Turn Your NGFW Refresh into a Security Modernization Opportunity

Enterprises approaching a next-generation firewall (NGFW) refresh are at a pivotal decision point. Many organizations are being forced into costly refresh cycles by incumbent vendors with no meaningful gains in security effectiveness, performance, or architectural flexibility for cloud applications.

Versa Next Generation Firewall provides a modern alternative. It delivers independently validated top-tier security effectiveness among leading NGFWs, the best throughput rating, low total cost of ownership (TCO), and unified management across on-premises and cloud environments. These capabilities establish a clean, low-risk path to Zero Trust and Unified SASE.

Challenges of Legacy Firewalls and Their Refresh Cycles

Performance degradation

Ongoing refresh cycles have exposed long-standing limitations in their firewall deployments. As encrypted traffic becomes the default and hybrid environments become the norm, many existing NGFWs struggle to maintain performance when advanced security features such as TLS inspection, IPS, and malware prevention are enabled. This forces security teams into an unacceptable tradeoff between protection and user experience.

Security gaps in a rapidly evolving threat landscape

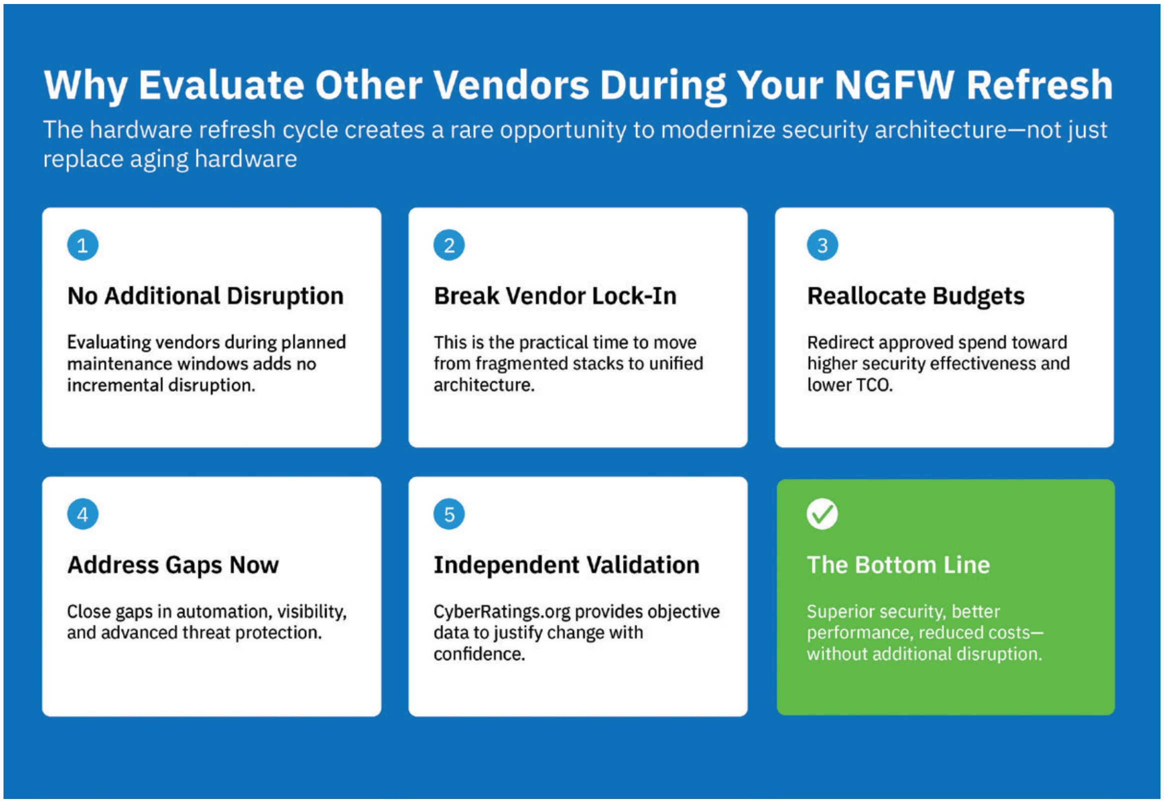
At the same time, the threat landscape has evolved. Today's attacks use evasion techniques, encrypted command-and-control channels, and AI-driven methods that legacy firewalls were never designed to handle. As a result, enterprises face increased risk just as they are making critical infrastructure renewal decisions.

Operational complexity and rising costs

Enterprises often manage multiple firewall platforms across branches, data centers, and cloud environments, each with separate consoles and upgrade cycles. Maintaining these fragmented systems creates operational overhead, while inconsistent visibility and policy enforcement increase risk. During refresh cycles, new licensing models, forced hardware upgrades, and unpredictable cost increases further raise the total cost of ownership without delivering meaningful architectural improvement.

Limited path to ZTNA or SASE:

Many incumbent firewall vendors offer cloud or SASE capabilities as bolt-ons rather than a unified architecture. Continuing with the same vendor often locks customers into another multi-year cycle without a clean migration path to Zero Trust or SASE.



Why Evaluate Other Vendors During Your NGFW Refresh

The hardware refresh cycle creates a rare opportunity to modernize security architecture—not just replace aging hardware

1

No Additional Disruption

Evaluating vendors during planned maintenance windows adds no incremental disruption.

2

Break Vendor Lock-In

This is the practical time to move from fragmented stacks to unified architecture.

3

Reallocate Budgets

Redirect approved spend toward higher security effectiveness and lower TCO.

4

Address Gaps Now

Close gaps in automation, visibility, and advanced threat protection.

5

Independent Validation

CyberRatings.org provides objective data to justify change with confidence.

✓

The Bottom Line

Superior security, better performance, reduced costs—without additional disruption.

Figure 1: Why is hardware cycle the right time to evaluate new NFGW vendors

Refresh cycle is the right time to evaluate other vendors

The NGFW hardware refresh cycle creates a rare opportunity to modernize security architecture, not just replace aging hardware.

Minimize disruption at crossroads

Firewall refreshes already require planned maintenance windows and operational coordination. Evaluating and switching vendors during this period adds no incremental disruption compared to replacing hardware with the incumbent vendor.

Align with next-gen firewall partner for future-proofing

Incumbent firewall vendors often force high-cost refreshes with limited innovation, relying on bolt-on cloud capabilities and fragmented security stacks. A refresh window is the most practical time to reassess long-standing vendor lock-in and move to a more unified architecture.

Get more out of pre-approved budgets

Refresh budgets are typically approved well in advance. This creates an opportunity to redirect spend toward higher security effectiveness, better performance, and lower total cost of ownership — rather than continuing to pay for the same limitations.

Address architectural gaps now

Continuing with the same vendor often means extending complexity, while threats, encryption, and hybrid environments evolve faster than legacy platforms. Refresh cycles are the right moment to close gaps in automation, visibility, and advanced threat protection.

Leverage independent third-party validation

Objective testing from CyberRatings.org provides clear, comparable data on security effectiveness, throughput, and cost per protected Mbps. This independent validation helps organizations justify change with confidence during refresh decisions.

Versa NGFW

Versa NGFW is purpose-built for modern hybrid enterprises. It combines advanced threat prevention, deep packet inspection, full TLS 1.3-encrypted traffic inspection, IoT and GenAI security, and ZTNA with other core NGFW features, delivering industry-leading security effectiveness and throughput.

Unlike legacy firewalls, Versa NGFW is designed to operate consistently across physical appliances, virtual form factors, and public cloud environments.

And in an independent assessment, it achieved the highest ratings on security effectiveness, throughput, and price/protected Mbps among all tier 1 vendors. (Figure 1)

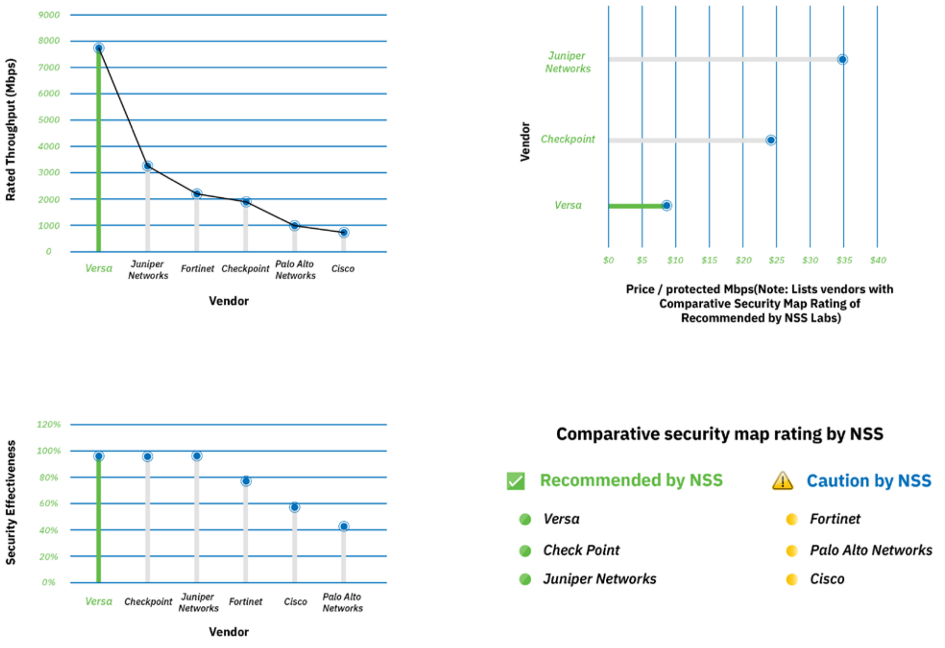
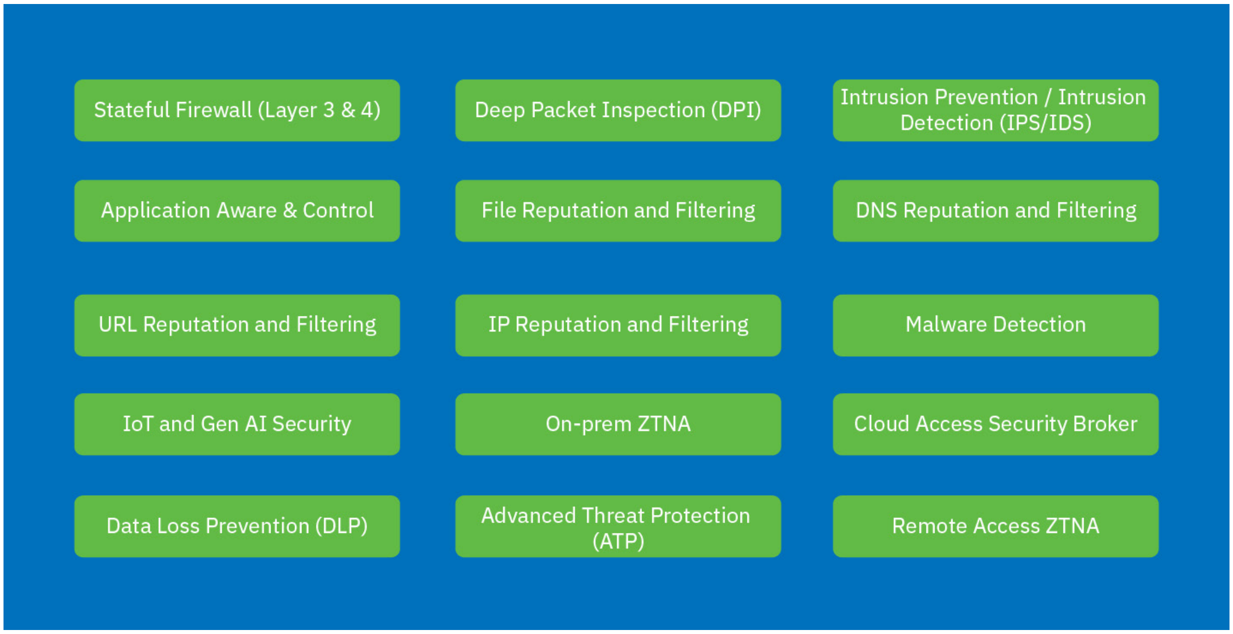


Figure 2: Versa NGFW NSS (Cyberratings.org) ratings, 2025

Critically, Versa NGFW is not just a standalone point product. It is also a foundational component of Versa SD-WAN and Versa's Unified SASE Platform, enabling organizations to address immediate firewall refresh requirements while future-proofing their security architecture for Zero Trust access, cloud security, and SASE adoption.

Versa NGFW Capabilities

Versa NGFW enforces security at the application layer using deep packet inspection, next-generation intrusion prevention, malware detection, and advanced threat protection (Figure 3). These capabilities operate at scale, allowing organizations to inspect encrypted and unencrypted traffic without degrading performance or disabling critical controls.



Stateful Firewall (Layer 3 & 4)

Deep Packet Inspection (DPI)

Intrusion Prevention / Intrusion Detection (IPS/IDS)

Application Aware & Control

File Reputation and Filtering

DNS Reputation and Filtering

URL Reputation and Filtering

IP Reputation and Filtering

Malware Detection

IoT and Gen AI Security

On-prem ZTNA

Cloud Access Security Broker

Data Loss Prevention (DLP)

Advanced Threat Protection (ATP)

Remote Access ZTNA

Figure 3: Versa NGFW capabilities

A single software stack and unified policy engine are used across all deployment models – on-premise, virtual machines, and public cloud environments (AWS, Azure, and GCP). Security teams define policy once and enforce it consistently across branch offices, campuses, data centers, and cloud workloads. A centralized management plane provides unified policy control, analytics, and telemetry across all deployments. Security teams gain end-to-end visibility, faster troubleshooting, and reduced operational overhead by managing a single, integrated platform rather than siloed firewall solutions.

Versa NGFW natively supports Zero Trust Network Access, software-defined micro segmentation, IoT/OT device fingerprinting, and data protection. Versa also provides LLM-aware controls that detect and govern GenAI usage and prevent sensitive data leakage into tools like ChatGPT and Gemini. All these capabilities allow organizations to limit lateral movement, protect unmanaged devices, and continuously adapt access based on user, device, and risk context. As requirements evolve, customers can extend from NGFW to full Unified SASE without forklift upgrades or re-architecting.

Why Versa?

Independently validated security and performance

Customers can realize measurable benefits by switching to Versa during an NGFW refresh. Independent testing has validated Versa NGFW's industry-leading security effectiveness, evasion resistance, and performance for encrypted traffic—key criteria that directly address most common reasons organizations replace firewalls.

Lower and more predictable total cost of ownership

From a cost perspective, Versa offers a lower, more predictable total cost of ownership. A software-defined architecture reduces reliance on frequent upgrades, while platform consolidation lowers licensing, operational, and infrastructure costs.

Purpose-built for hybrid environments

Versa provides true hybrid mesh firewall capabilities with consistent enforcement across branches, data centers, and cloud workloads—aligned with how enterprises operate today.

Why Choose Versa NGFW

- ✓ Achieved a 99.43% protection rate and a "Recommended" rating in independent CyberRatings (NSS) 2025 Enterprise Firewall testing.
- ✓ Delivers industry-leading encrypted traffic throughput with full security inspection enabled.
- ✓ Demonstrates superior price-per-protected-Mbps value when compared to incumbent firewall vendors.

Clear path to Unified SASE

Unlike point products, Versa NGFW is foundational to a single-vendor SASE architecture, with a single OS, policy framework, and management plane. Customers modernize incrementally, not through disruptive "rip-and-replace" migrations.

Thousands of enterprises globally rely on Versa NGFW as a core security control for Versa Secure SD-WAN and Unified SASE deployments, validating its scalability, reliability, and operational impact.

To learn more about how Versa NGFW delivers better security at a lower cost of ownership, explore Versa NGFW or request a demo.

VERSA

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
Tel: +1 408.385.7660 | Email: hello@versa-networks.com | Website: www.versa-networks.com