PENTERA | DATA SHEET

PENTERA CORE

Continuous Security Validation Of Your Internal Network

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

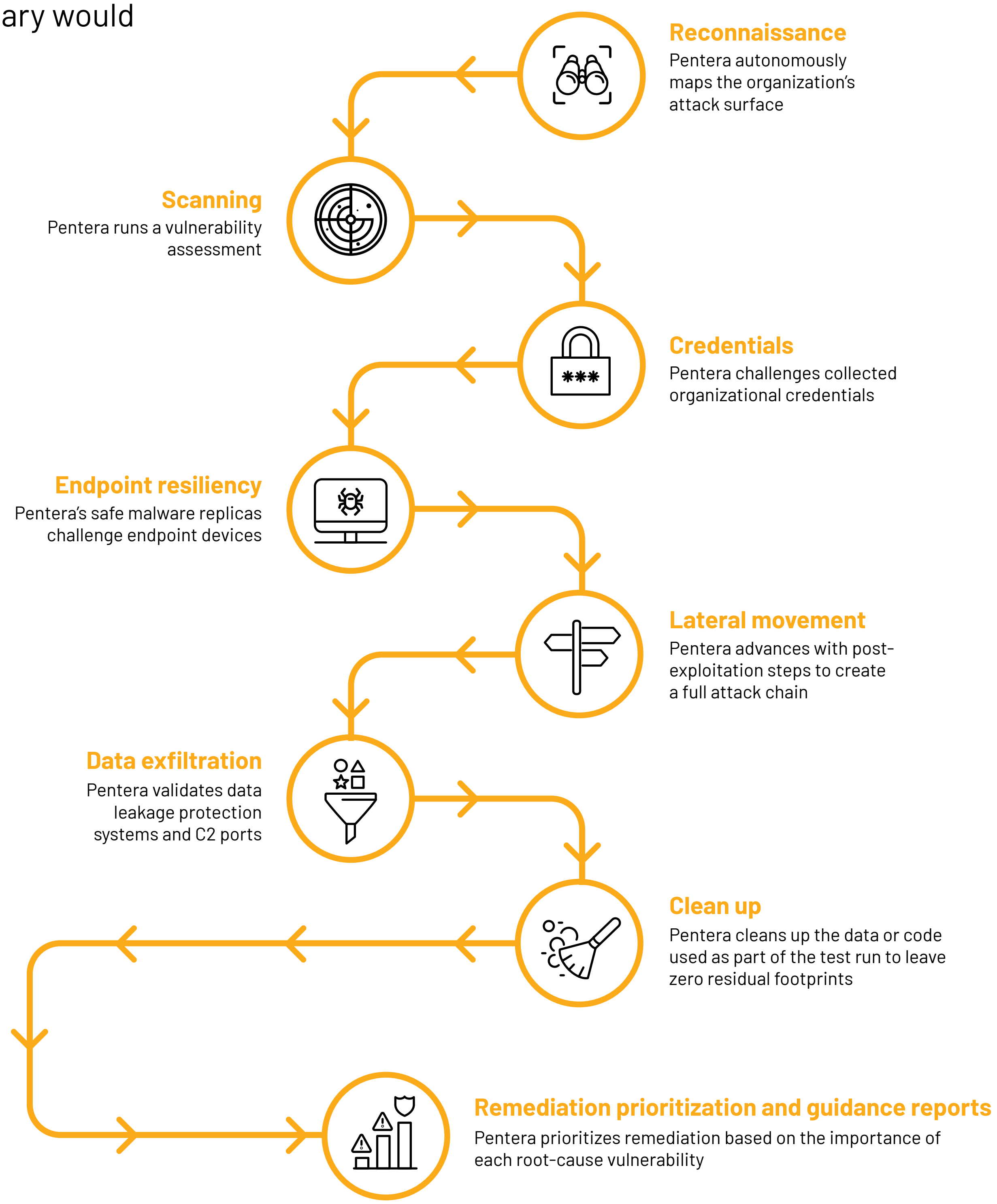
Flexible Deployment
Requiring no agents, Pentera is easy to install and maintain on your infrastructure of choice: on-premises or in the cloud.

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

For more info, visit: **www.pentera.io**

How it works

Pentera safely performs all the actions an adversary would



Reconnaissance

Pentera autonomously maps the organization's attack surface

Scanning

Pentera runs a vulnerability assessment

Credentials

Pentera challenges collected organizational credentials

Endpoint resiliency

Pentera's safe malware replicas challenge endpoint devices

Lateral movement

Pentera advances with post-exploitation steps to create a full attack chain

Data exfiltration

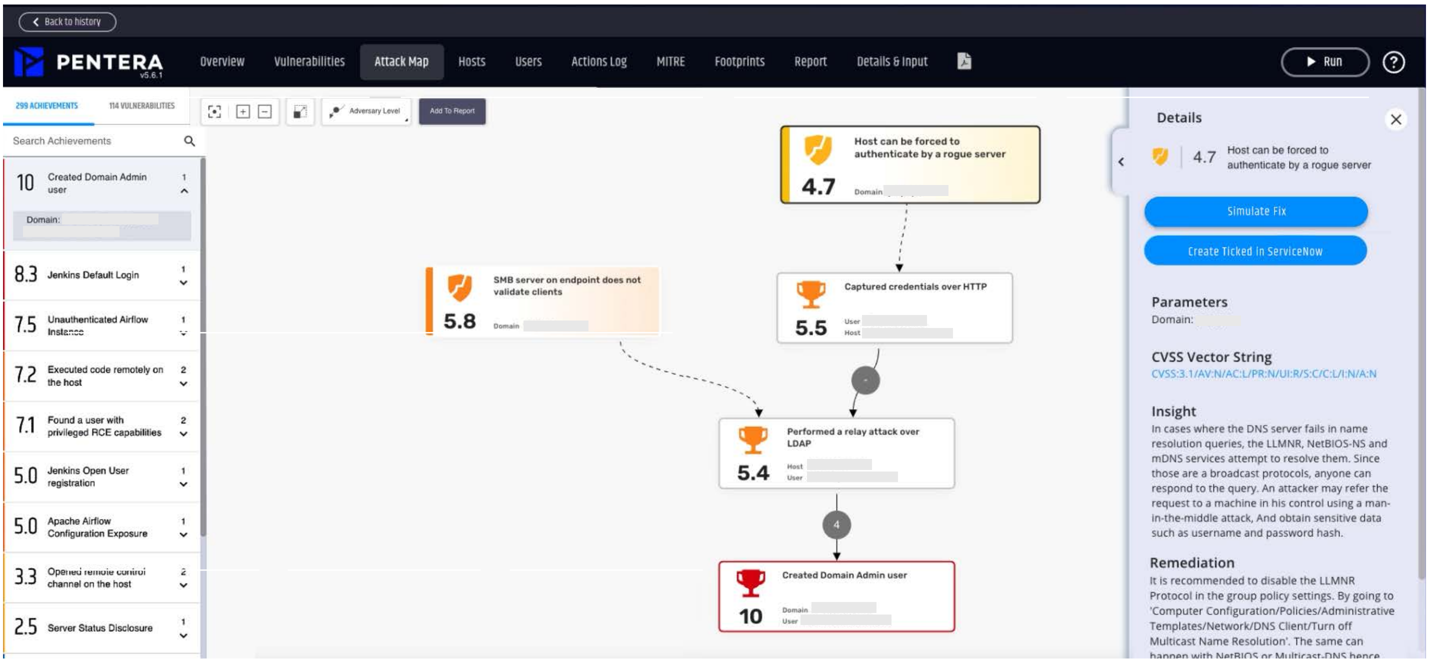
Pentera validates data leakage protection systems and C2 ports

Clean up

Pentera cleans up the data or code used as part of the test run to leave zero residual footprints

Remediation prioritization and guidance reports

Pentera prioritizes remediation based on the importance of each root-cause vulnerability



10	Created Domain Admin user Domain:	1
8.3	Jenkins Default Login	1
7.5	Unauthenticated Airflow Instance	1
7.2	Executed code remotely on the host	2
7.1	Found a user with privileged RCE capabilities	2
5.0	Jenkins Open User registration	1
5.0	Apache Airflow Configuration Exposure	1
3.3	Opened remote control channel on the host	2
2.5	Server Status Disclosure	1

4.7 Host can be forced to authenticate by a rogue server — Domain

5.8 SMB server on endpoint does not validate clients — Domain

5.5 Captured credentials over HTTP — User, Host

5.4 Performed a relay attack over LDAP — Host, User

4

10 Created Domain Admin user — Domain, User

Details

4.7 Host can be forced to authenticate by a rogue server

Parameters
Domain:

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

Insight
In cases where the DNS server fails in name resolution queries, the LLMNR, NetBIOS-NS and mDNS services attempt to resolve them. Since those are a broadcast protocols, anyone can respond to the query. An attacker may refer the request to a machine in his control using a man-in-the-middle attack, And obtain sensitive data such as username and password hash.

Remediation
It is recommended to disable the LLMNR Protocol in the group policy settings. By going to 'Computer Configuration/Policies/Administrative Templates/Network/DNS Client/Turn off Multicast Name Resolution'. The same can happen with NetBIOS or Multicast-DNS hence

Benefits

Maximize security with existing resources

Ongoing security validation allows the prioritization and repair of the most critical security gaps first.

Accelerate time to remediation

Identify the critical security gaps and mitigate potential risk before it materializes.

Reduce third-party testing reliance and expenses

Minimize cost and dependency on 3rd-party penetration testing services.

Increase cybersecurity team efficiency

Increase security personnel validation productivity 10X across the attack surface.

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. For more information, visit **Pentera.io**.