VERSATILITY

Security Where Work *Actually Happens*

Extending Zero Trust enforcement into the browser session-where users interact with SaaS, GenAI, and enterprise data every day.

Akshay Adhikari, Distinguished Engineer

Anusha Vaidyanathan, Sr. Director, Product Management

The Workspace Has *Moved*

90% of enterprise work now happens inside browser tabs-SaaS, GenAI, internal portals. The browser isn't a window to work. It is the workplace.

Your SASE stack secures managed traffic. But browser-local actions-clipboard transfers, screenshots, prompt edits on cert-pinned apps-never hit the network. On BYOD and contractor devices, even managed traffic is out of scope.

90%

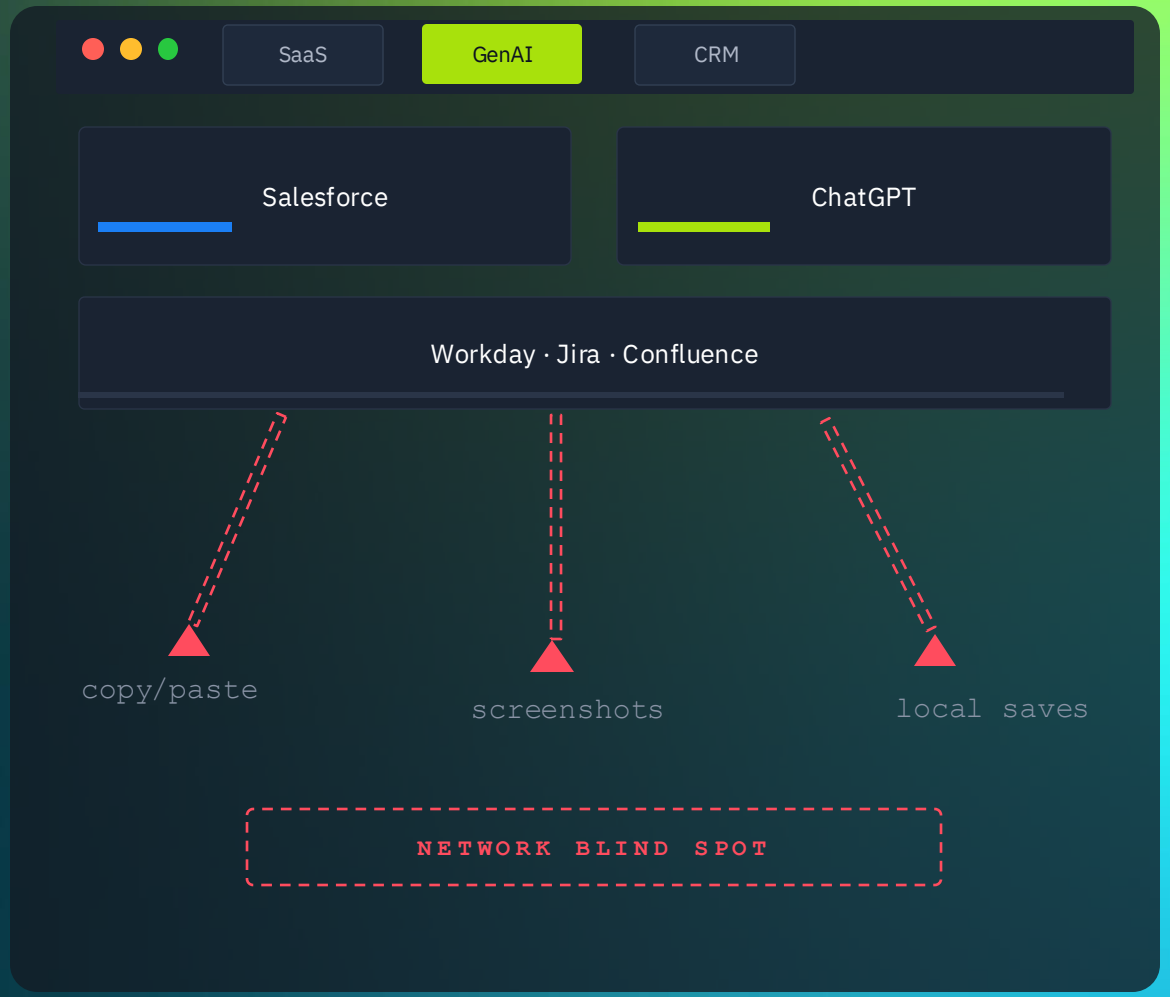
WORK IN BROWSER

75%

USE GENAI DAILY

0%

BROWSER-LOCAL VISIBILITY



VERSATILITY

Monday Morning at *Acme Corp*

A contractor. A personal laptop. No SASE client. A local LLM. Your policies exist-but every action stays off the network.

9:01 AM

Opens Salesforce

Downloads customer list-12K records with PII and deal values. Direct to internet, bypassing your SWG.

DLP: NOT IN PATH

9:04 AM

Pastes into Local LLM

Copies customer PII from Salesforce tab, pastes into a locally running model (Ollama, LM Studio). Zero network traffic generated.

NETWORK: NOTHING TO INSPECT

9:06 AM

Saves to Notepad

Pastes AI analysis with proprietary data into a local file. Browser-to-OS clipboard-no network request, no DLP trigger.

DLP: NOTHING TO INSPECT

9:08 AM

Data Exfiltrated

12K customer records analyzed locally and saved to an unmanaged device. No network trace. No audit trail. No alert.

ZERO CONTROLS IN PATH

Monday Morning at *Acme Corp*

A contractor. A personal laptop. No SASE client. A local LLM. Your policies exist-but every action stays off the network.

- User visits uncategorized malicious website by mistake
- Website Javascript reassembles malicious file from HTML and triggers a download
- File doesn't get scanned for malware

The Missing Layer:

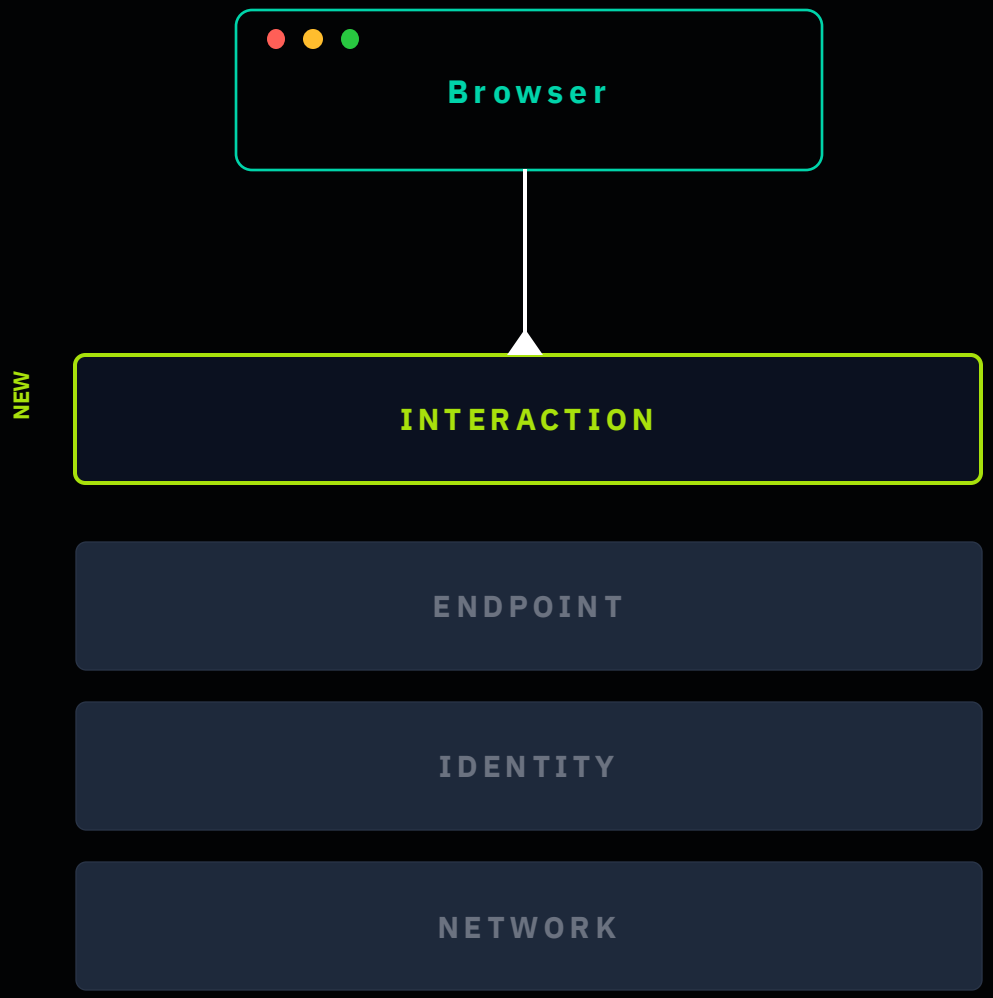
Interaction-Level and Last Mile Security

Security evolved from network perimeters to identity to endpoints. The next frontier is the interaction layer-controlling what users do inside browser sessions, in real time, with full context. Especially on devices your network controls can't reach.

The browser is the right enforcement point: it sees user intent before data moves. No TLS decryption required. Clipboard, paste, print — all intercepted pre-exfiltration. Even HTML smuggling attacks that bypass SWG are contained at the browser level.

The browser is the enforcement point. Not replacing SWG or CASB-extending your stack into the browser session itself, on any device.

Network → Identity → Endpoint → **Interaction**



VERSATILITY

Solutions

Versa Remote Browser Isolation

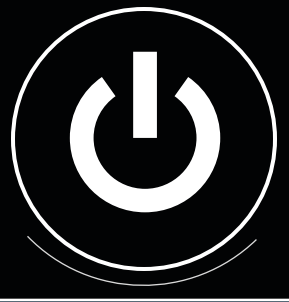
Improving security posture with differential access to protect against malicious threats and data exfiltration

Functionality

- Render a safe visual stream of websites
- Filter out active content
- Prevent malware
- Prevent data leaks

Actions supported

- Render sites in read-only mode
- Allow/Block uploads and downloads
- Preview downloads: Convert documents to pdf for preview
- Scan file transfers for malware
- Apply DLP policies to file transfers
- Control clipboard access, printing
- Block cookies



Powered by:

- DOM Mirroring
  - Filters active DOM content
  - Streams safe DOM elements to client browser
- Pixel Streaming
  - Visual stream rendered onto canvas
- Support for audio/video streaming
- Works with any HTML5 compliant client browser -- Chrome, Edge, Firefox, Safari

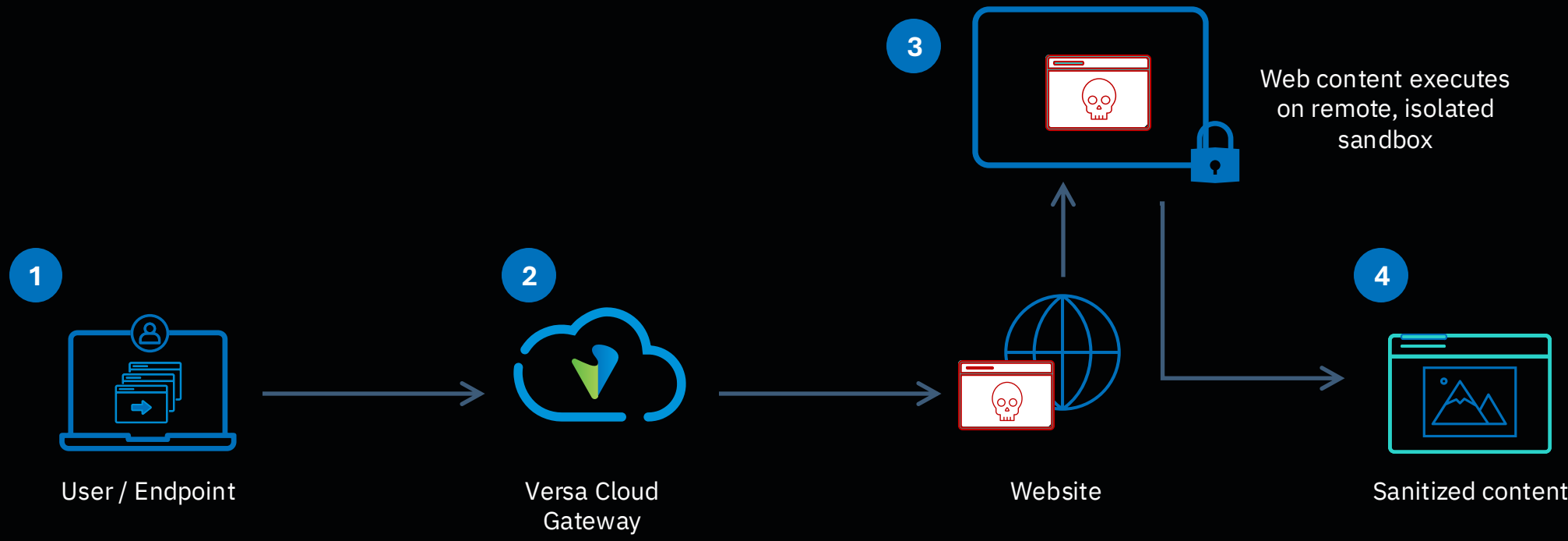
Versa RBI: Highly responsive, native experience – the *next best thing* to browsing in real time

VERSATILITY

** Additional licensing required for RBI*

How RBI Works – Client based access

1. User enters URL
2. VCG applies policies and evaluates the URL in question
3. Risky sites open in isolated browser
4. DOM Mirroring or Pixel Streaming renders the page allowing safe downloads, uploads, clipboard governed by policy



VERSATILITY

Context Aware Policy

Centralized via Versa Concerto. Dynamic policy based on user, group, device posture, URL category, geolocation, and risk score.

POLICY RULE-"GENAI DATA PROTECTION"

MATCH

Users	**Engineering, Finance**
Applications	**ChatGPT, Gemini, Copilot**
URL Category	**Generative AI**
Device Posture, User Risk	**Any**
Geolocation	**US**

ACTION

Read Only	**No**
Clipboard	**Block**
Upload	**Block**
Download	**Allow**
Print	**Allow**

RBI with clientless access/Private Apps

Clientless App access offered through Privileged Access Management (PAM)

Clientless App access includes –

- Support for RBI for SaaS apps
- Support for RBI for Private apps

Example Use Cases

- **Risky URL Isolation:** Isolate uncategorized or suspicious URLs instead of blocking outright
- **Phishing & Credential Protection:** Render email-linked pages in isolation to block credential harvesting
- **Device Posture-Based Access:** Enforce differential controls based on endpoint health — block downloads in RBI sessions where antivirus is disabled or disk encryption is not enabled
- **Contractor & BYOD Access: Private application access for contractors without VPN client**

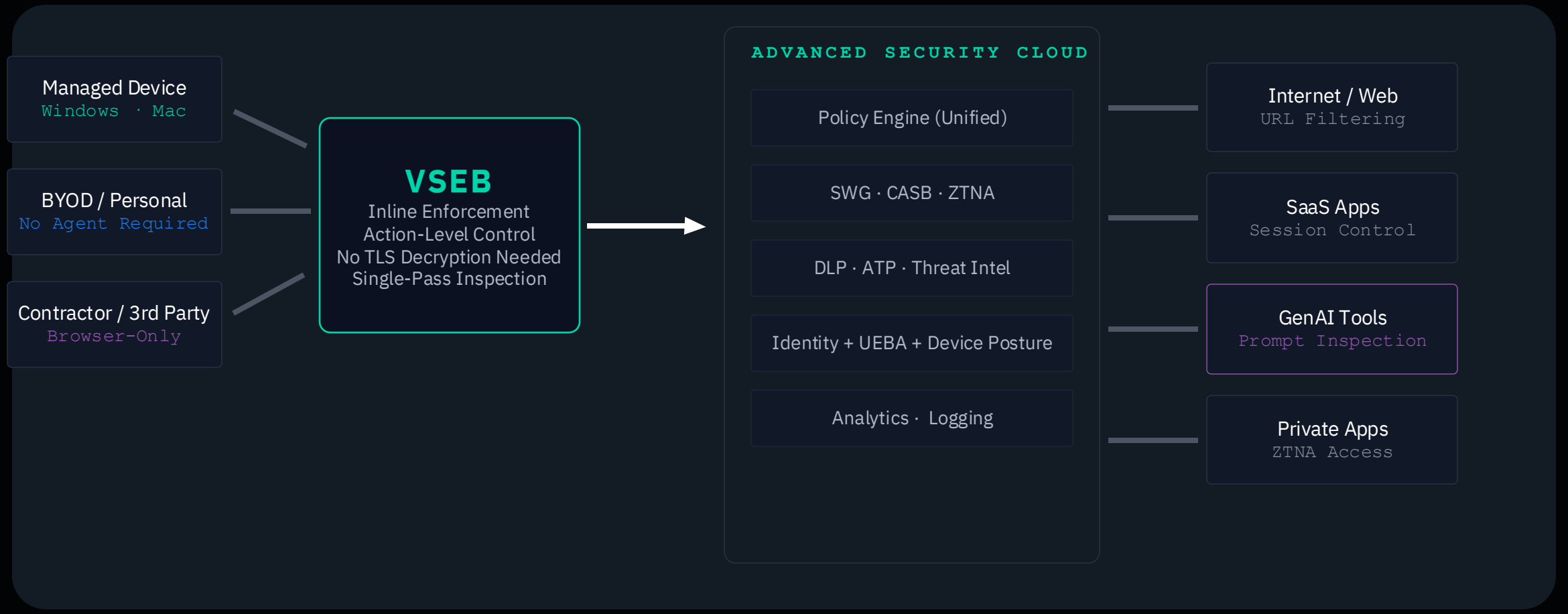
Versa Secure Enterprise Browser

ROADMAP

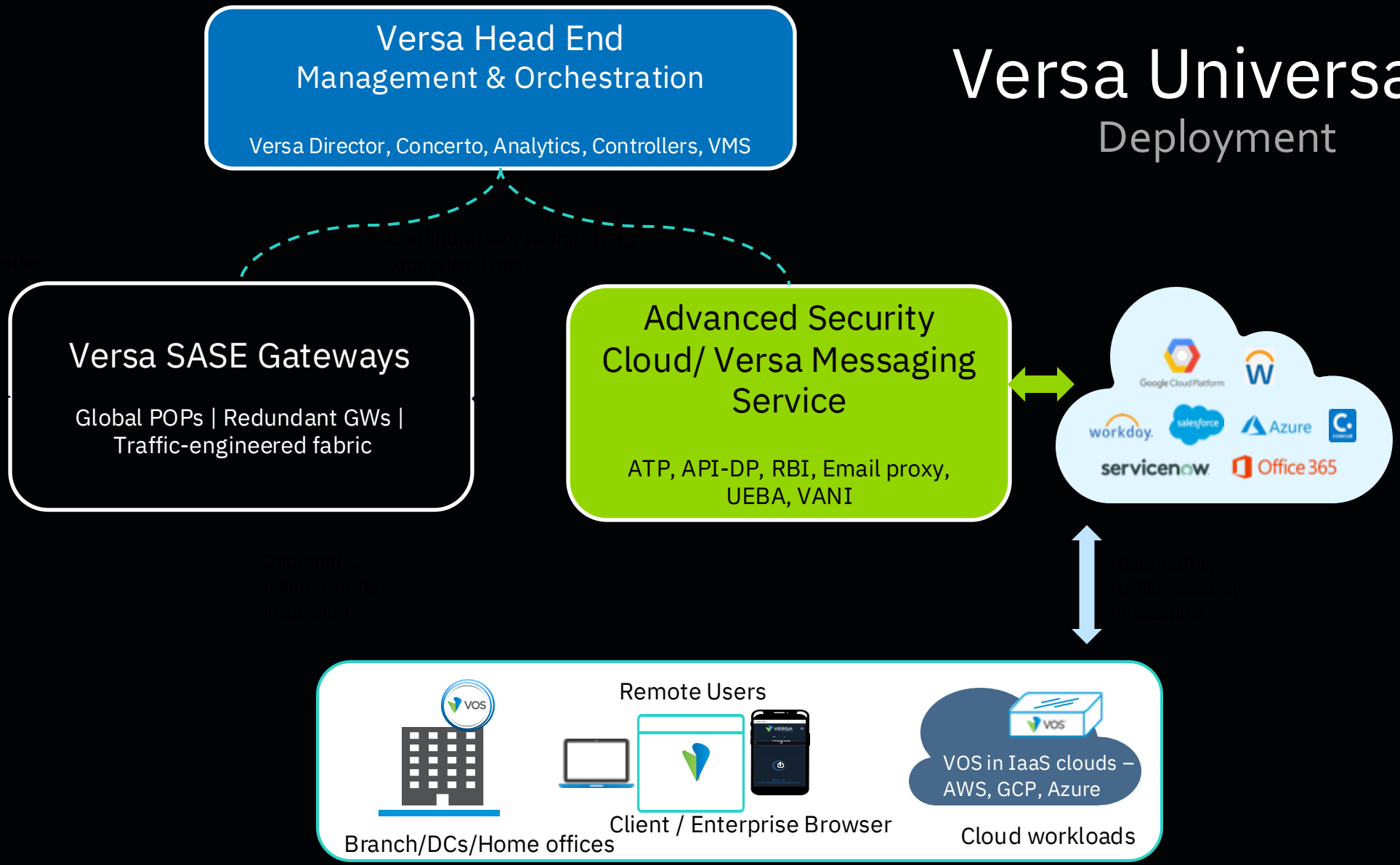
- Centrally managed secure browser
- Secures access to internet, SaaS and private applications
- Provides a familiar (but secure) browsing experience
- Improves “out-of-box” privacy and security of the browser
- Protects from sensitive data exfiltration
- Based on the open-source chromium browser platform

VSEB Architecture: *Inline, Unified, Zero Trust*

Same policy engine, same Concerto/Director, shared data plane services as your Versa SASE deployment. Not a silo.



Versa Universal SASE
Deployment



VERSATILITY

Browser-Level Threat Prevention & Data Protection

Threats that bypass network controls are caught at the browser. Last-mile defense before content reaches the user.

WEB-BORNE THREAT DEFENSE

- √ **Malware scanning on downloads**
- √ **URL filtering for phishing and malicious sites**
- √ **HTML smuggling containment**
  Malware reassembled in JS is caught at the browser before file system write
- √ **Zero-day isolation via RBI integration**
  Risky/uncategorized sites rendered in sandboxed remote browser

BROWSER HARDENING

- √ **Extension permission control**
  Block extensions requesting cookie access, traffic proxy, or broad host permissions
- √ **Extension allow/deny lists**
- √ **Disable JavaScript JIT compilation**
- √ **Certificate and TLS policy enforcement**
  Enforce DNS-over-HTTPS, HSTS, block ability to ignore certificate verification errors
- √ **Controlled browser update cycles**

DATA PROTECTION AT THE EDGE

- √ **Content-based file transfer controls**
  DLP scans file content, not just the upload/download action
- √ **Content-based clipboard controls**
  DLP scans clipboard content, not just the paste action
- √ **Content-based print controls**
  DLP scans print content, not just the print action
- √ **On-page content redaction**
  PII and sensitive data masked at DOM level before rendering
- √ **Screenshot and screen recording protection**
- √ **Session watermarking (visible/invisible)**
- √ **Encrypted download with VSEB-only access**

Private Application Access

- Access to private applications without requiring VPN client
- Integrates with the rest of the ZTNA components
- Access policies based on
  - User identity
  - Device posture
  - Geolocation

Application and activity visibility

- Security Events
  - Malicious URLs blocked
  - Malicious downloads blocked
- Activity Events
  - Application access
  - File transfers
  - Clipboard access
  - Print
  - Logins

Context Aware Policy

Policy as *ACL*

Think of browser enforcement like a firewall ACL- match conditions, then action per interaction type. Granular, programmable, instantly familiar to any security architect.

Centralized via Versa Concerto. Dynamic policy based on user, group, device posture, URL category, geolocation, and risk score.

POLICY RULE-"GENAI DATA PROTECTION"

MATCH	
Users	Engineering, Finance
Applications	ChatGPT, Gemini, Copilot
URL Category	AI / ML Tools
Device Posture, User Risk	Any
Geolocation	US

ACTION	
Navigate	Allow
Clipboard Paste	Block
Upload	Block
Download	Allow
Screenshot	Allow
Printing	Allow
Watermark	Enabled
Text Masking	Enabled

Context-Aware Policy in Action

Same policy engine, four different contexts. Identity, device, app, location — every dimension shapes enforcement.

Finance Analyst on BYOD

Group: Finance · Device: Unmanaged · App: Internal CRM · Geo: Office country

Browse: **Allow** · Download: **Block** · Clipboard Out: **Block** · Page PII: **Redact** · Watermark: **On**

Developer with Local AI Tools

Group: Engineering · Device: Managed · App: GenAI application · Content: Source code

Browse: **Allow** · Clipboard In: **Block (code patterns)** · Upload: **Block** · Activity: **Logged**

Marketing using ChatGPT

Group: Marketing · App: ChatGPT · Risk: Low · Device: Managed

Browse: **Allow** · Prompt: **Inspect for PII** · File Upload: **Block** · Session: **Monitored**

Contractor Accessing HR Portal

Identity: External · Device: Any · App: HR Portal (private) · Geo: Allowed countries

Access: **VSEB only** · Download: **Encrypted** · Screenshot: **Block** · Print: **Disabled**

Two Use Cases That Drive Immediate ROI

GENAI SECURITY

Browser-Native Prompt Inspection

Inspect GenAI inputs at the DOM level-works on cert-pinned apps that bypass TLS decryption. Extends your GenAI Firewall into the browser.

Clipboard & Paste Control

Block copy/paste of sensitive content into AI tools-browser-local actions invisible to network DLP.

Control file uploads

Block uploading of files with sensitive content

Browser-Local Action Logging

Capture clipboard transfers, prompt edits, and in-page interactions that never generate network traffic. Complements your Shadow AI dashboard.

BYOD & 3RD PARTY

No Agent, No VPN

Extend your SASE policies to any personal device via managed browser session. No endpoint software. No VDI overhead.

Browser-Based Posture Checks

Assess OS version, browser configuration, and patch level via browser signals-basic posture validation without an agent.

Secure workspace - Encrypted Downloads

Files encrypted with user identity key. Accessible only through authenticated browser session.

Contractor Access

Give third parties access to private apps through browser-no VPN, no managed device. Same Director policies you already manage.

Same Monday. With VSEB.

Same contractor, same personal laptop, same browser tabs. But now VSEB is the managed browser-your policies are in the path.

Opens Salesforce

Attempts to download customer list. VSEB DLP policy detects PII content-blocks download at the browser level.

DOWNLOAD BLOCKED

Pastes into Local LLM

Clipboard paste detected by VSEB. Sensitive data identified inline before it leaves the browser.

PASTE BLOCKED + LOGGED

Saves to Notepad

Sensitive content on page redacted before reaching OS Clipboard

CLIPBOARD REDACTED

Compliant Work Continues

Non-sensitive browsing and app access works normally. Zero friction for allowed use.

ZERO DATA EXFILTRATED

Market *Validation*

The enterprise browser category is accelerating. Analyst recognition and market data confirm the shift.

G

Gartner Prediction

By 2030, enterprise browsers will be the core platform for delivering secure digital workforce experience-managing 70% of web-based productivity.

$

Market Growth

Enterprise browser market projected to reach $3.2B by 2028, growing at 25%+ CAGR driven by SaaS adoption and GenAI data protection needs.

V

RSA 2026 Launch

VSEB announced at RSA Conference 2026-extending Versa's unified SASE platform into the browser workspace.

Where VSEB Fits in Your Versa Deployment

Existing Versa Customer

- Same Concerto console you already manage
- Same policy engine — extend existing rules to browser
- Same ATP and DLP profiles applied inline in session
- Incremental deployment, no infrastructure change
- Unified analytics across network + browser

New to Versa

- Start with VSEB as first touchpoint
- Expand to full SASE when ready
- No rip-and-replace required
- Chromium-based — zero user retraining
- Cloud-delivered, rapid deployment

Browser Security Evolution

RBI isolates. VSEB enforces. Together, they cover the full spectrum of browser security.

RBI — ISOLATE RISKY SESSIONS

- Air-gapped isolation of risky or uncategorized sites
- Zero-day vulnerabilities contained in sandbox
- Remote browser renders site, streams safe visual (DOM or pixel)
- Active content filtered before reaching client
- Basic DLP: clipboard, print, download controls

Best for: **high-risk browsing, sandboxed access**

VSEB — ENFORCE DAILY-DRIVER SECURITY

- Centrally managed Chromium browser on user devices
- Full-featured content-based DLP (clipboard, upload, download, page redaction)
- Screenshot protection and watermarking
- Browser extension control and hardening
- Encrypted downloads viewable only in VSEB

Best for: **all-day SaaS, GenAI, BYOD, contractors**

VSEB + RBI — UNIFIED

- VSEB integrates with RBI for risky site isolation
- Policy-driven: trusted sites in VSEB, risky sites routed to RBI
- Seamless user experience, context-aware switching
- One Director console manages both
- Full coverage: daily work + high-risk browsing

Best for: **Complete browser security posture**

Not a migration, not a replacement. RBI and VSEB are complementary tools within the same Versa platform, managed from a single console.

When to Use What

Criteria	Enterprise Browser	Versa SASE (SWG/ZTNA)
Applications	Secure all web traffic	Secures non-web and web traffic including laptop apps
TLS Decryption	Secures certificate pinned apps that cannot be inspected	Requires inline TLS decryption to break and inspect traffic for threats or data exfiltration
Security	Sophisticated last-mile attacks like HTML smuggling can be inspected and blocked	Application-level attacks cannot be protected in transit
Deployment	Requires new browser on user device	Solution is transparent to the end user
Security add-ons	Built in DLP for browser-based redaction, Cloud DLP add-on does additional file-based DLP inspection, Cloud ATP for malware detection	Inline+API-based+Email proxy DLP are add-ons
Security enforcement	Enforcement in the local browser and user device	Stops malware from propagating in the network, protects other enterprise users
Complements	Versa SASE	RBI + Enterprise Browser

Questions?

Thank You

VERSATILITY