SN1PER

WHITEPAPER · 2026 · BUILD 2026.1

THE NEXT-GENERATION ATTACK SURFACE PLATFORM

One offensive-security workspace for recon, scanning, vulnerability intelligence, and verified exploitation. Built for on-prem and air-gapped environments.

EDITIONS COVERED: **PROFESSIONAL** & **ENTERPRISE**

90+	10,000+	600+	Since 2014
INTEGRATED SECURITY TOOLS & APIS	NUCLEI DETECTION TEMPLATES	METASPLOIT EXPLOIT MODULES	BATTLE-TESTED IN THE FIELD

THE BUSINESS CASE

Your attack surface is growing faster than your team can test it.

Modern organizations expose thousands of internet-facing assets across cloud, hybrid, and on-prem estates. New domains, subdomains, ports, and services appear every week, and each one is an opportunity for an attacker. Point-in-time assessments and a drawer full of disconnected tools cannot keep pace with that drift.

$4.88M

Average cost of a data breach

IBM Cost of a Data Breach, 2024

$8,000+

Annual cost of the point tools Sn1per consolidates

Published list pricing, tool-stack math

80%

Of evaluators prefer or accept on-prem deployment

Sn1per trial-form responses

The fragmentation tax. Recon, port scanning, web testing, vulnerability assessment, threat intelligence, exploitation, and reporting typically live in separate products that do not share context. Analysts spend more time stitching output together than acting on it, and findings that only matter in combination slip through the gaps.

The visibility gap. You cannot defend what you cannot see. Assets discovered once and never re-checked become tomorrow's exposure. Sn1per continuously re-discovers the attack surface and flags what changed, so teams act on new exposure in hours rather than weeks.

The sovereignty requirement. Offensive tooling handles your most sensitive data: what is exploitable, and how. Sending that to a third-party cloud is a risk many security teams will not accept. Sn1per runs entirely inside your perimeter, including fully air-gapped deployments.

The consolidation opportunity. One platform that unifies the full recon-to-exploit workflow replaces thousands of dollars in overlapping licenses and removes the integration burden, without giving up the depth security operators expect.

THE CONSOLIDATION MATH

Web app scanning Burp Suite Pro · $499	**Vulnerability assessment** Nessus Pro · $3,390	**Threat intelligence** Recorded Future · $2,500+
Asset discovery Shodan · $828	**Pentest reporting** PlexTrac · $1,000+	**Exploitation** Metasploit & more

→

ONE PLATFORM, FROM

$984 / yr

Replaces ~~$8,000+~~ in separate annual licenses, with 90+ integrations in one workspace.

Figures cited from IBM, Verizon DBIR, and published list pricing only. Sn1per does not publish invented customer savings or unverifiable risk-reduction percentages.

THE SN1PER APPROACH

The best defense is the attacker's perspective.

Sn1per is an offensive-security and attack surface management platform, not a passive vulnerability scanner. It gives security teams an attacker's view of their organization and the tooling to act on it, all from a single self-hosted workspace.

One platform, not a toolbox

Recon, scanning, vulnerability intelligence, and verified exploitation share one workspace and one data model. Replace $8,000+ of separate point tools with 90+ integrations wired into a single reporting interface.

CONSOLIDATION

On-prem & air-gapped by design

Docker-first deployment on Kali, Ubuntu, or Debian. Your recon data, findings, and exploit context never leave your network. Offline-token mode supports fully air-gapped environments.

DATA SOVEREIGNTY

Coverage that verifies

27 scan modes across 12+ attack surfaces, with automated Metasploit, SQLMap, and Nmap scripts that confirm the exploitability of known vulnerabilities, so you prioritize what is genuinely exploitable rather than a wall of unvalidated CVEs.

OFFENSIVE DEPTH

ONE PLATFORM, 12+ ATTACK SURFACES

- Penetration testing
- Attack surface management
- Red team simulation
- Vulnerability scanning
- Bug bounty automation
- Threat intelligence
- Application security (DAST)
- Mobile pentesting
- Dark web monitoring
- Continuous monitoring
- AI-augmented testing

Positioned against modern attack surface platforms such as Pentera, Detectify, and Intruder, Sn1per pairs comparable offensive depth with on-prem control your security team can audit, at a fraction of the price. Trusted by **500+ teams** and battle-tested by the open-source community since 2014.

PLATFORM CAPABILITIES

Everything you need to run the full engagement.

27 scan modes

recon, web, stealth, airstrike, discover, vulnscan, fullportscan, masspwn and more, from Web UI, CLI, or API.

Web UI + CLI + JSON API

Drive Sn1per point-and-click, from the terminal, or programmatically. **JSON API** for CI/CD and SOC integration.

Recon & asset discovery

Continuous internal and external discovery of domains, subdomains, ports, services, and technologies with change notifications.

Verified exploitation

Automated Metasploit, SQLMap, and Nmap scripts confirm the exploitability of known vulnerabilities, not just version matches.

Live threat intelligence

Live CVE, exploit, and data-breach feeds from **20+ sources** keep detection current against emerging threats.

Unified reporting

Export the full attack surface and vulnerability findings to CSV, XLS, and PDF from one centralized interface.

8 ADD-ON MODULES · INCLUDED WITH PROFESSIONAL & ENTERPRISE, NOTHING EXTRA TO BUY

Command Execution · MassPwn · Nessus · Fuzzer · Brute Force · Port Scanner · Threat Intel · ReverseAPK

HOW IT WORKS

From discovery to decision, in one pipeline.

Every Sn1per engagement follows the same repeatable offensive workflow. Run it on demand, or schedule it daily, weekly, or monthly to catch attack-surface drift the moment it appears.

1 **Discover**
Map the full internal and external attack surface: hosts, ports, services, and technologies.

2 **Enumerate**
Recon and OSINT enrich each asset with subdomains, exposed repos, and threat intel.

3 **Scan**
27 scan modes plus 10,000+ Nuclei detections surface the latest CVEs and misconfigurations.

4 **Verify**
Automated Metasploit, SQLMap, and Nmap scripts confirm the exploitability of known vulnerabilities.

5 **Report**
Findings and risk scores roll up into the workspace and export to CSV, XLS, and PDF.

DEPLOYMENT STACK · ON-PREM, SELF-HOSTED, NO MANDATORY CLOUD DEPENDENCY

`Base:` Kali Linux | `Web:` Apache 2.4 | `Runtime:` PHP 8.4 | `Data:` PostgreSQL

`Deploy:` Docker 1338 → 1337 | `Auth:` SSL + Digest

RUN IT ONCE, OR RUN IT CONTINUOUSLY

Scheduled scans
Daily, weekly, or monthly engagements keep coverage current as your attack surface drifts.

Change detection
Get notified when new domains, URLs, or ports appear, so you act on new exposure in hours.

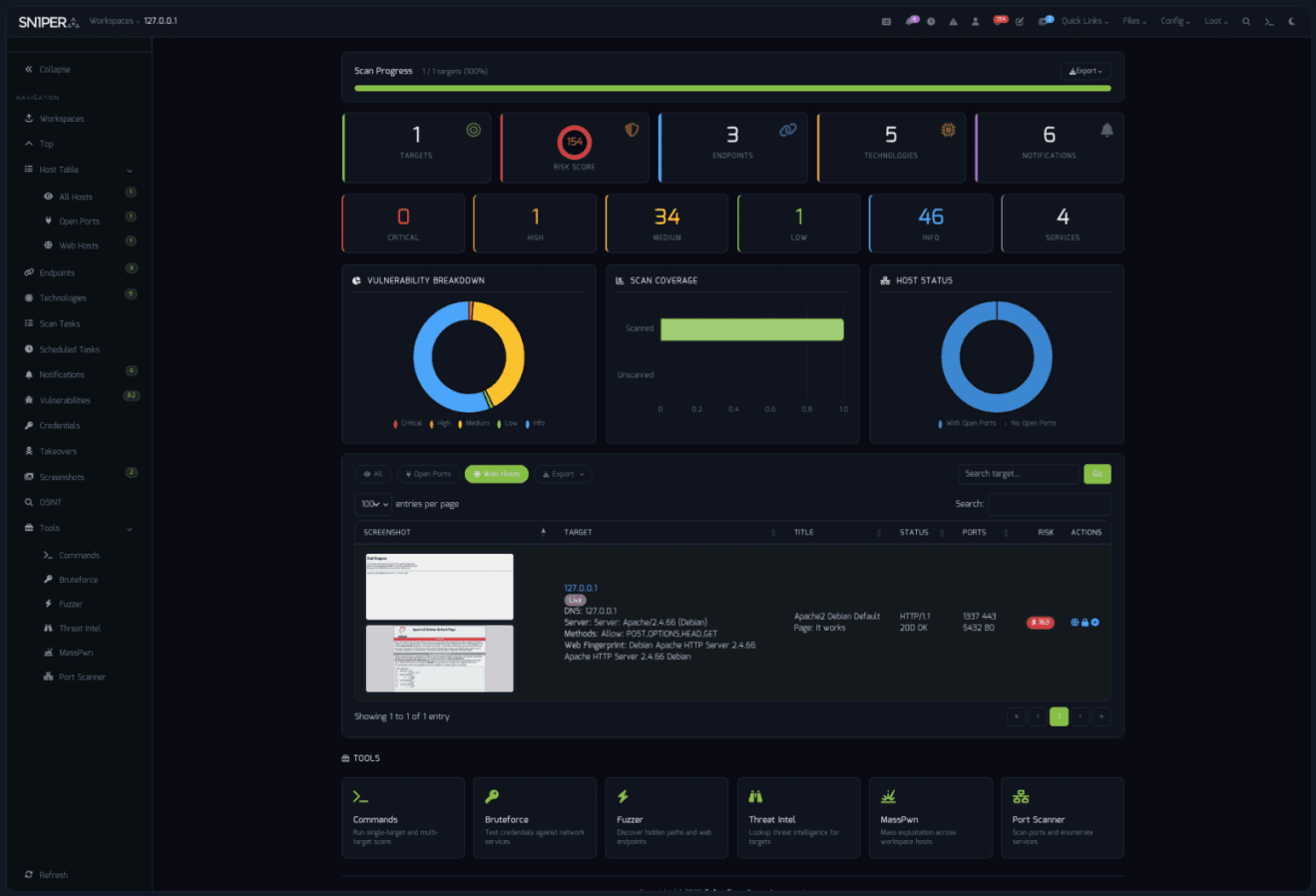
Stealth & airstrike
Throttled low-noise profiles and multi-target sweeps for red-team and large-scope work.

Runs on Kali Linux 2025.x, Ubuntu 24.04 LTS, Debian 12, or the official Sn1per Docker container. Single-command deployment; first scan in under 20 minutes.

PLATFORM INTERFACE

Built for security operators.

A modern 2026 web interface with a dark-first design system, severity dashboards, and per-workspace risk scoring, backed by the same scan engine on the CLI and JSON API.



Executive dashboard SEVERITY TILES · RISK SCORING · LAUNCHPAD

Workspace navigator PER-WORKSPACE RISK · TOP VULNERABILITIES

EDITIONS & PRICING

A tier for every stage of your security program.

Start self-serve with Professional and expand to Enterprise as your attack surface grows. Both editions ship every module and integration, on-prem, with a full year of updates and email support.

Professional

MOST POPULAR

PENTESTERS & SMALL TEAMS

$984 / yr per seat

- Professional Web UI, CLI, and JSON API
- 27 scan modes and all 8 add-on modules
- **30** assets/workspace · **5** workspaces · **150** total assets
- Unlimited scans · 1 licensed system
- On-prem, self-hosted, air-gap capable
- 1 year of email support and updates

Start with Professional

Enterprise

ORGANIZATIONS SCALING ASM

Custom pricing

- Enterprise Web UI, CLI, and API
- **Unlimited** assets and workspaces (500+ headline)
- Multi-instance distributed scanning ($SERVERS)
- Asset risk scoring and attack-path mapping
- Continuous monitoring and change notifications
- Centralized asset inventory and reporting (CSV, XLS, PDF)

Request an Enterprise quote

Enterprise is priced per environment. **Request a quote** for a deployment plan matched to your asset count.

EDITION COMPARISON

CAPABILITY	COMMUNITY	PROFESSIONAL	ENTERPRISE
Interface	CLI	Web UI + CLI + API	Enterprise UI + CLI + API
Assets per workspace	–	30	Unlimited
Workspaces	–	5	Unlimited
Add-on modules & integrations	Core engine	All included	All included
On-prem / air-gapped	Yes	Yes	Yes
Multi-instance scanning	–	–	Distributed ($SERVERS)

For context, comparable attack surface platforms are quote-only and materially more expensive: Pentera is estimated at $50,000 to $75,000 per year by third-party sources. Sn1per delivers on-prem offensive depth at a fraction of that, with pricing you can see.

SECURITY & ROI

Built to the standard it is testing for.

Sn1per is engineered with the same rigor it tests for, and it consolidates an entire offensive toolkit into one self-hosted platform, so security and savings arrive together.

SECURITY ARCHITECTURE

Encrypted access
SSL with HTTP Digest authentication; randomly generated admin credentials on install.

Hardened by design
CSRF protection, input validation, safe output encoding, and a data-access layer that replaces raw shell calls.

Your data stays put
On-prem and air-gap capable; offensive data never leaves your perimeter.

THE ROI MATH

$8,000+
in overlapping point-tool licenses, consolidated into one platform starting at $984 / year.

$4.88M
average breach cost that continuous, verified testing is designed to help you avoid.
IBM Cost of a Data Breach, 2024

500+	90+	27	Since 2014
Teams worldwide	Integrations	Scan modes	Battle-tested

See your organization the way an attacker does.

Deploy in minutes, fully on-prem. First scan in under 20 minutes.

Start with Professional | Book a live demo

Sn1perSecurity LLC · Independent US company · Developed since 2014, open-sourced 2015 support@sn1persecurity.com · sn1persecurity.com