Pentera RansomwareReady™

Answer the Burning Question: Am I Ransomware Defense Ready?

Eliminate Ransomware Exposure

Validate ransomware defenses by emulating attacks safely in production, testing security controls, and blocking propagation paths in your network.
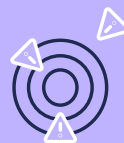
Key Product Pillars

Complete Ransomware Testing

Validate your security against a wide range of ransomware strains such as REvil, Conti, Maze, LockBit, and more.

Proof of Ransomware Resilience

See if your endpoint security can withstand ransomware attacks and if your SOC can detect and respond the way it should.

Proactive Exposure Identification

Understand where your defenses are lacking and fix them before they can be exploited by real-world ransomware actors.
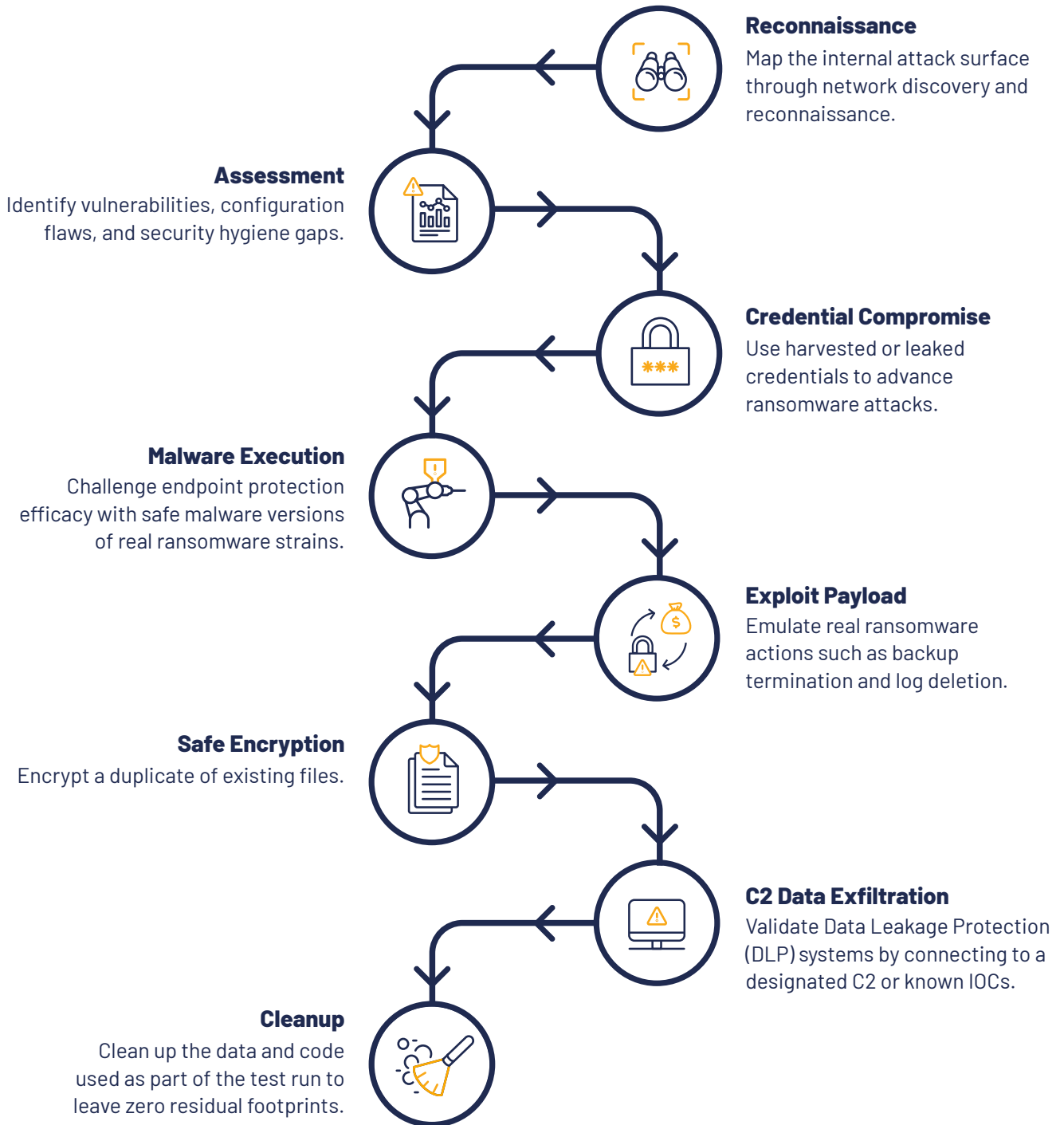
Clear, Actionable Remediation Insights

Cut ransomware kill-chains by remediating vulnerable hosts, deficient controls, and misconfigurations with step-by-step guidance.

Ransomware Defense Validation In-Depth

Pentera safely performs all the actions an adversary would.

Reconnaissance
Map the internal attack surface through network discovery and reconnaissance.

Assessment
Identify vulnerabilities, configuration flaws, and security hygiene gaps.

Credential Compromise
Use harvested or leaked credentials to advance ransomware attacks.

Malware Execution
Challenge endpoint protection efficacy with safe malware versions of real ransomware strains.

Exploit Payload
Emulate real ransomware actions such as backup termination and log deletion.

Safe Encryption
Encrypt a duplicate of existing files.

C2 Data Exfiltration
Validate Data Leakage Protection (DLP) systems by connecting to a designated C2 or known IOCs.

Cleanup
Clean up the data and code used as part of the test run to leave zero residual footprints.

Targeted Testing

Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options

- ✓ Info
- ✓ Ranges
- ✓ Attack Interface Selection
- ✓ Credentials for Initial Access
- ✓ **Settings**
- ✓ Scheduling and Duration
- ✓ Notifications
- ✓ Residue Cleanup

Ransomware Emulation

Validate that your AV/EDR protections are ready to block ransomware

Execute end-to-end attack flows of notorious ransomware campaigns to validate the configurations and efficacy of your antivirus and endpoint protection tools. This test follows the Assume Breach approach.

✓ **Settings**

Select a Campaign

Run an end-to-end attack flow of the selected campaign.

Conti ▼

Encryption Mode

The test encrypts a random sample of user data copied from the hosts - never the originals.

○ Slow
 Fully encrypt targeted files.

● Fast
 Partially encrypt targeted files. Maximum of 100K bytes per file.

Data Exfiltration

Your data is never exfiltrated with Pentera.
Our exfiltration process randomly generates false data instead.
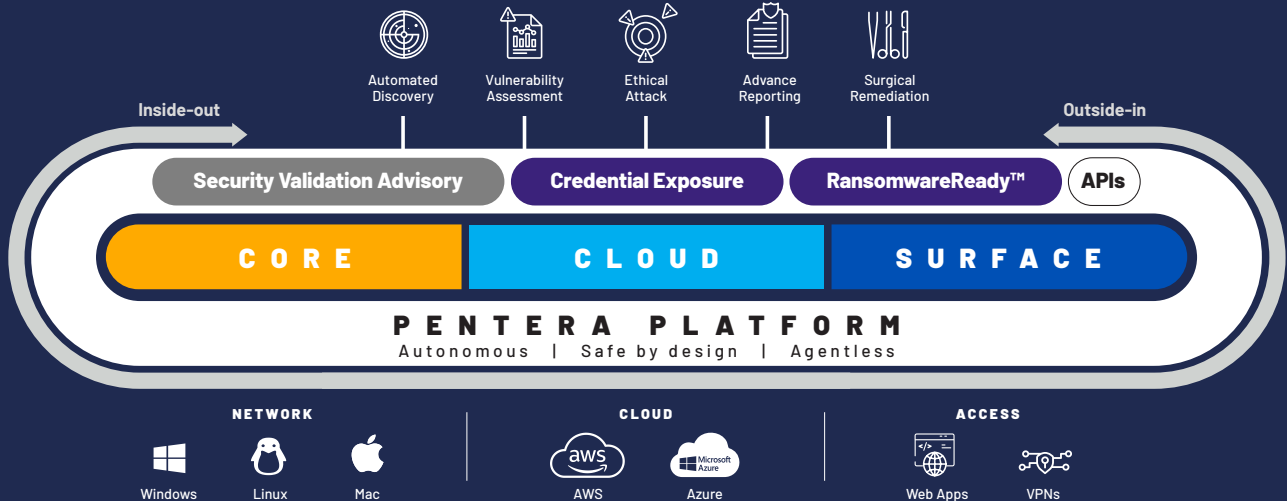
○ No exfiltration

○ Exfiltrate false data to your own designated C2

● Challenge your defenses against known IOCs
 Calibrate your defenses by exfiltrating false data to known IOCs and validate your ability to detect and prevent connections.

Benefits

➕ **Reduce ransomware risk exposure**
Proactively build resilience against your biggest cyber threats.

➕ **Reduce ransomware testing expenses**
Minimize cost and dependence on third-party ransomware testing services.
Leverage automation to emulate attack techniques used by the largest ransomware groups.

➕ **Increase cybersecurity team efficiency**
Focus remediation efforts on proven security gaps to cut ransomware kill-chains.

All your attack surfaces, tested continuously 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
Microsoft 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.