VERSATILITY

Prove It

Rethinking Security Visibility in the Age of AI

Vikram Phatak

CEO, NSS Labs

Why We’re Here

Trust Isn’t Evidence

Regulators, boards, and auditors now demand proof your security controls actually work — not just that you bought them.

Deployed ≠ Effective

Dozens of tools across the stack, assumed to be working. Rarely validated. The gap between assumed and actual is widening.

AI Changes the Math

AI-accelerated threats outpace point-in-time testing. Can your products keep up?

How NSS Labs Tests

- We mirror the tactics real attackers use — real threats, real exploits, real evasions layered into millions of unique attack combinations. Tested in hyperscale cloud infrastructure.

- Every vendor tested against the same published methodology. Ratings published: Recommended, Neutral, or Caution. No marketing spin — just the data.

Real-World Testing at Scale

- A cloud infrastructure built for hyperscale testing with real-time validation against malware, exploits, evasions, and false positives.
- Decades of expertise from world-class test engineers.
- Enabling hundreds of thousands of real-world attack scenarios.

5,700+
Evasion samples for exploits & malware

10,000+
Curated exploit samples drawn from 250,000+ CVEs

15,000+
App and content samples for false positive testing

100,000+
Malicious URLs sourced daily

1,000,000+
“In the wild” malware samples

VERSATILITY

Versa’s Test Results

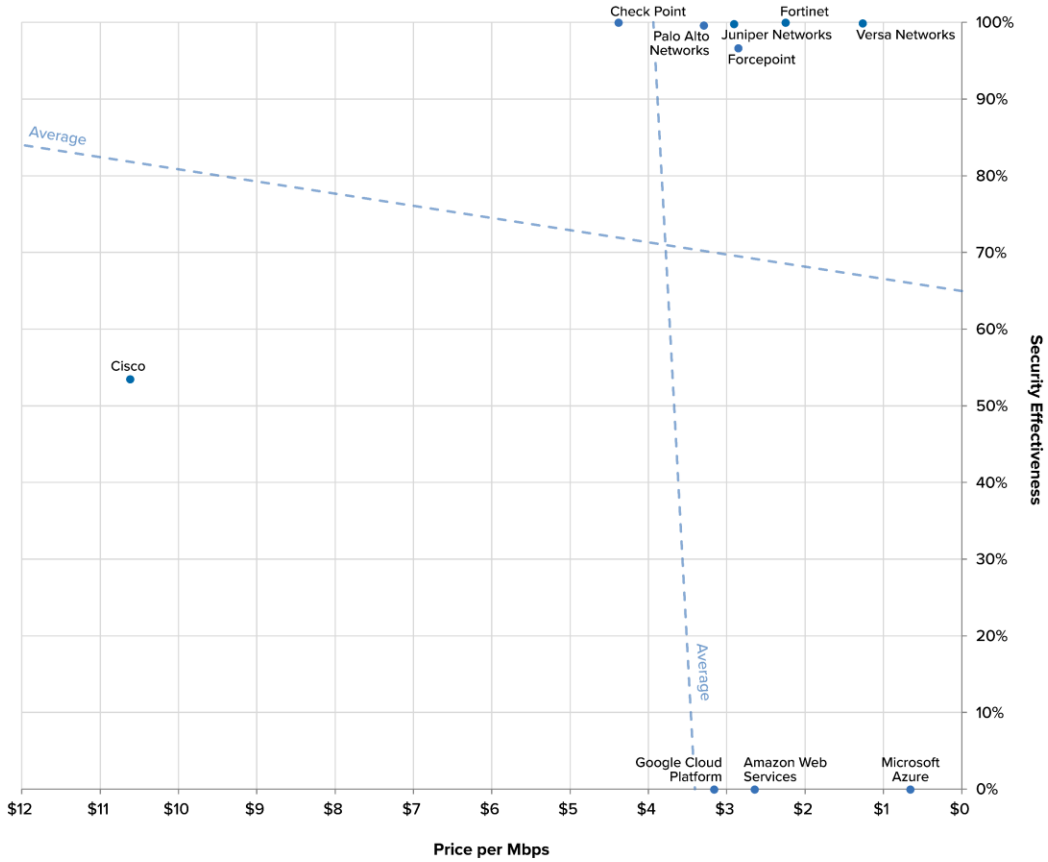
Independent, adversarial testing by NSS Labs

VERSATILITY

Cloud Network Firewall – Q1 2025

99.90% Security Effectiveness RECOMMENDED

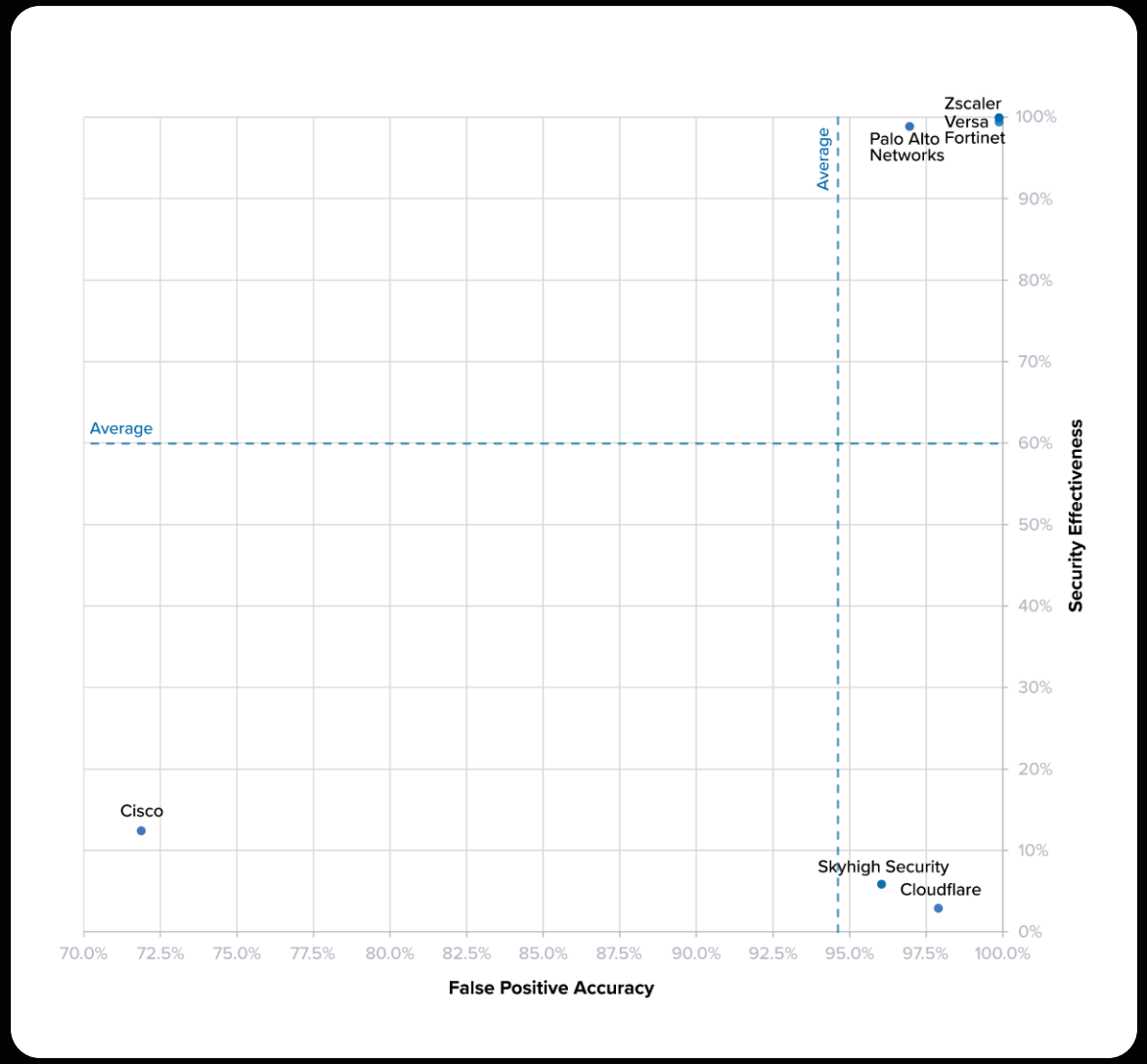
- Exploits: 2,028 attack samples from widely exploited vulnerabilities in enterprise environments
- Evasion Techniques: 2,500 attacks spanning 27 evasion techniques tested across multiple network layers to bypass firewalls
- 6 of 10 products were Recommended



Security Service Edge – Q3 2025

99.98% Security Effectiveness RECOMMENDED

- Near-perfect effectiveness across 205 exploits, 6,184 malware samples, 1,154 evasions
- 99.87% false positive accuracy — tied for highest
- Only 4 of 7 products earned Recommended

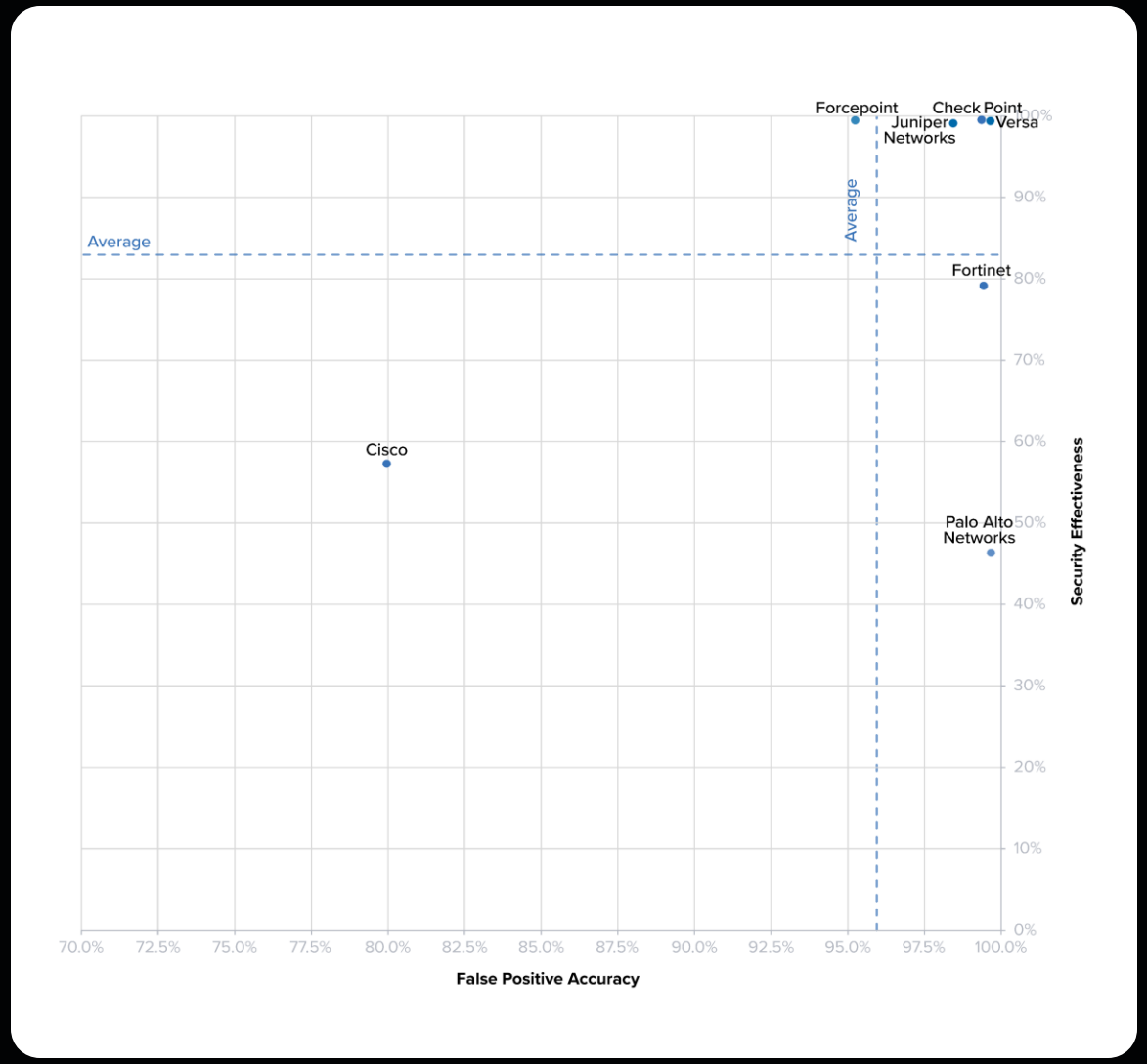


VERSATILITY

Enterprise Firewall – Q4 2025

99.43% Security Effectiveness RECOMMENDED

- 100% evasion resistance — 5,752 variations across 53 categories
- 7,626 Mbps rated throughput — highest in category
- 99.63% false positive accuracy
- Only 3 of 7 products were Recommended



Three Questions for Today

Do You Know What Your Security Stack is Blocking?

- Assumptions → Proof

Do You Know What Your Security Stack is Blocking… Today?

- Point in time → Continuous

Are Your Security Products Keeping Up with AI?

- Human speed → AI

Can Security Products Keep Up with AI?

- AI is accelerating the arms race. It’s now machine vs. machine.
- Attackers are using AI to generate novel exploits and evasions at machine speed.
- Manual defenses can’t keep up with the speed of AI.
- If your defenses are AI-driven, who watches the AI?

From Point-in-Time to Continuous

Point-in-Time Testing

- Tested once at purchase.
- Re-tested annually at best.
- Regulators will no longer accept it.
- Boards will no longer believe it.

Continuous Validation

- Always-on adversarial testing.
- Real-time visibility into effectiveness.
- Audit-ready evidence on demand.
- Required by modern GRC frameworks.

Meet Minion by NSS Labs

Continuous Proof of Security Effectiveness

- Decades of NSS Labs testing methodology — supercharged with AI, verified by engineers.
- Continuous Control Validation platform.
- Real attacks, real evidence, on your infrastructure.

VERSATILITY

How Minion Works

Security Control Validation Platform

- Minion deploys in your environment and runs adversarial tests against your security controls — at machine speed.
- Continuous validation that proves your security controls block real-world attacks.

What it tests

- Real-world malware, exploits, evasions, and false positives. Plus, our new AI Protection Systems (AIPS) test methodology — the first independent framework for evaluating enterprise AI security and AI guardrails.

What you get

- Executive dashboards, historical reporting, test version control, and audit-ready evidence mapped to NIST, PCI DSS, DORA, NIS2, and SEC frameworks.

Why Versa + Minion Wins for Your Customers

Buy with Confidence

- NSS Labs run PoCs
- Remote, repeatable validation
- Evidence of efficacy

GRC Differentiator

- NIST, PCI DSS, DORA, NIS2, SEC
- Audit-ready evidence by default
- Compliance edge competitors lack

Continuous Proof

- Ongoing validation after deployment
- Protect reputation
- Backed by data

Independent Credibility

- Third-party NSS Labs validation
- Proof you can hand to enterprise buyers
- Reports that satisfy procurement & risk

VERSATILITY

Prove It.

Thank you — Questions?