnaissance and progresses attacks across the network in a fully automated manner, offloading repetitive tasks from security teams.

Flexible Deployment
Requiring no agents, Pentera is easy to install and maintain on your infrastructure of choice: on-premises or in the cloud.

Surgical Remediation
Pentera unveils complete possible attack kill chains, pinpointing the root cause of the attack for efficient remediation with step-by-step guidance.

Use Cases

Core

Validate your security resilience across IT and hybrid environments to quickly identify exposure and minimize impact on your business.

- Track risk exposure trends across your complete attack surface
- Continuously validate tools and processes

Ransomware Ready Validation

Safely emulate complete ransomware attacks to test readiness against ransomware in your live environment.

- Act before compromise by pinpointing specific security gaps in your security program
- Test the most prevalent ransomware strains to ensure data cannot be accessed without authorization or exfiltrated during cyber attacks

Credential Exposure Validation

Continuously validate stolen and compromised credentials against your complete attack surface to preempt breaches.

- Reduce manual work by correlating threat intelligence with active credentials
- Identify and remediate credential-sourced exposure based on true business impact

Surface

Continuously map your organization's external attack surface, launch safe-by-design attacks, and prioritize exposure remediation to see your most attractive assets the way an adversary would.

- Reduce cyber risk exposure
- Reduce third-party testing reliance and expenses
- Increase cybersecurity team efficiency