PENTERA PROOF OF VALUE

What is a proof of value?

A Proof of Value (PoV) is an easy one-day assessment that allows you to evaluate Pentera's automated security validation platform *within your own environment*. The PoV empowers organizations to understand why some of the world's leading companies are relying on Pentera. With Pentera, customers gain unprecedented visibility into their networks and uncover unknown security gaps - before they develop into damaging data breaches. Pentera experts deploy Pentera within minutes, giving you access to our groundbreaking attack orchestrator engine. At the end of the PoV, a report is produced automatically, providing you with findings, and a validated roadmap for cyber exposure reduction.

Why do a PoV?

Validate your security controls & true cyber exposure

Today's networks are distributed and segmented making it very difficult to work out what is going on, where and how, at all times. Pentera automatically discovers all assets across your network, down to devices and network protocols, identifies security weaknesses, and initiates attack techniques to advance the attack.

- Get a true read of your network and security configurations
- Understand if and where your defensive controls are misconfigured or falling short
- Have the ability to 'zoom-in' on complete attack operations and assess enterprise-wide exposure

Identify exploitable vulnerabilities you did not know exist

Pentera's unique 'one-click' approach does not rely on prior network knowledge and is *completely agentless*. The Pentera platform continuously assesses vulnerabilities detected for exploitability and business risk impact.

- Find the vulnerabilities that you didn't know exist and in reality poses the highest risk
- Understand what your top security priorities are - Pentera lets you see and remediate vulnerabilities without getting distracted by static and low-fidelity ones.
- Take timely remedial action to minimize risk to your organization

Evaluate enterprise readiness and start reducing risk

Security practitioners and regulators have become more aware of the need to integrate the adversarial perspective into an organization's ongoing cyber defense strategy. Pentera's offensive and MITRE ATT&CK alignment approach empowers organizations to be better prepared by focusing on high-risk 'breacheable' vulnerabilities.

- Benefit from attack intelligence gained at the frontline by red-teamers & incident responders
- Receive executive-level report providing analysis of your environment's top vulnerabilities and MITRE ATT&CK TTPs mapping
- Get expert advice and guided remediation actions to key security gaps detected

How does it work?

Discover root-cause vulnerabilities automatically

Pentera is deployed on-premises or on a cloud instance and is operational-ready in a matter of 15-30 minutes or less, without any disruption to your team. Pentera's agentless approach applies zero friction and enables immediate discovery and validation across your hybrid infrastructure.

Progress the attack operation

The Pentera discovery and enumeration process immediately starts identifying network protocols and assets enterprise-wide. As new discoveries are detected, Pentera's attack engine initiates exploitation of its proprietary attack frameworks and safe exploits arsenal. A complete attack timeline is built and presented alongside its respective risk and business impact. Over the course of the PoV, new attack exploits will be made available for you to approve.

Report & guide remediation

Pentera equips your team with conclusive priorities allowing you to focus on the most risk-baring security gaps. An executive summary report is automatically generated providing you the true read of your attack surface to speed up guided remediation solutions.

PoV timeline

Schedule	***Actions***	***Your Resource***
Pre-PoV	Schedule deployment of the Pentera instance	*You are assigned a dedicated Security Engineer (SE)*
	• Deployment completed (in under 30min) • Discovery process validation (sanity test) • Attack techniques are activated	
PoV Day (4-6 hours)	**Learn about your network, assets, and enterprise** • Assets in scope (up to 200 endpoints) are mapped • Start assessing network security posture • Identify and focus on exploitable vulnerabilities	*Your assigned SE and access as needed to Pentera researchers*
	Initiate attack operation • Gain insights how vulnerabilities are used to progress the attack • Evaluate attack operation scope and attack frameworks used • Safe Exploits are approved	
	Investigate achievements and analyze attack operations • Gain deeper understanding into risk prioritization • Simulate remediation fixes against discovered root vulnerabilities	
	Evaluate & review • Final executive summary report is delivered at review meeting • Proof of Value assessment is completed	*Pentera team and client executive sponsor*
Post-PoV	• Sign agreement • Plan enterprise deployment and your support needs	*Executive Sponsor*

Resources required for success

For an Onsite PoV:

- RJ45 port in the wall
- Whitelisting the PoV Machine in NAC
- Meeting room with monitor to display Pentera

For a Remote PoV:

- Physical Windows machine for SoftEther VPN Bridge deployment
- RJ45 NIC (not wireless or dongles)
- Port TCP 443 open from Bridge Machine → VPN Server
- Network connection enabled in Network Access Control (NAC), 802.1x Authentication, Port Security

A Secure Connection

Pentera's remote instance was designed with rigid security controls. Multiple layers of defense are incorporated to ensure that all operations performed are safe and fully audited. Encrypted outbound VPN communication is forced with a designated virtual private cloud instance assuring complete client isolation from external network traffic. Customers maintain total control of the connection, which is initiated and maintained from the Pentera instance and can be started, terminated or audited at any time. To ensure a successful PoV, we request that a connection is maintained during the one day PoV.

Safe by design

Pentera conducts real ethical and harmless exploitations to progress the attack the same way an adversary would. Production-grade safety is a promise we live by, where multiple safeguards are in place to assure the resilience of our customer's environments. "Almost safe" is not good enough. When the PoV concludes, a clean up routine commences to ensure the system removed all residuals of the activities performed across the defined network range.

Privacy and legal considerations

- The Pentera technology does not affect network and business operations
- Data is securely deleted once the PoV is concluded
- A legal agreement (MNDA) is required to initiate the PoV

About Pentera

Pentera is the world leader in Automated Security Validation. Our agentless technology, Pentera, allows your security team to launch network infrastructure attacks on your organization's network, on-demand, reducing corporate cyber security risk. Pentera identifies, analyzes and focuses remediation efforts on breachable vulnerabilities, validating organization's defensive security controls and improving organizational immunity against cyber attacks, across their enterprise-wide network.

www.pentera.io