Pentera Surface
Pinpoint True Web-facing Security Gaps

Harden Your External Attack Surface

Continuously map your organization's external attack surface, launch safe-by-design attacks, and prioritize exposure remediation to focus your team on reducing the most critical security exposure.

Key Product Pillars

Attack Surface Monitoring
Gain complete visibility of your external assets and get alerts about new external-facing exposures.

Adversary Perspective
Spot configurations and attributes that indicate potential attacker entry points.
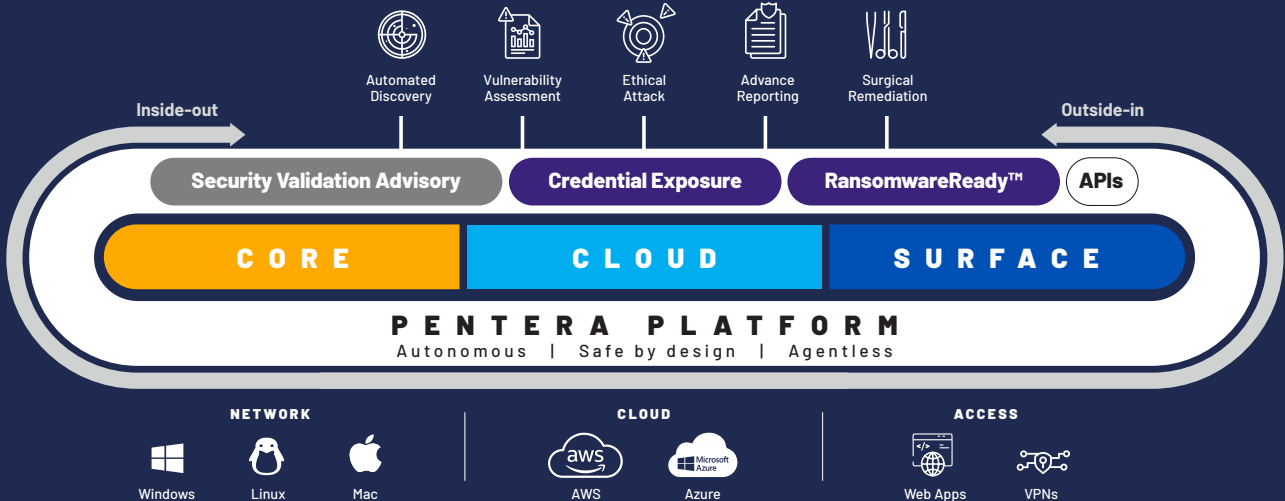
Web Exposure Validation
Safely exploit mapped assets to uncover potential attack vectors and exploitable security gaps.

Focused Remediation
Target remediation efforts on the most pressing security gaps based on proven impact.

All your attack surfaces, <mark>tested continuously</mark> with the Pentera Platform

Automated Discovery

Vulnerability Assessment

Ethical Attack

Advance Reporting

Surgical Remediation

Inside-out ⟶

Outside-in ⟵

Security Validation Advisory   Credential Exposure   RansomwareReady™   APIs

CORE   **CLOUD**   **SURFACE**

PENTERA PLATFORM
Autonomous | Safe by design | Agentless

NETWORK
Windows   Linux   Mac

CLOUD
AWS   Azure

ACCESS
Web Apps   VPNs

About Pentera

Pentera is the category leader for Automated Security Validation™, allowing every organization to test with ease the integrity of all cybersecurity layers, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited.
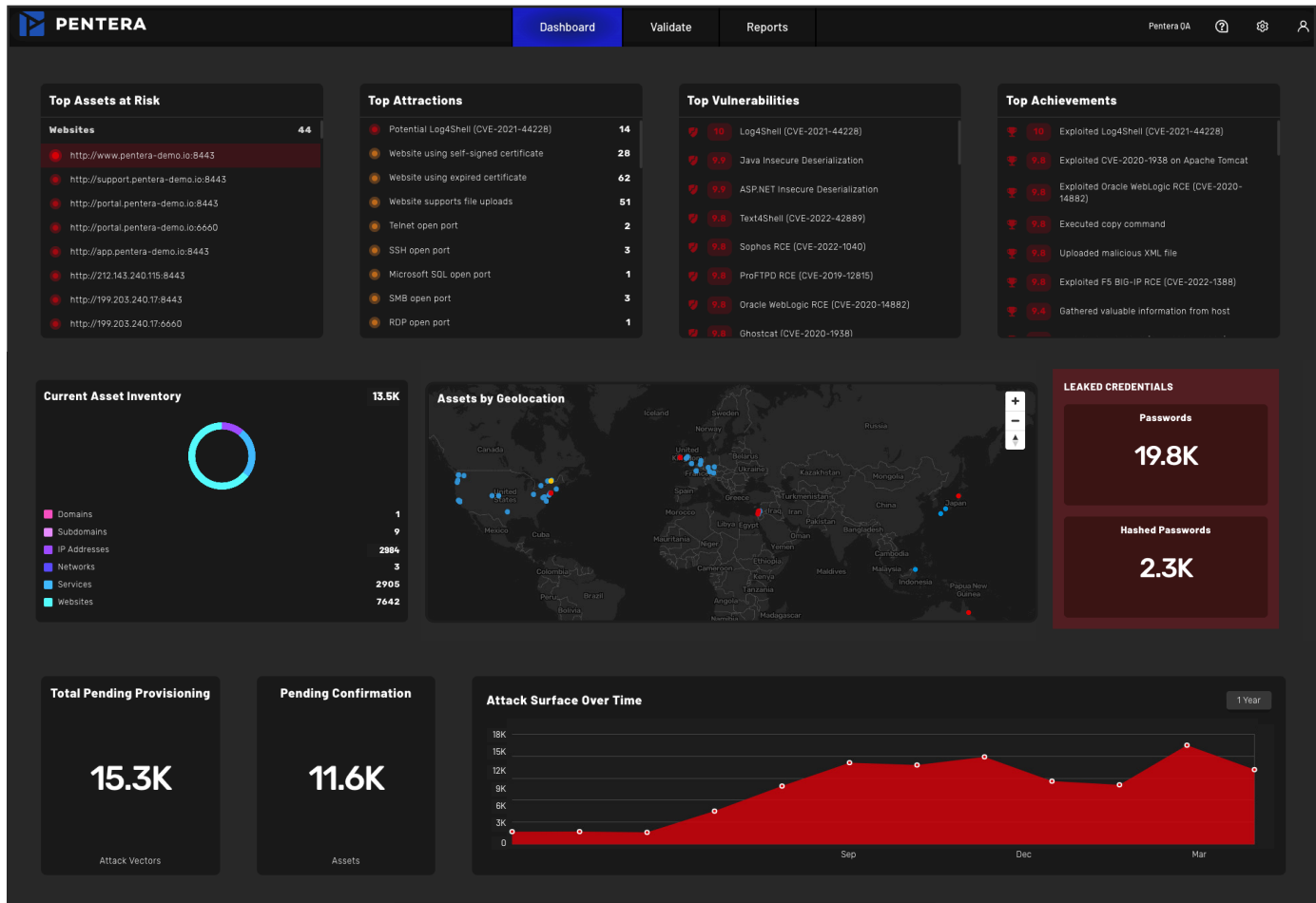
Benefits

+ **Reduce cyber risk exposure**
Surgically identify and eliminate critical gaps with algorithm-based automated security validation.

+ **Reduce third-party testing reliance and expenses**
Minimize cost and dependence on 3rd party external penetration testing services.
Leverage automated, enterprise-grade tests that run at scale.

+ **Increase cybersecurity team efficiency**
Automate security validation testing activities for external-facing assets, focusing your security team's attention on the assets that matter the most.

External Security Validation In-Depth

Pentera safely performs all the actions an adversary would

Reconnaissance
Collect open-source intelligence (OSINT) and map the external-facing attack surface through ongoing asset inventory discovery and reconnaissance.

Enumeration
Gather comprehensive details about public facing assets, including operating system information, open ports, running services and other points of interest.

Threat Prioritization
List the most attractive assets, reflecting the attacker's perspective.

Risk Assessment
Scan for vulnerabilities and assign a risk level to every asset based on the highest associated CVSS score.

Credential Testing
Find and validate the attack surface against leaked credentials by performing credential stuffing where applicable.

Attack Impact Testing
Uncover exploitable kill-chains with safe attack actions, aligned to OWASP and MITRE ATT&CK® frameworks.

Remediation Prioritization
Eliminate critical attack paths and prioritize fixing of identified security gaps based on true impact.

Reporting
Document findings for internal communication with executives and security teams.