VERSATILITY

Versa Blueprint for Data Centers

Dogu Narin & Rajesh Kari

Three Forces Reshaping the Datacenter

Sovereignty

70%+

of global countries with strict data localization laws by 2026

EU AI Act, GDPR, India DPDP, China Data Laws and others. Forcing function to a distributed yet in-country and localized datacenter footprint

[Coherent]

Security

75%

of enterprises actively consolidating security vendors with single-vendor SASE

Datacenters are being rebuilt around identity-aware, policy-enforced, inspection-everywhere fabrics with SSE/SASE extending into the datacenter.

[Gartner]

AI

70%

of global datacenter demand will be driven by AI in 2026

Performance, connectivity, and low-latency access to AI inference, data, and AI apps are placing significant demands on datacenter connectivity

[McKinsey]

VERSATILITY

Challenges with Current Data Center Solutions

Sovereignty

68%

of banks updated their datacenter vendor assessments in 2024 –25 to address sovereignty requirements

- Workloads can be placed in-region, but management planes often run from foreign cloud control regions which exposes data
- Legacy datacenter fabrics were designed to route packets for performance, not for residency
- Each new sovereign region typically means another firewall instance, another segmentation tool

Kiteworks

Security

90%

of organizations experienced a security incident involving lateral movement in the prior year

- Legacy datacenters were secured north-south while implicitly trusting east-west traffic
- Newer traffic like AI Apps, agents, MCP and similar protocols were not in scope with existing security stack
- Legacy security stack did not include all SSE capabilities in the datacenters

Elisity

AI

40%

of AI performance stalls are due to communication bottlenecks and network failures

- With AI multi-terabyte assets that need to move between training clusters, inference sites, and edge locations
- Lack of congestion control, multi-path bandwidth aggregation, and integrated security
- Legacy solutions constantly fail to meet the latency SLAs that AI applications need to be useful at the user's endpoint

North Star

The Right Solution for Today's Secure and AI-ready Data Centers

Sovereignty

Sovereign-by-design, jurisdiction-aware distributed fabric

Security

Zero Trust extended to every workload, every flow, and every AI agent

AI

AI-grade, low-latency, high-bandwidth distributed fabric with edge inference and AI-aware observability

VERSATILITY

Versa Data Center Solution

Versa's Edge-to-Cloud Data Center Solution

Sovereignty

Intelligent Fabric for AI and Enterprise Workloads

Unified L 7 Software-Defined Data Center F ic

VOS unifies L2–L7 services including routing, segmentation, security, and traffic engineering. EVPN/VXLAN overlays connect AI racks to enterprise workloads with application-aware, SLA-driven intelligence.

Security

Inline Zero Trust & Micro-Segmentation on DC Edges

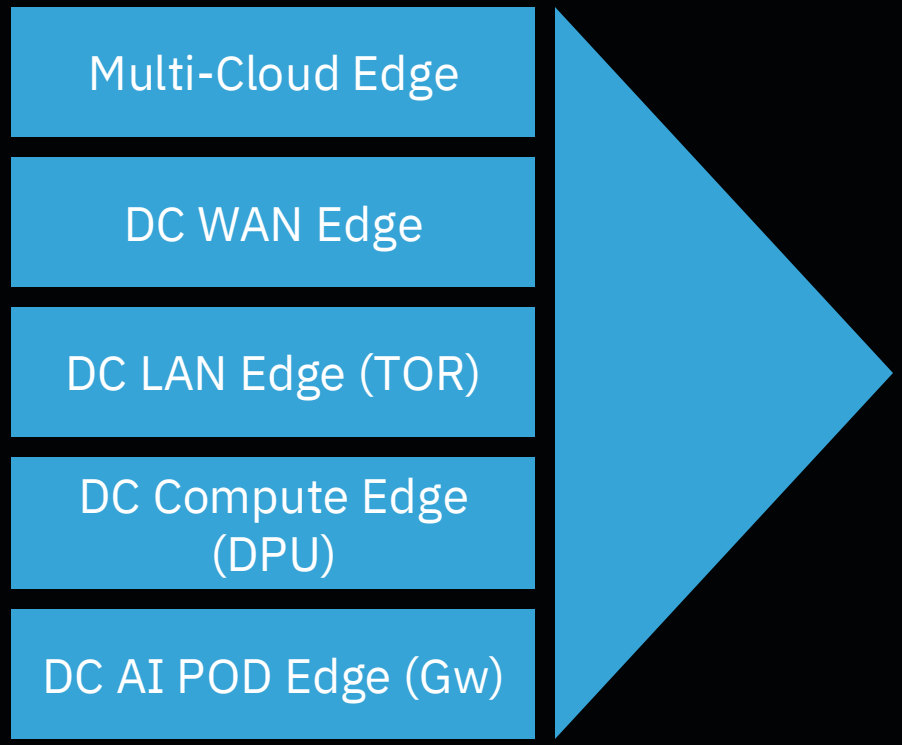
Deploy on Versa SD-NICs within compute systems or dedicated switches. Provides inline micro-segmentation and ZTNA access control to AI clusters while bridging classical and modern data center segments.

AI

AI-Ready Distributed Architecture

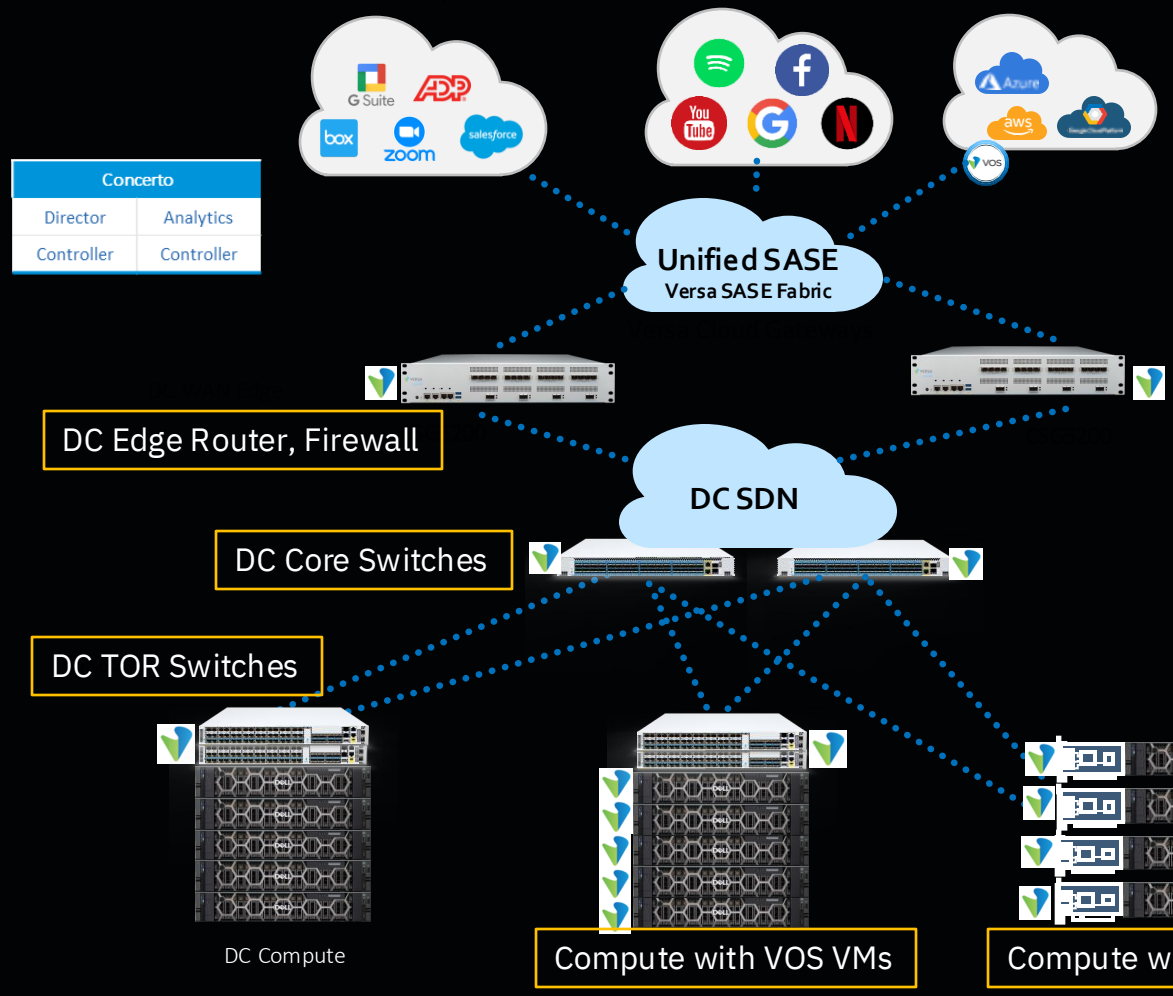
Purpose-built for AI with low-latency, high-bandwidth fabric, multi-path traffic engineering, and AI-aware observability across DC, WAN, and edge.

Connectivity and Security from Network Edges



- L2-L3 for connectivity – overlays for connecting edges
- Segmentation / micro-segmentation
- Security posture assessment
- L4-7 security
- User identity
- Device identity
- ZTNA
- Policy based traffic control, enforcement
- AI Security

Versa's Data Center Solution for Enterprises

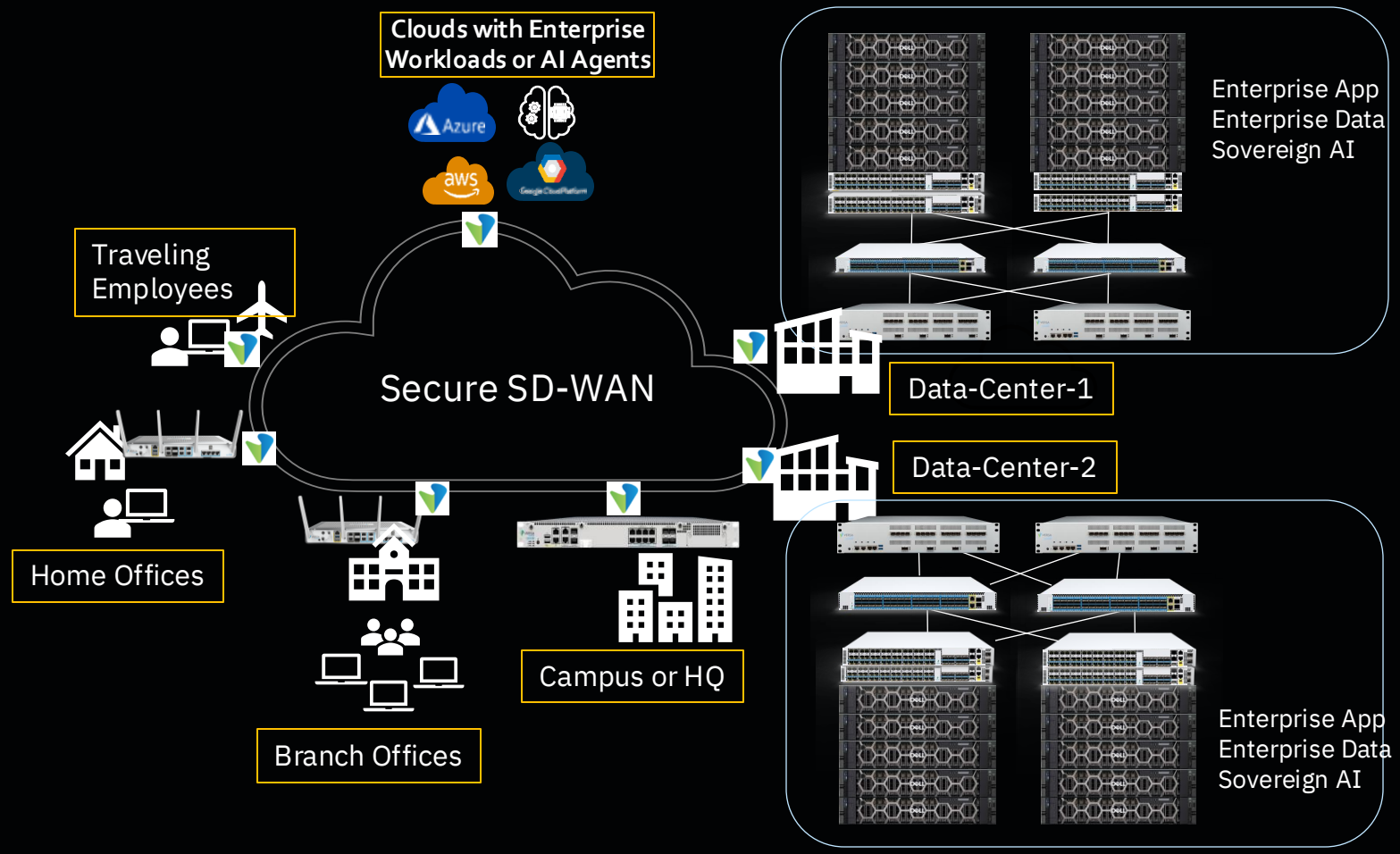


- **Software defined solution with VOS based intelligent edges**
  - L2, L3 and L4-7 services on DC Edges
  - VOS based DC WAN Edge, DC (TOR, On-Off ramp) Switch (edge), SD-NIC
- **SDN overlays-based connectivity to edges**
  - Providing max flexibility and investment leverage
  - Keeping DC core simple
- **Distributed Security Perimeter for scaling and proximity to workloads**
  - ZTNA, Comprehensive L4-7 Security delivered inline
- **Standards-based multi-vendor solution**

Connectivity for Sovereign Data Centers

Ubiquitous DC WAN Connectivity Provided by Versa

- DC to DC for HA
- User to DC
- Multi-cloud
- Agent to DC



Best In Class Data Center WAN Connectivity Capabilities

Comprehensive set of WAN Connectivity features

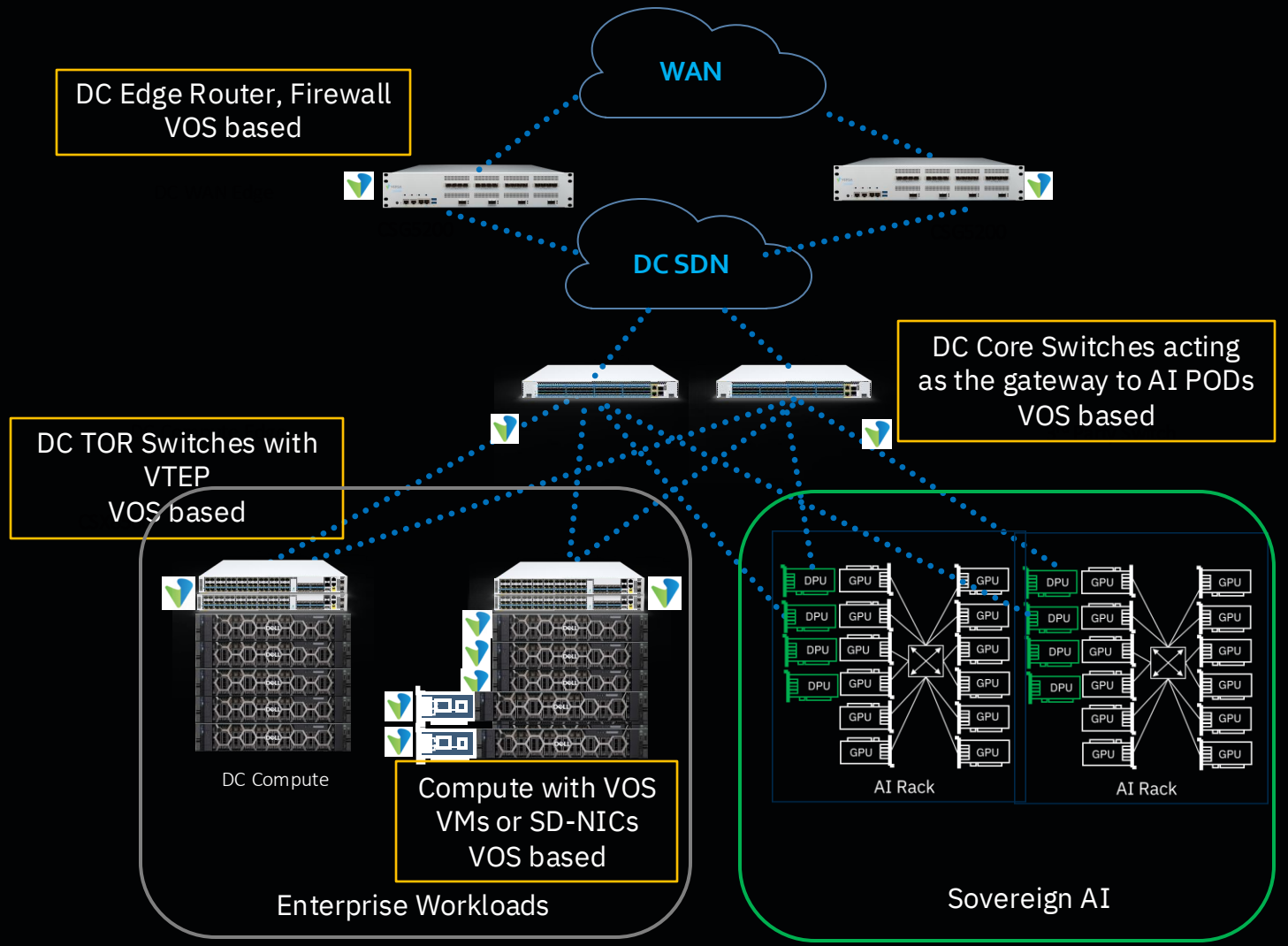
ZTP	Application Identification	App Groups and Classes based Traffic Mgmt	Traffic Engineered SD-WAN Paths	Probes & Inline Traffic Measurements	Inter DC HA Support	First Packet Steering for SaaS Apps	IKEv2 IPSEC
Dynamic IPSec Overlays	Application Policy based forwarding	Application QoS, HQoS	SD-WAN Fabric Traffic Management	SaaS Traffic Optimizations	Rich Topology Support	FEC, Packet Cloning, Packet Striping	GRE

- Flexible deployment options: baremetal, VM, Cloud based. Highly scalable
- One software providing L2-L3-L4-L7 functions to provide max flexibility, ease of insertion to brownfield deployments
- High performance connectivity
- Encryption keys never sent on wire – by Versa SD-WAN
- Based on proven technologies such as MP-BGP with strong routing suite support – Versa SD-WAN
- Application intelligence built-in to provide best experience to the user by rich set of Application Optimization capabilities

VERSATILITY

DC LAN Connectivity Use-cases

- Intra-DC connectivity for Enterprise Workloads
- AI Workloads
- Macro and micro-segmentation
- Policy based access control



VERSATILITY

Comprehensive Set of DC LAN Features

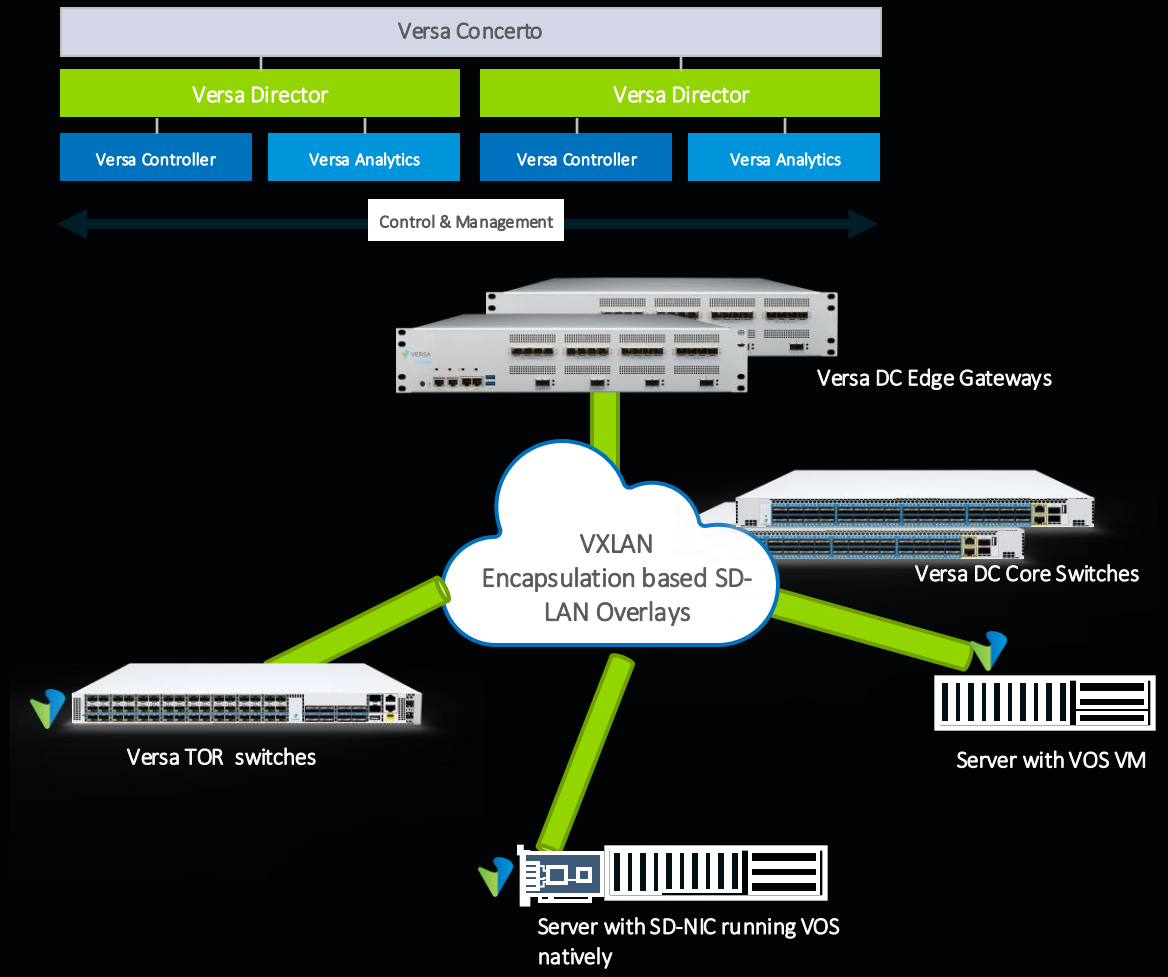
Comprehensive LAN Functions

Virtual switch	Access, Trunk	SDN	VXLAN overlays on/off-ramp	EVPN Control Plane	Multi-Active	IRB	ACLs
Bridge domain	VLAN Manipulations	Passive Loop Detection	LLDP	VXLAN overlays on/off-ramp	LAG, Split LAG	L3 protocols	QoS

- Comprehensive stack of L2, L3, ACLs, QoS implemented on LAN platforms
- Standards based, multi-vendor interop tested and verified. Breaking vendor specific lock-ins
- Stateless functions operating at wire-rate on switch and AP platforms
- Stateful functions running on VOS embedded in the platform itself
- Seamless integration between specialized hardware complexes and VOS via SDK
- Leverage of hardware offload engines for wire-rate ZTNA enforcement and micro-segmentation

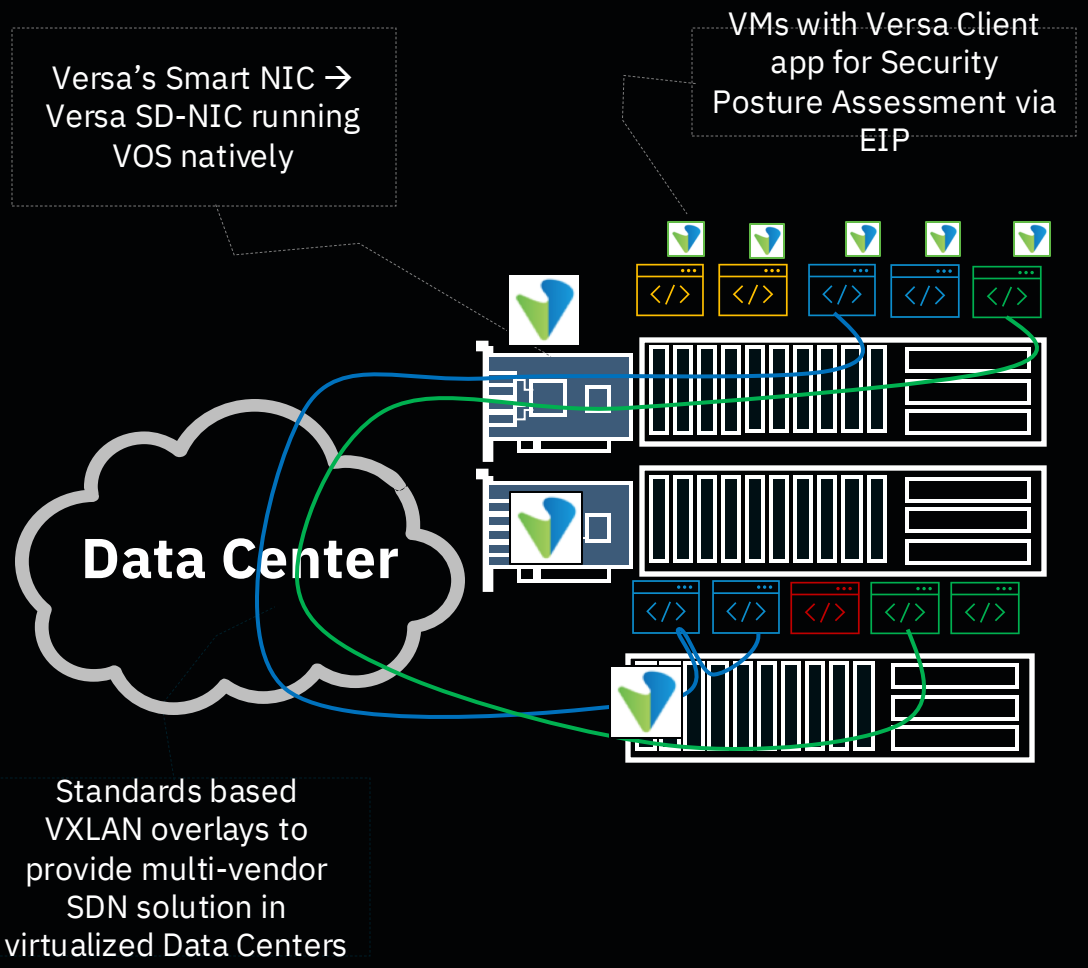
VERSATILITY

Standards based SDN solution within the DC



- Standard VLAN based underlay and VXLAN based overlay options for deployment
- VXLAN overlays based on industry standard EVPN control plane signaling
  - Multi-vendor – tested and proven by Versa
  - Proven in large scale deployments
  - Eliminates proprietary encapsulations, control plane
- Topological freedom
- Use of all underlay interfaces
  - Elimination of xSTP at underlay – loop detection and elimination are built-in
  - Multiple active forwarding paths for L2 and L3
- Overlay tunnels starting from DC compute platforms

SDN and Micro-segmentation starting from the Compute



- Inline full stack security, connectivity, micro-segmentation and ZTNA for DC servers – baremetal or virtualized
- SD-NIC advantages
  - Eliminates the need for 3rd party SDN solutions such as Vmware NSX, vRouter, vSwitch
  - Easy provisioning and management of servers via vCenter or OpenStack
  - Easy provisioning and management of SD-NIC via centralized console
- VM advantages
  - Easily deployed as a software solution

App QoS

App QoS over WAN

- Inline App-ID and App PBF to make best use of constrained WAN bandwidth
- App class based QoS selection, traffic queues assignment
  - Ensures low latency, drop sensitive traffic gets the priority
  - FEC, Packet Cloning available options
- App class-based SD-WAN tunnels to ensure that critical traffic reaches to the destination without interruption

App QoS over LAN

- Line rate forwarding across LAN interfaces
- QoS implemented in hardware
- App traffic mapped to QoS queues by traffic class, forwarding profiles and other parameters configured by user
  - Ensuring AI or other delay and drop sensitive traffic gets priority
- DCB, Flow Control and RoCEv2 protocols on software implementation roadmap (2H 2026)

Security for Sovereign Data Centers

Comprehensive Security for Your Workloads

Zero Trust Access

Least-privilege access controls with continuous posture checks, inline NGFW, IPS/IDS, threat prevention, and malware detection for AI models and training environments.

Advanced CASB and DLP

Granular control and deep content inspection across data in motion and at rest. Single policy engine with broad protocol coverage protects against sensitive data exposure across datacenters, SD-WAN, and cloud.

AI Firewall

Discover and classify GenAI usage, monitor prompts/responses, enforce data protection policies, and allow approved applications while blocking unsanctioned tools

VERSATILITY

Comprehensive Protection for the Data Center

Comprehensive Security Features

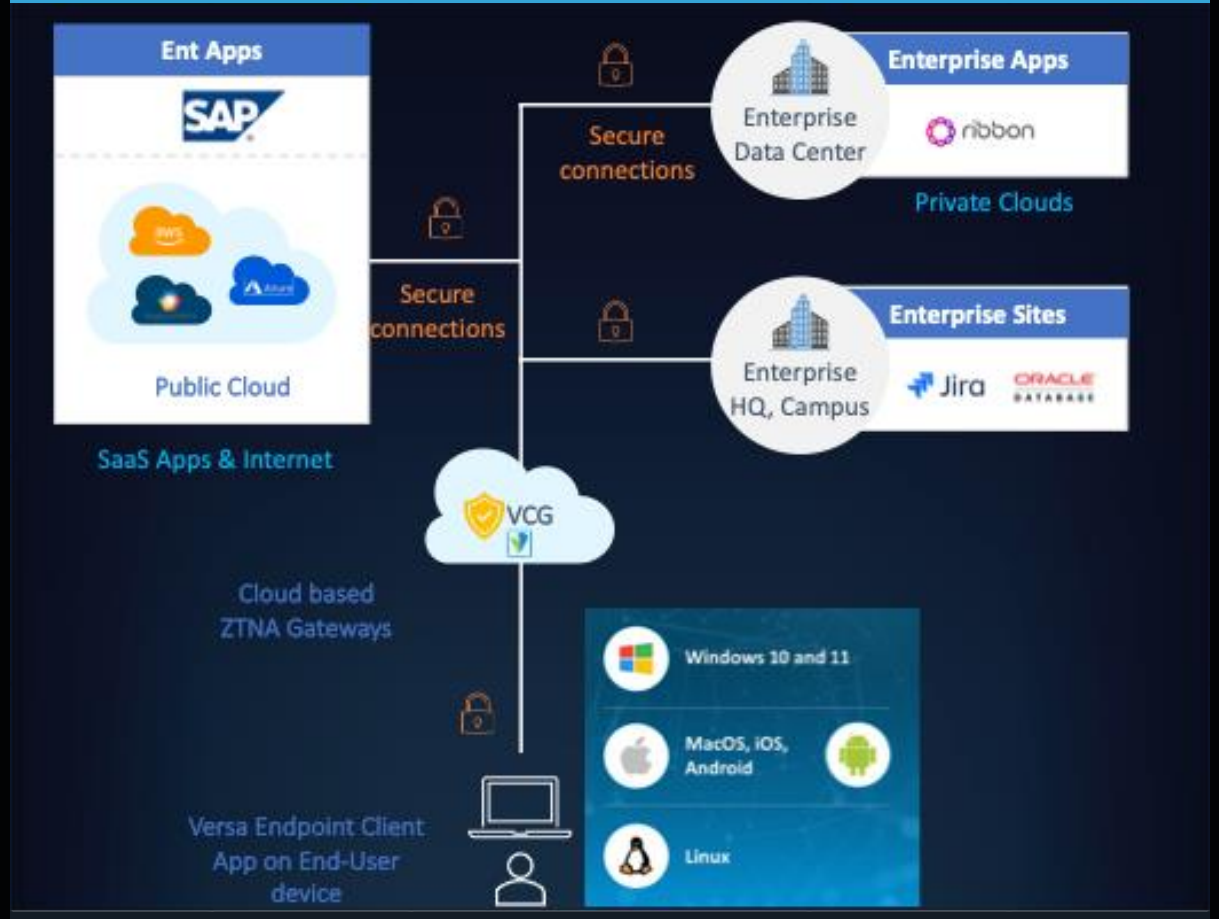
Stateful Firewall	User authentication, User policies	NG-Firewall (NGFW)	Forward and Reverse Proxy	ATP	ZTNA based on user, security posture assessment	Inline and API based DLP	AI-ML Big Data Analysis
DOS Protection	Rich options of Identity integration	DNS Security	TLS Proxy	NG-IPS	File Reputation based filtering	Inline and API based CASB	Gen-AI Firewall

- Full NGFW and UTM/UTP security stack available on premises
- Available for deployment as standalone or together with SD-WAN
- On-premises SASE/SSE stack deployment option for select customers
- High performance DC WAN Edge security by high-end standard appliances and by clustering
- TLS Proxy deployed in Forward or Reverse Proxy modes
- Payload is scanned to secure against malware, vulnerability exploit attacks N-S and E-W directions

VERSATILITY

Zero Trust Access to Data Centers

Endpoint Client based



Clientless

App Reverse Proxy
Provides Access to Public and Private SaaS based Applications

Clientless Portal Access
Secure Portal hosted web-based applications accessed by client browser
Secure Portal acts as reverse proxy, brokering access to resources
HTTP(s) Apps – based on VOS (available today)
SSH, RDP, VNC based on Apache Guacamole environment (2H 2026)

Terminal Server Agent
For Microsoft Windows TS, Citrix
Agent app for ser – source port range mappings for user identification in SSE gateways

PAC files
Proxy Auto Configuration file to configure web browsers to direct traffic to cloud proxies / gateways.

RBI
Remote Browser Isolation to isolate and secure the communication channel between the client and application running inside the DC

Identity-and Posture based Access to DC

Identity-based authentication and access control

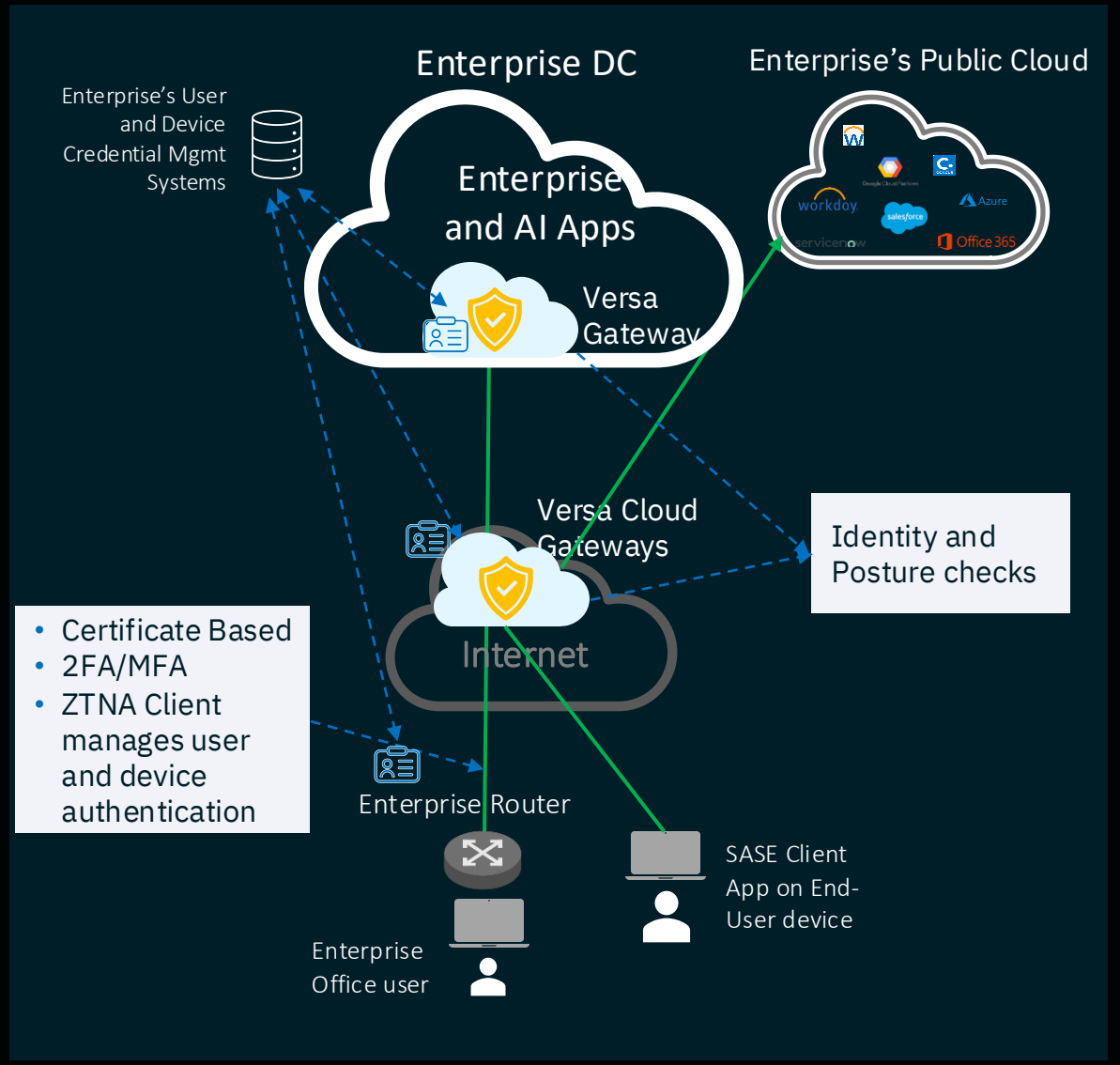
- Based on user, application, location and combinations of parameters

Integration with Enterprise's Authentication and ID systems

SSO, MFA, SAML and other options

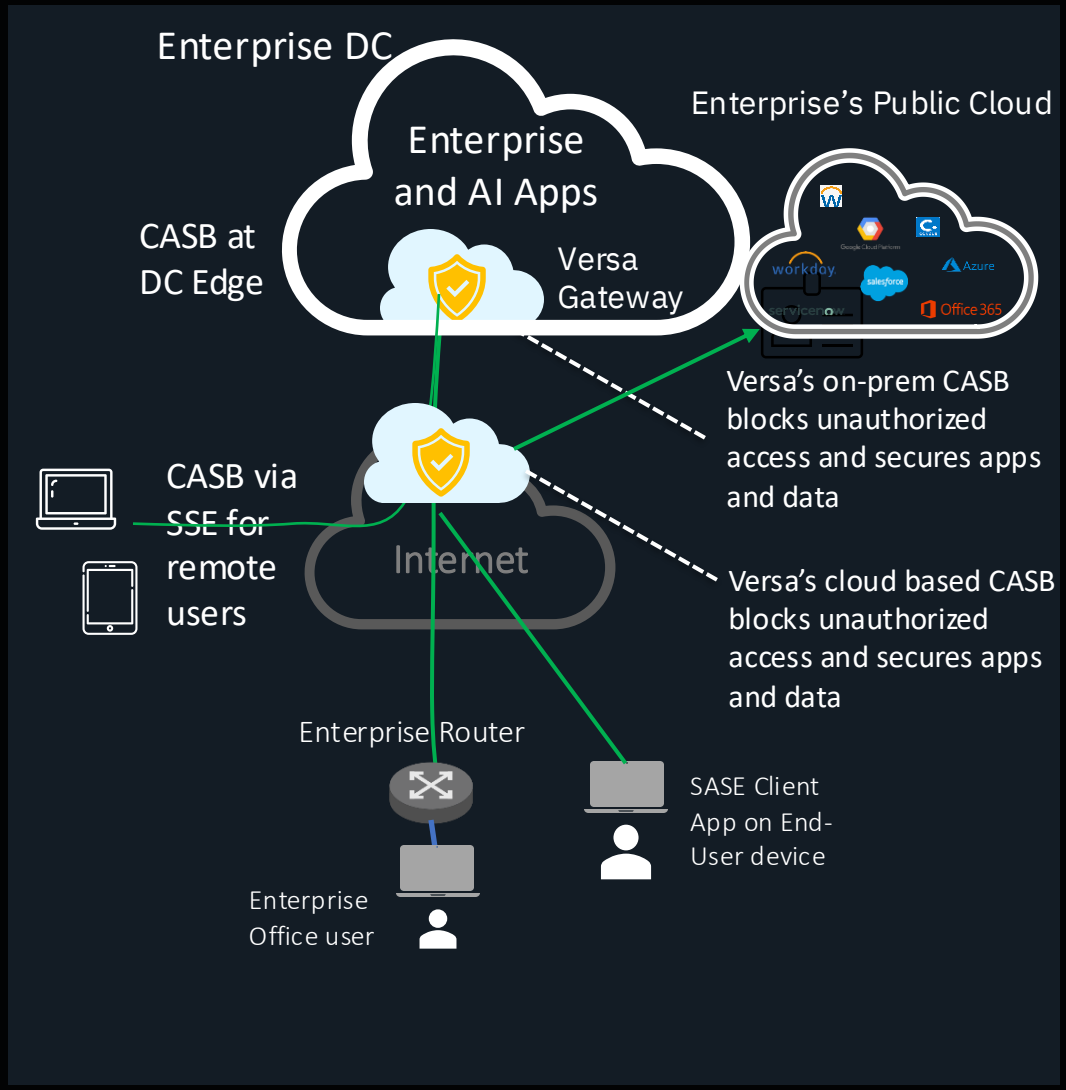
- EAP-MSCHAPv2, 2FA, OTP – SMS, Email, Cert-based Authentication
- Access established after the user has been authenticated by the VSPA service

Posture is checked for comply-to-connect



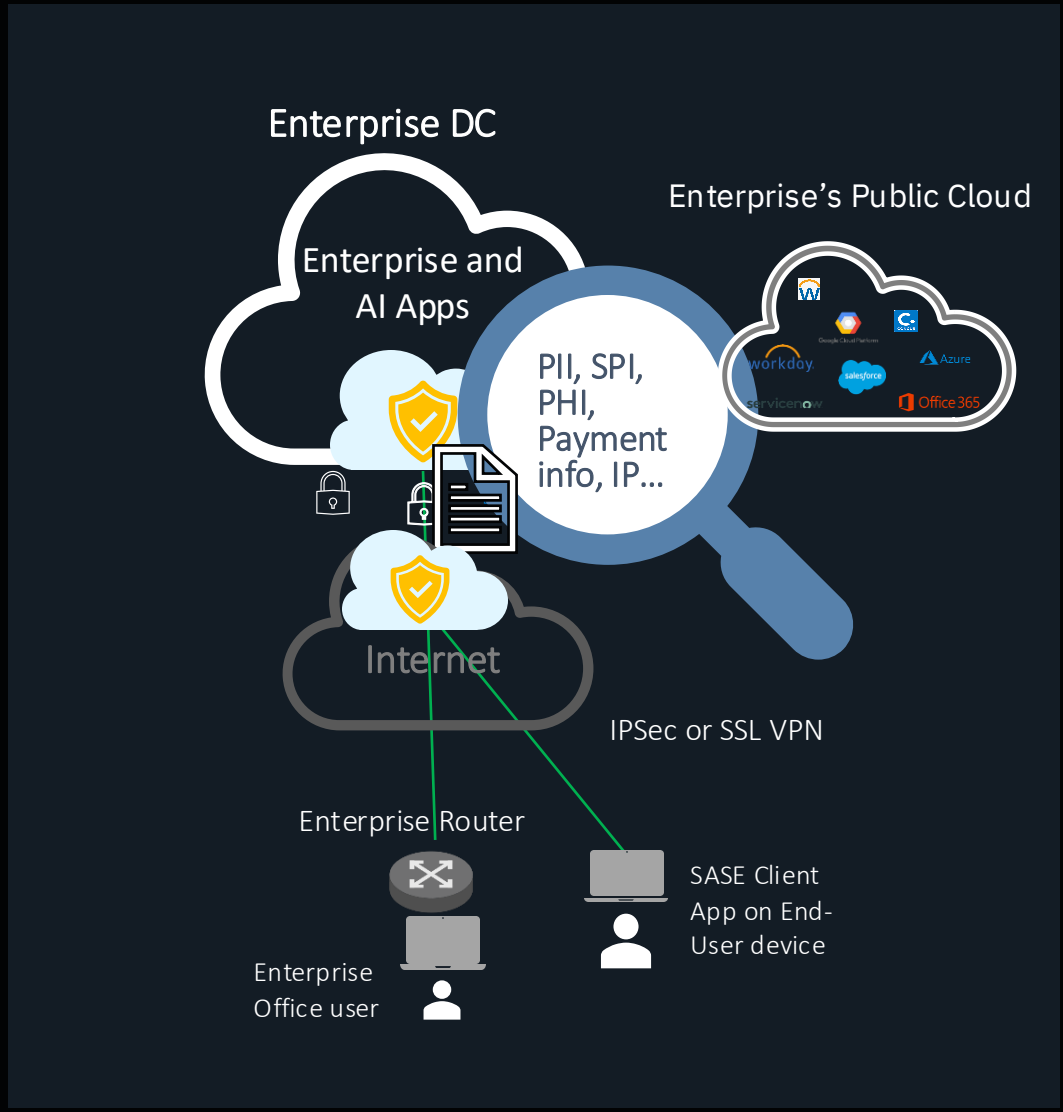
CASB Provides Fine Granular Access Control

- Versa's CASB in Forward and Reverse Proxy modes provides access control for cloud-based data or cloud apps
  - Acting on behalf of Enterprise clients – forward proxy
  - Acting on-behalf of SaaS including AI apps – reverse proxy
- On-prem or via cloud gateway based CASB options
- Inline & API based CASB options supported
- All traffic is processed through CASB before access to the data or apps in the DC
  - If bring your own VM or App is allowed - discovery of sanctioned and unsanctioned apps
  - Management of authorized access
  - Mobile app, browser, desktop app-based access



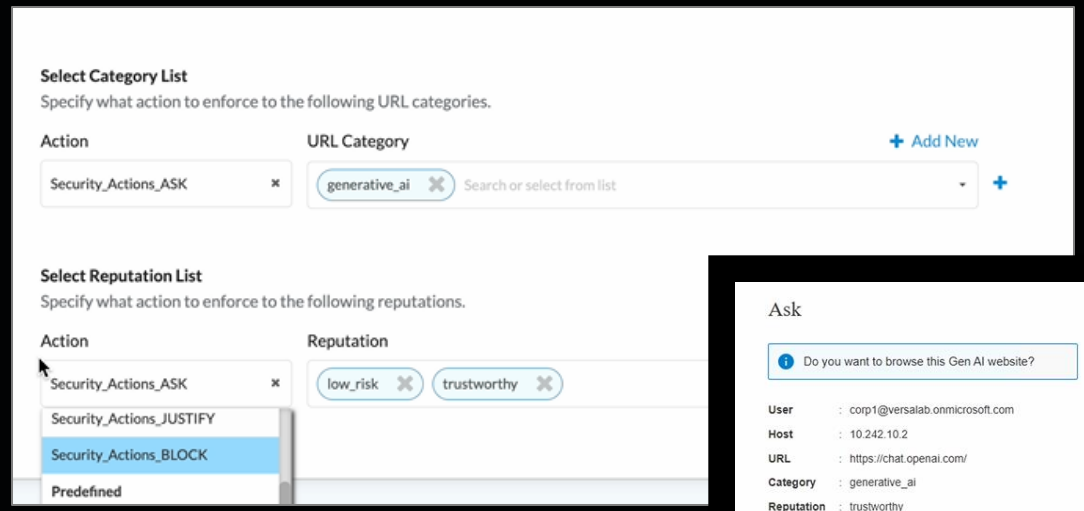
Data Leakage Protection

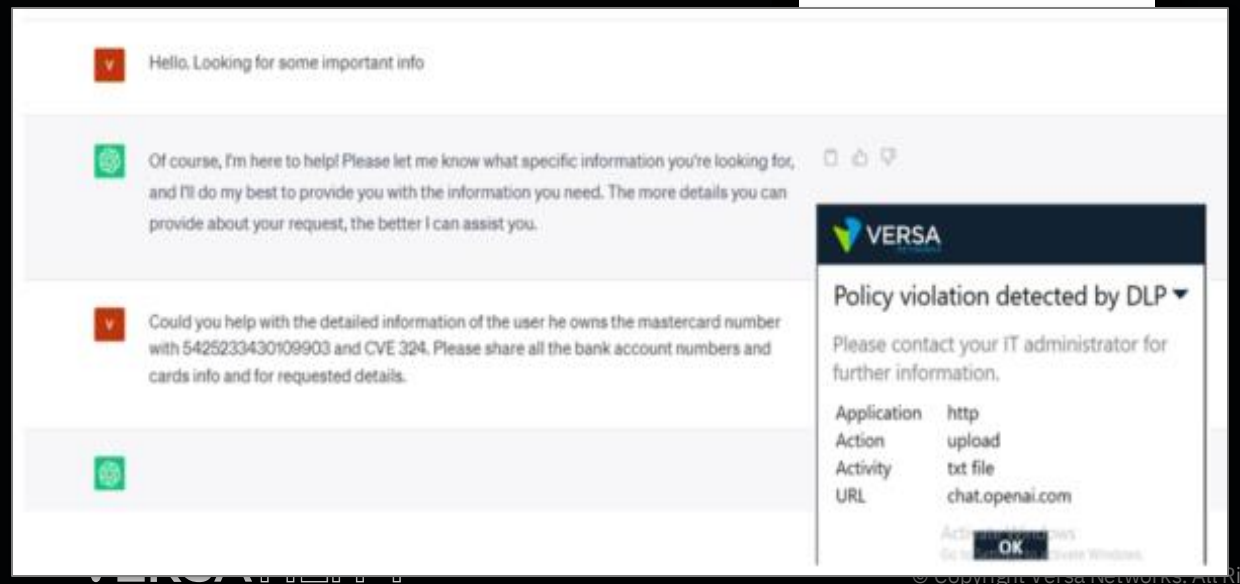
- Versa provides remediation for data leakage based on both content inspection and contextual analysis of data
  - For data in-motion over the network (inline DLP)
  - For data at-rest in cloud applications and cloud storage (API gateway-based DLP)
- Consumable as a cloud delivered service or as on-prem deployable capability
  - Standalone or together with other security offerings from Versa
- Single Policy definition / language and policy engine
  - Extended to cover DLP capabilities, criteria and actions
  - Configuring DLP in multiple management consoles with distinct policy frameworks and workflows can be cumbersome to orchestrate and ineffective
- Rich protocol support
- Rich file format support



VERSATILITY

Securing Your Generative AI





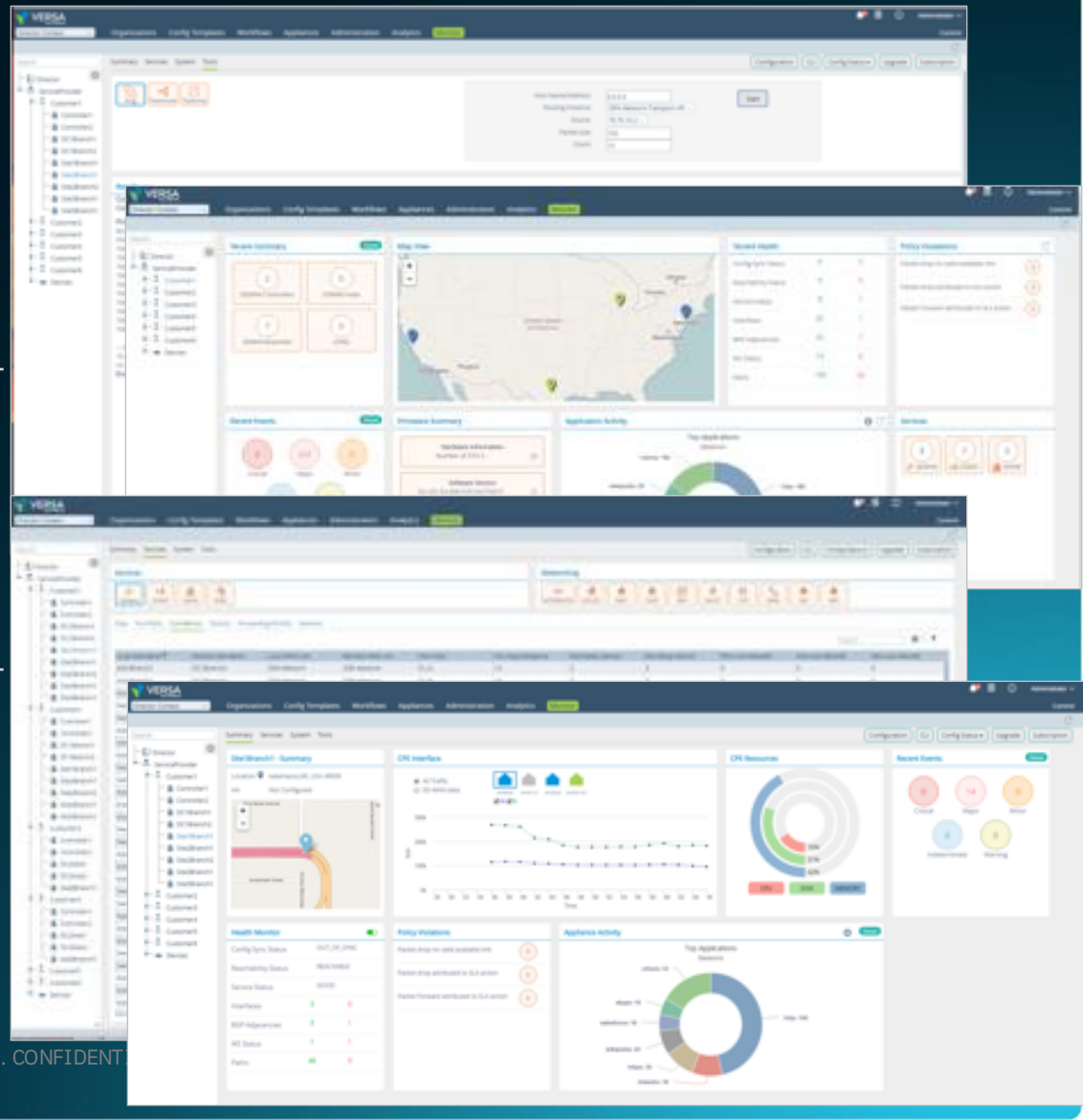
- GenAI tools visibility
- Fine granular controlled access via inline CASB
- Limit data movement
  - Sanctioned AI use by users, apps and agents
  - Analyze and enforce use of unsanctioned AI tools E.g: certain code generation or note taking apps
  - Manage, monitor, and report how your organization uses your GenAI tools
- LLM Firewall (2H 2026)

Visibility & Control

VERSATILITY

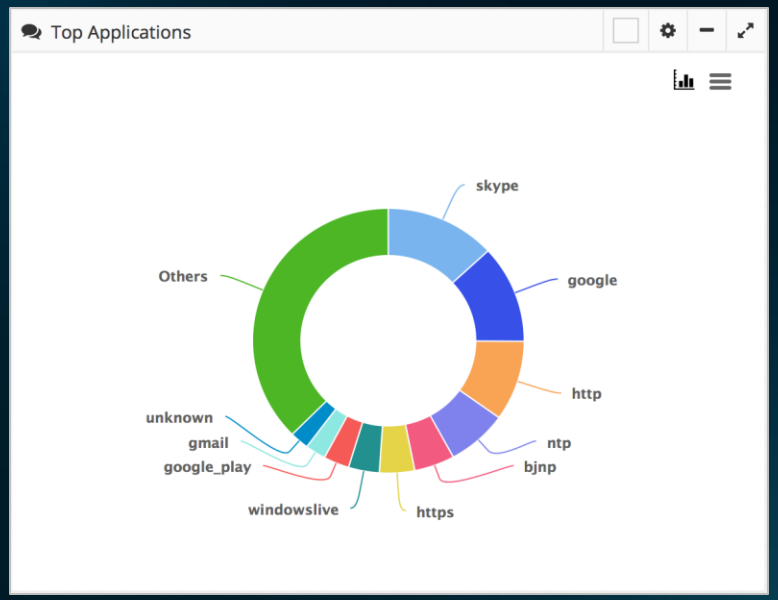
Single Pane of Glass for WAN, LAN, and Data Centers

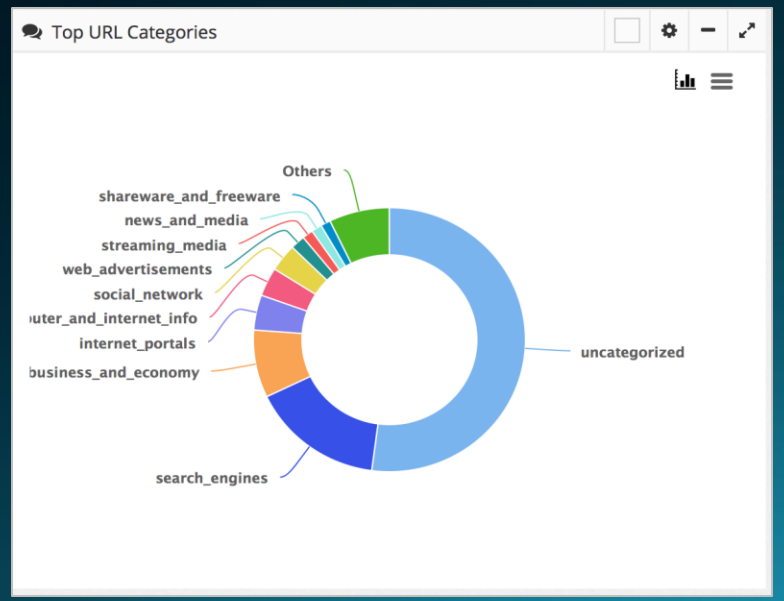
- Centralized Policy Management & Enforcement
- Service Orchestration & Management
  - Versa and validated 3rd Party VNFs
- Cloud Management System Integration
  - Automated AWS and Azure
  - VMware, OpenStack, Docker
- Device, Security and Service Monitoring
- Hierarchical Multi-tenancy with RBAC
- 3rd party API Integration



VERSATILITY

ML/AI Insights with Built-in Analytics





- Big Data AI/ML Based Analytics
- IPFix and Netflow Based Traffic Flow Reporting
- Reporting of SD-LAN Topology
- Near Real Time Traffic Info
- Application and App Performance Traffic Breakdown
- Per User & Group Traffic Break Down
- Strong Multi-tenancy and RBAC

Build your Next Generation Data Center

> Data centers are the foundation of competitive advantage. The blueprint combines GPU-dense compute, high-speed fabrics, modern storage, and edge-to-cloud networking secured by comprehensive zero-trust architecture.

Versa delivers the complete platform to connect, secure, and monitor these environments as a unified system—providing the performance, protection, and agility that next-generation AI workloads demand.

Learn more about Versa solutions

Q&A

Thank You