

CONTINUOUS SECURITY VALIDATION, BUILT IN AUSTRALIA

Know what an attacker could reach today, not last quarter

Most organisations test once a year and spend the other eleven months without evidence. Every deployment and configuration change since that test is untested, yet the board, your auditor and your cyber insurer all want proof your defences hold today. PentestOps runs the work of a professional penetration testing team continuously, as software you switch on yourself, so you always have a current, evidence-backed view of your real risk.

Reduce Exposure

Continuously find and watch the assets and weaknesses attackers can see, as your environment changes.

Validate Real Risk

Safely prove which weaknesses are genuinely exploitable, so you fix real problems instead of chasing scanner noise.

Accelerate Fixes

Get AI-assisted, plain-language remediation steps and an automatic re-test that confirms the fix worked.

Prove Compliance

Hand auditors a report mapped to the frameworks you are measured against, always up to date.

THE DIFFERENTIATOR

Proof, not a list of maybes

Where you authorise it, PentestOps does not just flag a possible weakness, it safely demonstrates that the weakness is genuinely exploitable and captures the evidence, within scope you control.

Continuous Validation

Assurance that runs all year, not a once-a-year snapshot.

Exploitability, Not Just Severity

Proof of what an attacker can actually reach, backed by evidence.

Governed Autonomous Testing

AI-driven testing bounded by Rules of Engagement you define.

Unified Coverage

External, internal, web, API, identity, cloud and Kubernetes, in one platform.

WHAT IT COVERS

Covers every part of your business an attacker can reach

Your Internet-Facing Systems

Agentless discovery and testing of the domains, addresses and services exposed to the public internet.

Your Internal Network

A lightweight agent tests internal systems from the inside, using outbound connections only.

Active Directory & Identity

Testing of your identity infrastructure for misconfigurations attackers use to escalate privilege.

Your Websites, Apps & APIs

Coverage of the OWASP Top 10 and API Top 10, with findings streaming in live as the test runs.

Your Cloud & Microsoft 365

A read-only review of your AWS, Azure, GCP and Microsoft 365 configuration against best practice.

Kubernetes & Containers

Configuration and workload testing across your clusters, surfacing weaknesses attackers target.

EMAIL

info@pentestops.com

WEB

pentestops.com

PHONE

+61 1300 290 196

LOCATIONS

Australia



HOW A TEST RUNS

The seven-phase validation loop

Every test follows the same seven steps, then repeats.



Findings are ranked by what a real attacker could actually use, not just a raw severity score. We combine CVSS severity, whether a working exploit exists in the wild, and whether it is on the US CISA list of vulnerabilities known to be actively attacked, with automatic false-positive reduction before anything reaches your report.

YOUR DATA

Your most sensitive data stays yours

Your data is stored in Australia. The AI that triages findings, scores risk and drafts reports is self-hosted by default, so findings are never handed to a third-party AI provider unless you choose to. Internal testing runs on an outbound-only agent over TLS 443, so you never open an inbound connection into your network. Every customer runs in their own isolated environment with its own database. Extranet Systems is ISO/IEC 27001:2022 certified, with operations across Australia, the Middle East and North Africa, and commercially launched PentestOps in July 2026.

REPORTING & COMPLIANCE

Board-ready evidence, mapped to your frameworks

Turn any completed test into a professional report carrying your own company name and logo, written for whichever audience needs it: executives, engineers, auditors or the people applying the fixes. The mapping is a reporting aid that shows where a finding sits against each framework's controls, not a certification.

OWASP Top 10

PCI DSS v4.0

NIST 800-53

SOC 2

HIPAA

GDPR

ISO 27001

SMB1001

CIS Benchmarks

STAYS CURRENT

It keeps testing after the first scan

Coverage does not stop at the first test. PentestOps re-checks your assets on a rolling cycle, flags configuration drift as it appears, and re-validates your internet-facing footprint on a schedule you choose, so you are never relying on a snapshot that is weeks out of date.

See it on your own environment. Book a technical demonstration.

EMAIL

info@pentestops.com

WEB

pentestops.com

PHONE

+61 1300 290 196

LOCATIONS

Australia

