VERSA

SOLUTION BRIEF

Secure GenAI Usage

Gain Visibility, Control, and Compliance Across GenAI tools in the Enterprise with Versa GenAI Firewall

Generative AI (GenAI) is quickly becoming a mainstream enterprise productivity tool, but most organizations lack visibility into how users access and move sensitive data across GenAI web-based, copilots, and client-based solutions. Unapproved AI applications can cause data exfiltration and non-alignment with evolving AI regulatory mandates, introducing significant risk. Versa GenAI Firewall, part of Versa's Unified SASE platform, restores visibility and control over AI usage, enforces data protection, and ensures continuous compliance without adding operational complexity.

Challenges: GenAI Adoption Outpaces Security

With 65% of organizations regularly using GenAI, AI adoption has outpaced security controls. Security teams lack the visibility and tools to govern AI use, leaving organizations exposed to data loss, compliance failures, and cybersecurity attacks using GenAI vulnerabilities such as prompt injection.

GenAI Pain Points

Shadow AI Creates Blind Spots

ISSUE

Employees use unapproved GenAI tools without IT's knowledge.

IMPACT

IT/security teams cannot fully monitor data movement, creating visibility, audit, and security gaps.

GenAI Increases Data Exfiltration Risks

ISSUE

GenAI processes sensitive company data without DLP controls or oversight.

IMPACT

Organization faces increased breach risk and data loss.

Orgs Struggle to Meet Evolving Compliance Requirements

ISSUE

EU AI Act, GDPR, and other mandates introduce new AI governance requirements.

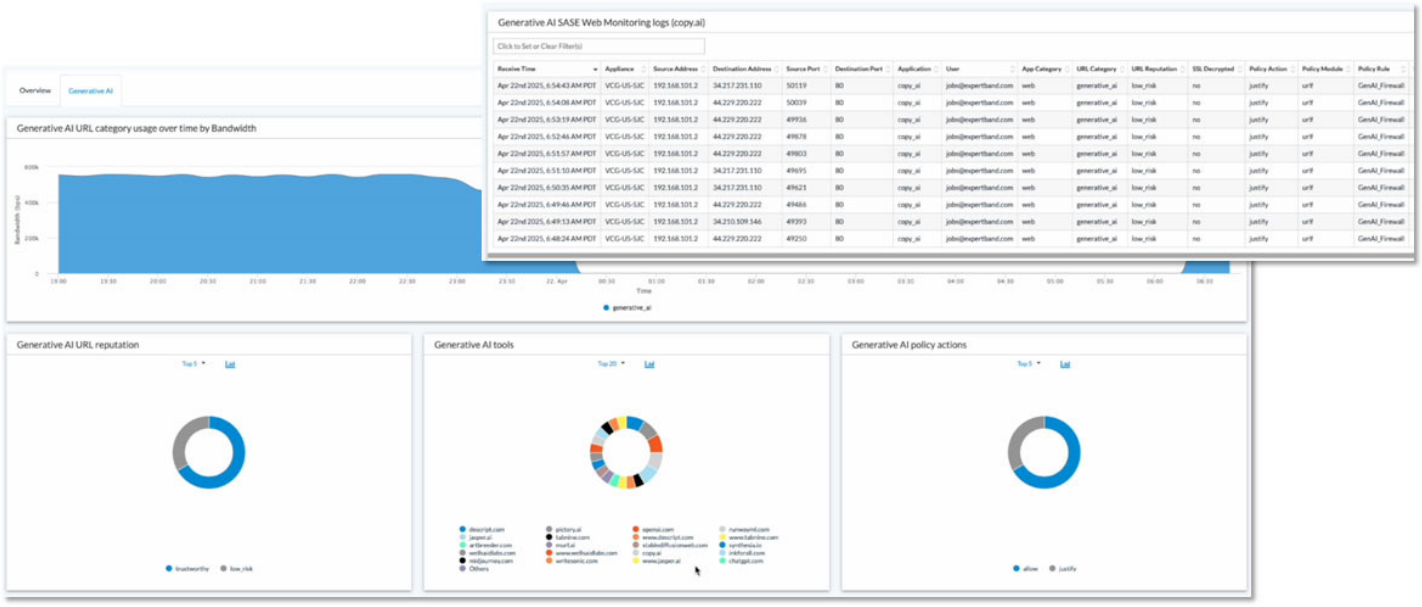
IMPACT

Organizations face penalties and brand damage for noncompliance.

Organizations need a security model built for the AI era that provides visibility into AI usage, prevents data leakage, and ensures continuous compliance without adding management overhead.

Versa GenAI Firewall

Versa GenAI Firewall provides end-to-end visibility and protection for enterprise AI use, integrated directly into Versa Unified SASE. This native approach eliminates security silos and delivers consistent visibility and control across all users and locations, even within encrypted traffic.



Versa GenAI dashboard and logs

Zero Trust for GenAI

Versa GenAI Firewall secures GenAI use by applying Zero Trust policies to AI tools, classifying them by risk level and enforcing admin-defined, least-privilege access. Versa further reduces the attack surface by allowing only authorized users access to approved AI tools and limiting risky actions, such as code or sensitive data uploads.

Unified AI Visibility and Control

Versa provides complete visibility into GenAI use across the enterprise, detecting both approved and unauthorized AI tools without agents or complex integrations. Network-native telemetry identifies GenAI activity, even in encrypted traffic, showing who is using which tools and what data is being accessed. Security teams can monitor, audit, and enforce policies across all users, devices, and environments from a single dashboard.

Data Leak Prevention

Versa GenAI Firewall prevents sensitive data from being exposed to AI tools by enforcing real-time data protection controls, ensuring secure GenAI use across the enterprise. Integrated DLP policies restrict risky actions, such as uploading source code, PII, or confidential data, to GenAI applications, reducing the risk of data exfiltration, including in cases with prompt injection attacks.

Versa GenAI Firewall Key Benefits

Complete AI Visibility

Detect and classify all GenAI traffic, reduce blind spots without agents and integration overhead

Secure AI Usage

Enforces Zero Trust for AI, preventing sensitive data uploads AI.

Simplified Compliance

Automated audit trails, policy-based controls, and reporting dashboards keep organizations audit-ready.

Unified SASE Architecture

Embeds AI governance natively into a single platform with networking and security.

Continuous Compliance

Versa GenAI Firewall enables compliance with AI regulations such as the EU AI Act and GDPR by enforcing policy-based controls and maintaining detailed audit trails. Built-in dashboards provide real-time visibility into GenAI risk and activity, helping organizations monitor adherence, support audits, and stay compliant as regulatory requirements evolve.

Unified SASE Platform for Streamlined Operations

Versa GenAI Firewall is natively integrated into Versa's Unified SASE platform, combining embedded AI governance with SWG, CASB, ZTNA, DLP, and SD-WAN under a single policy engine and management console. This unified architecture eliminates security silos, simplifies operations, and delivers consistent visibility and enforcement.

Why Versa

Versa GenAI Firewall delivers scalable AI governance built for modern, distributed enterprises. Versa integrates Security Service Edge (SSE) capabilities and industry-leading SD-WAN for a unified SASE platform powered by a single policy engine. This converged architecture provides visibility into AI usage without agents, delivering dynamic protection for GenAI-specific applications. Unlike endpoint-based discovery tools with limited traffic context, Versa classifies and enforces action-based protection natively through the SASE platform.

To learn more about how Versa GenAI Firewall secures AI adoption across enterprises, request a demo.

Explore Versa GenAI Firewall.

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