PENTERA

Data Sheet

SAFETY BY DESIGN
SECURITY VALIDATION

Have the confidence to know
your assets are secure

Digital transformation and recent supply chain data breaches have not only changed the way companies do business. They also underscore the need for an uncompromising security-first approach. To help organizations meet this critical objective, Pentera, the pioneer of Automated Security Validation™, has placed the highest security standards and the do-no-harm policy at the core of our offering.

From the ground up, we built our platform with safety by design in mind, incorporating every possible safety control as a key component of every new functionality that is introduced. In fact, we infuse security across the entire software development lifecycle (SDLC), from ideation and design to development, delivery, and operations. As a result, hundreds of organizations around the world trust Pentera to ensure that no security validation assessment impacts the organization's network assets, and that business continuity is assured. In this paper we share the principles of our unique approach to safety by design.

Validate what you need. Nothing more.

Pentera enables its operators with full control over the scope and duration of the validation process regardless of how complex, distributed, and hybrid your network infrastructure is. Defined boundaries are always kept; nothing more, nothing less.
Whether a complete network test is in scope, or a dedicated security weakness validation, Pentera provides the speed and flexibility to help you scale your security program and assure attack readiness.

Safety controls

- Testing scope guardrails
- Approval process of vulnerability ethical exploitation
- Arsenal of attack tactics & techniques applied
- Attack stealthiness level
- Data hygiene and sanitation verification
- User credential validation
- Code integrity

Business as usual. Always.

Once a testing range is defined, Pentera immediately initiates an attack surface exposure of network protocols, infrastructure assets, configuration, and known vulnerabilities. Once Pentera identifies new vulnerabilities, further exploitations are made available for the user to approve. In case a single action has failed, Pentera stops and disposes of collected information from further use. This foundational design approach prevents users from being locked out and ensures business continuity.

Assuring data hygiene

Pentera does not delete, encrypt, or manipulate the organization's data. Data that is collected is stored and encrypted on premise, while no metrics, hashes, passwords nor vulnerabilities are sent externally. Once a security validation evaluation is concluded, sanitation is performed to assure that all files and accounts created are completely removed. In addition, an audit log with required context is available in the Footprints report.

Proprietary ethical exploits

Similar to malicious adversary tactics and techniques, Pentera leverages real exploits without any disruption to service.
The platform attack engine focuses only on the exploitable vulnerabilities that pose the greatest risk to the organization. Aligned to the MITRE ATT&CK framework, Pentera's exploitation and post-exploitation phases leverage proprietary exploits and payloads, purposely built in-house by Pentera's Research team. By design, we never exploit vulnerabilities that may cause system issues. Moreover, several exploits are switched off by default (e.g ARP Poisoning and DHCP MITM), and will not run unless specifically enabled.

Test as you want, reduce risk

Distributed network segments can be validated against a variety of attack tactics and techniques. Pentera leverages a variety of TTPs to enable your team to easily configure how intrusive and noisy or stealthy and quiet the specific emulation will be. The stealthier the setting, the less network traffic is generated. This way we substantially reduce the amount of network traffic, risk, and the load on the organization.

Integrity Assured
Design > Code > Production

○ The Pentera software development process is based on the OWASP Secure SDLC framework. Where multiple layers of protection, starting from the engineering environment, ensure the integrity of our codebase and delivery.

○ When building a security architecture that thinks, acts, moves, and exploits vulnerabilities as an attacker would, you can understand what's at stake and how critical is the safety and integrity of code.

○ We also invested early in ISO27001 certification regarding processes and procedures to assure overall quality and integrity of the Pentera platform.

Each ethical exploit undergoes rigorous and uncompromising tests to ensure complete safety and adherence to our do-no-harm policy before being implemented in the platform

PENTERA

Complete transparency

Every action performed by Pentera is documented and reported within the audit log report so that your security teams can easily identify every task performed, directly from the Pentera user interface. Reviewing all payloads and files injected, users can review their removal status and enable further actions to be taken.

Pentera can also be set to require approvals prior to every action performed by the platform, and against every security achievement exposed. This allows specific scenarios to be run against specific hosts, providing a high degree of granularity and control where no exploits are triggered unless explicitly approved by the security team.

6 Years

>350 Customers

0 Failures

Ready to start validating?

Understand cyber exposure, prioritize vulnerabilities, and focus on the most risk-bearing security gaps. Our one-day proof-of-value enables you to evaluate the Pentera Automated Security Validation™ platform in your own environment. Start getting unprecedented visibility into your network and uncover security gaps - before they develop into damaging data breaches.

Pentera experts deploy the platform within minutes, giving you access to our groundbreaking attack orchestrator engine. Upon completion, a report is produced automatically, providing you with findings and a validated roadmap for cyber exposure reduction.

Get in touch with us today

to understand why global industry leaders rely on Pentera to boost their security posture.

Learn more at www.Pentera.io

Request a Demo