AI Category Vendor Integration

Secure, govern, and monitor enterprise AI usage while applying AI to protect data, users, applications, and network operations.

Key Benefits

- **Govern GenAI use** - discover and control sanctioned, tolerated, and risky AI applications.
- **Protect sensitive data** - inspect prompts, uploads, responses, and unstructured content before data leaves the enterprise.
- **Secure agentic operations** - broker AI tool use through Zero Trust MCP with RBAC, tenant isolation, approvals, and audit trails.
- **Detect advanced threats** - apply AI/ML to malware, user/entity anomalies, data leakage, and suspicious traffic patterns.

Challenges

Employees are rapidly adopting public and private AI tools such as ChatGPT, Claude, Gemini, and copilots, often faster than security teams can define acceptable-use policy. This creates shadow AI, sensitive data leakage, prompt and response exposure, and compliance risk. At the same time, attackers are using AI to obfuscate malware, automate phishing, and hide data exfiltration attempts, while network teams need safer ways to use AI automation without privilege sprawl or unapproved changes.

Solution

VersaONE integrates with AI vendors and brings AI security into the SASE enforcement path. Versa GenAI Firewall discovers and controls AI applications, inspects prompts and responses, and applies DLP profiles to prevent unauthorized data movement. Versa AI-powered DLP, ATP, UEBA, VANI, and security dashboards add contextual detection across users, devices, traffic, files, SaaS, private applications, and network behavior.
Verbo and Zero Trust MCP extend AI-assisted operations with brokered execution, RBAC, tenant isolation, human-in-the-loop approval, and audit trails, so AI can help without bypassing governance.

Business Value

Use Case/ Challenge	1. Employees use public AI tools without clear governance, creating shadow AI, data leakage, and compliance exposure. 2. Regex-only DLP and siloed security tools struggle with prompts, images, obfuscation, and fast-changing AI apps. 3. AI agents connected to network and security infrastructure need control, approvals, and auditability before taking action.
Solution	1. Enforce GenAI Firewall, AI-powered DLP, CASB, SWG, ATP, UEBA, ZTNA, and NGFW policy from VersaONE. 2. Inspect AI prompts, uploads, responses, and model destinations while applying user, device, application, and data context. 3. Use Verbo and MCP to broker AI-assisted operations through authorized APIs, RBAC, tenant isolation, and human approval.
Benefits	1. Safer adoption of ChatGPT, Claude, Gemini, Microsoft Copilot, private LLMs, and other AI services. 2. Faster detection of risky AI use, data leakage, malware, anomalous behavior, and degraded user experience. 3. Reduced operational friction through natural-language assistance, automated triage, and governed action workflows. 4. Stronger compliance posture with consistent policy, monitoring, reports, and audit trails.

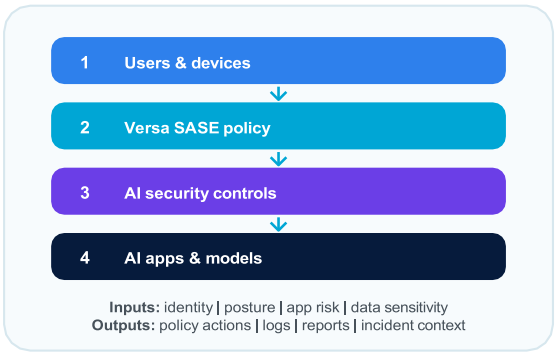
Technical Solution

Versa SASE AI security combines inline enforcement, AI analytics, and governed AI operations. Traffic from branches, campuses, remote users, and managed devices is inspected by the Versa SASE platform before it reaches AI applications and models. Policies can discover AI apps, categorize model risk, inspect prompts and responses, apply AI-powered DLP, block or ask users before risky actions, and generate usage reports. Operational AI clients connect through Versa MCP and Verbo, which translate natural-language requests into governed API workflows rather than direct autonomous access to infrastructure.

Category Capabilities

- Co-pilot: Conversational AI assistant for Versa help, configuration guidance, troubleshooting, and report generation.
- Data Protection: GenAI Firewall and AI-powered DLP inspect prompts, uploads, responses, text, images, and unstructured data.
- MCP: Securely connects AI clients to Versa Director and Concerto through brokered, RBAC-controlled API workflows.
- VANI: Anomaly detection, predictive insights, intelligent alerting, and troubleshooting for user experience and network health.

AI Security Integration Loop



- Threat Protection: AI/ML malware detection, ATP analysis, UEBA, and contextual analytics detect zero-day, insider, and evasive threats.

Vendor Integrations

Google Gemini	Anthropic Claude	OpenAI ChatGPT
AI application governance Apply SASE policy and DLP controls to Gemini prompts, uploads, and data movement.	AI DLP and MCP client use Secure Claude queries with policy enforcement and auditability.	Prompt and response protection Control ChatGPT access, inspect prompts, prevent data leakage, and report AI usage.

AI Security Workflows Enabled by Versa

Discover	Identify GenAI applications, sanctioned and unsanctioned AI use, shadow AI activity, model destinations, and user behavior.
Inspect	Analyze prompts, uploads, responses, files, and web traffic with GenAI Firewall, DLP, ATP, CASB, and SWG controls.
Govern	Apply policy by user, device, group, location, app reputation, AI risk category, and data sensitivity.
Automate Safely	Use Verbo and Zero Trust MCP for natural-language operations with authorization checks, approvals, audit logs, and tenant isolation.

Additional AI ecosystem integrations include: Microsoft Copilot, private LLMs, GitHub Copilot, Perplexity, enterprise AI gateways, SIEM/SOC platforms, and ServiceNow-style ITSM workflows.

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

About Versa
Versa, the global leader in unified networking and security, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE Platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while providing a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users, trust Versa with their mission-critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock. For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.

Part# SB_SASE-AISECCAP-01.0