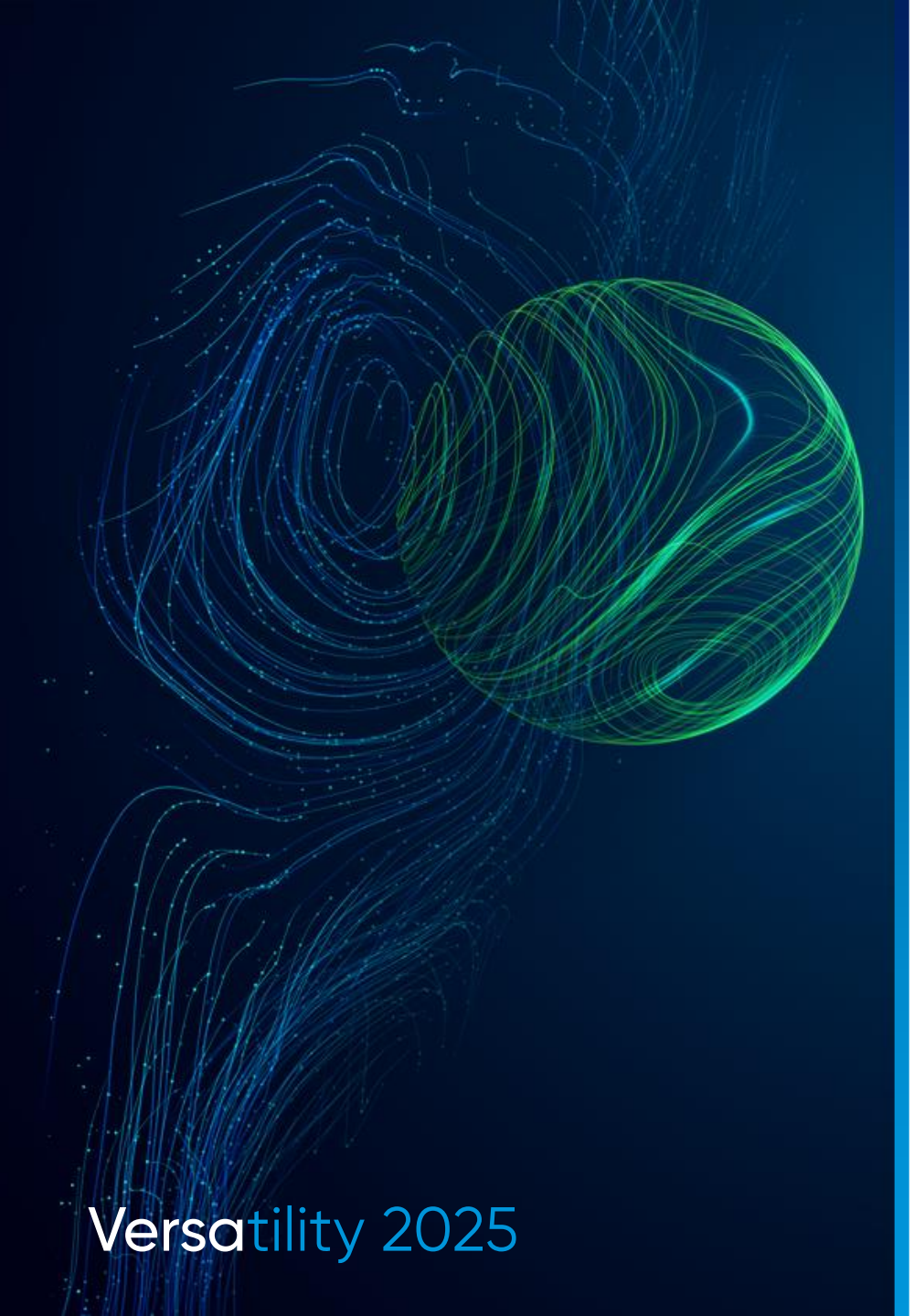
Next Generation Firewall:
Micro-Segmentation, Zero Trust, and IoT Security

VERSA



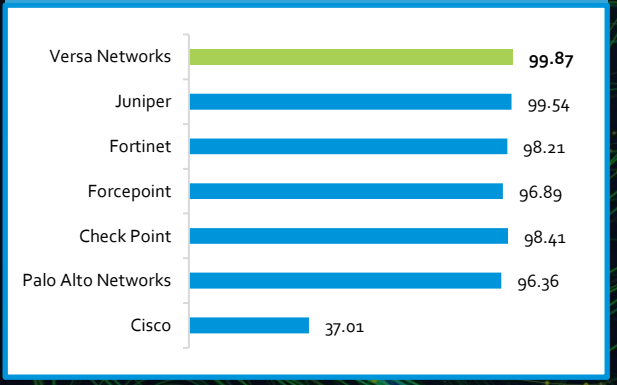
Versatility 2025

If we could give you the same level of protection at a better cost of ownership, would you consider an alternative firewall?

VERSA

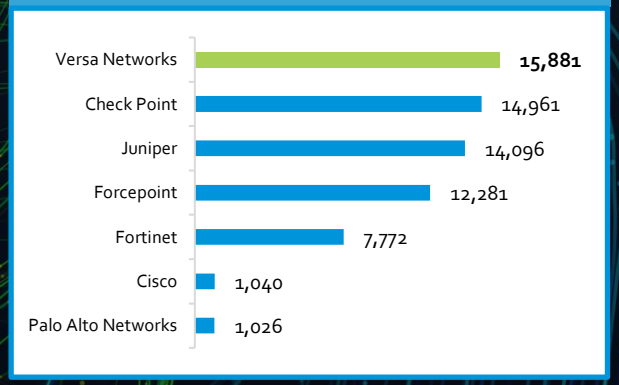
Enterprise Firewall Comparative Security Value Map ™ Q2, 2024

Industry-leading Security Effectiveness 99.87%



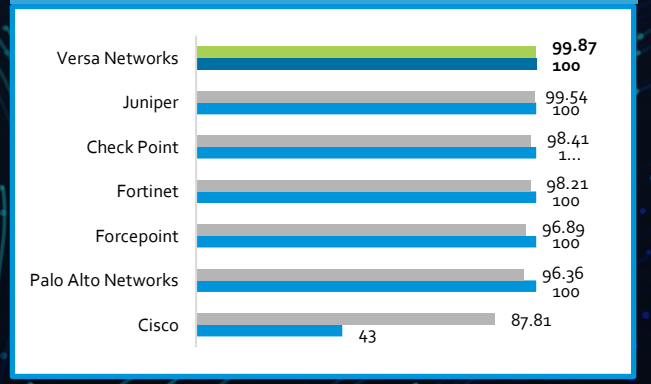
How effective was the enterprise firewall in controlling network access, applications, and users while preventing exploits and evasions.

HTTPS Throughput (Mbps)



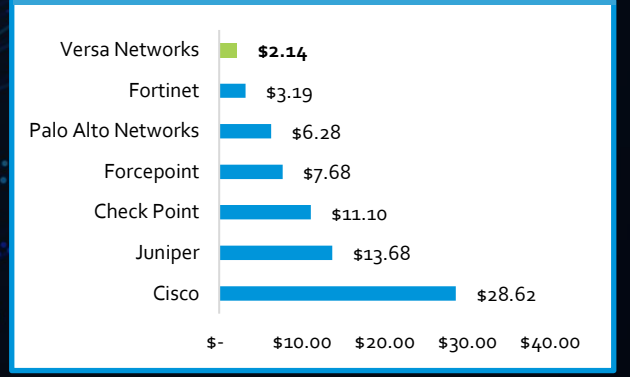
Throughput performance with different packet sizes payloads to capture firewall's performance for HTTPS

Threat Prevention (Exploits/Evasions)



Threat Prevention against exploits and evasions using CyberRatings exploit repository.

Lowest Price per Protected Mbps

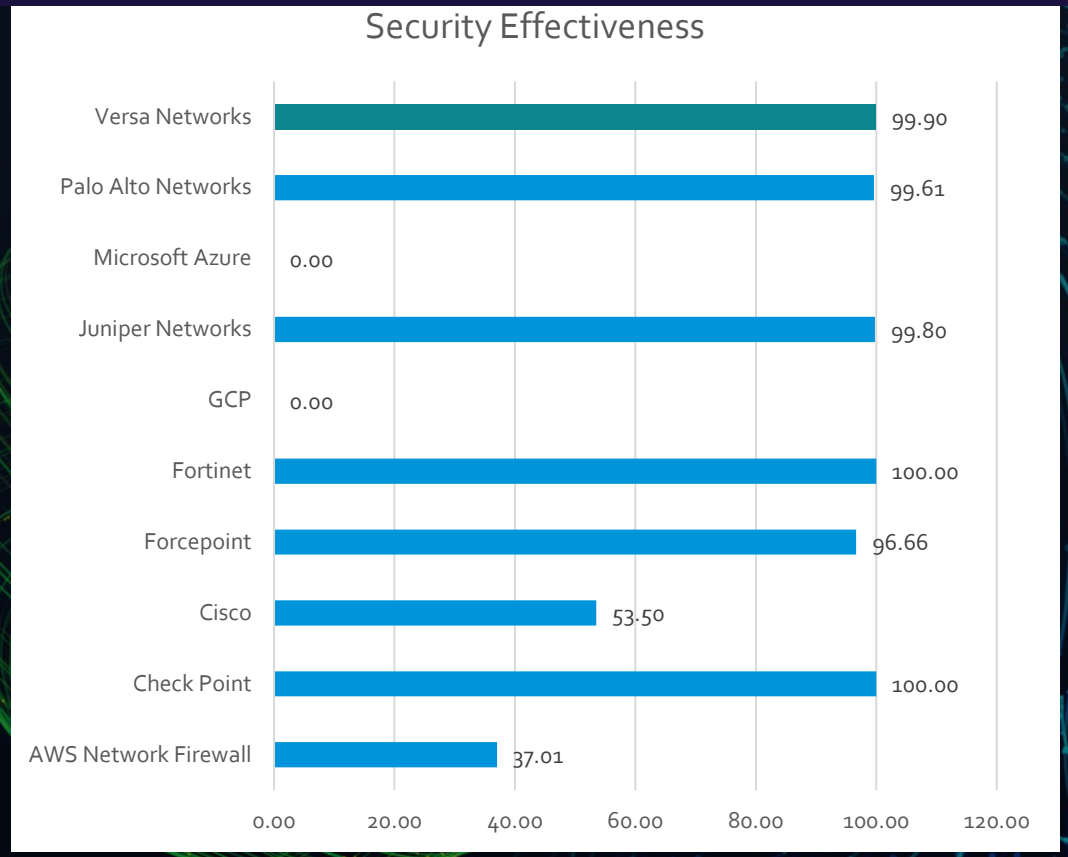


Calculated by considering price, performance, manageability, and security; the Price per Mbps and divide it by security effectiveness

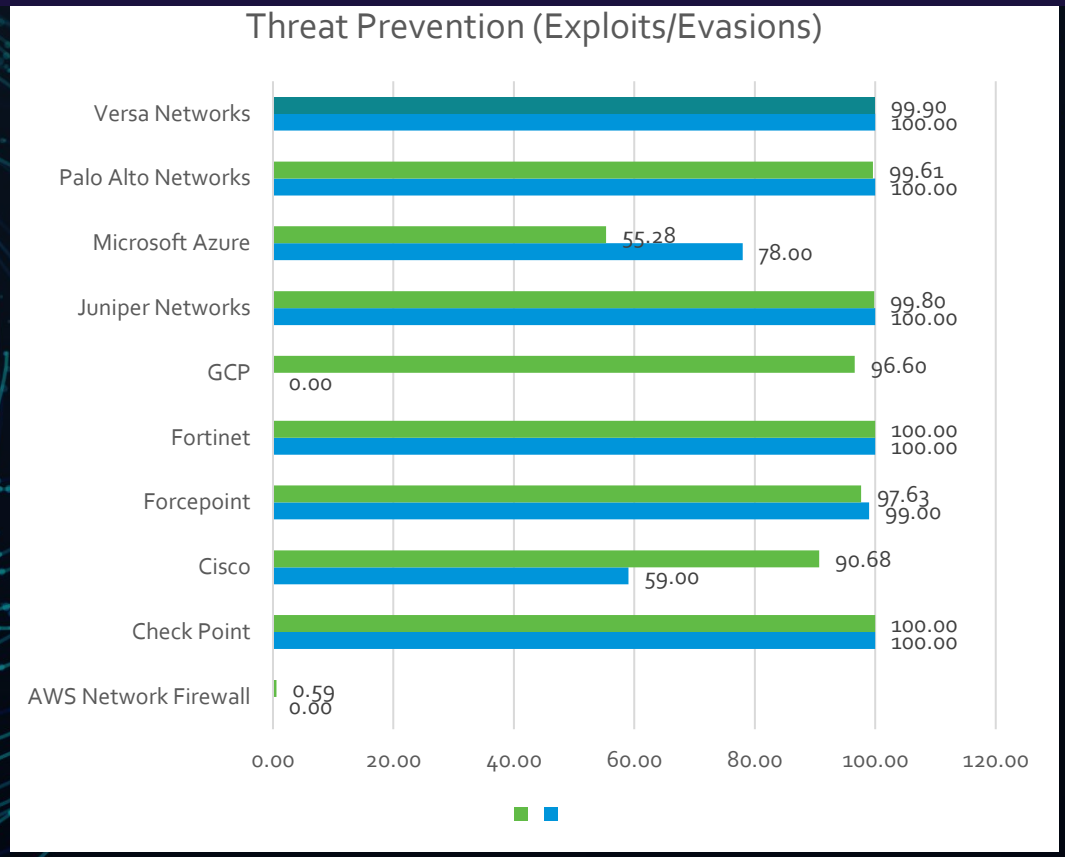
Versatility 2025

VERSA

Cloud Firewall Comparative Security Value Map ™ Q1, 2025



How effective was the enterprise firewall in controlling network access, applications, and users while preventing exploits and evasions.

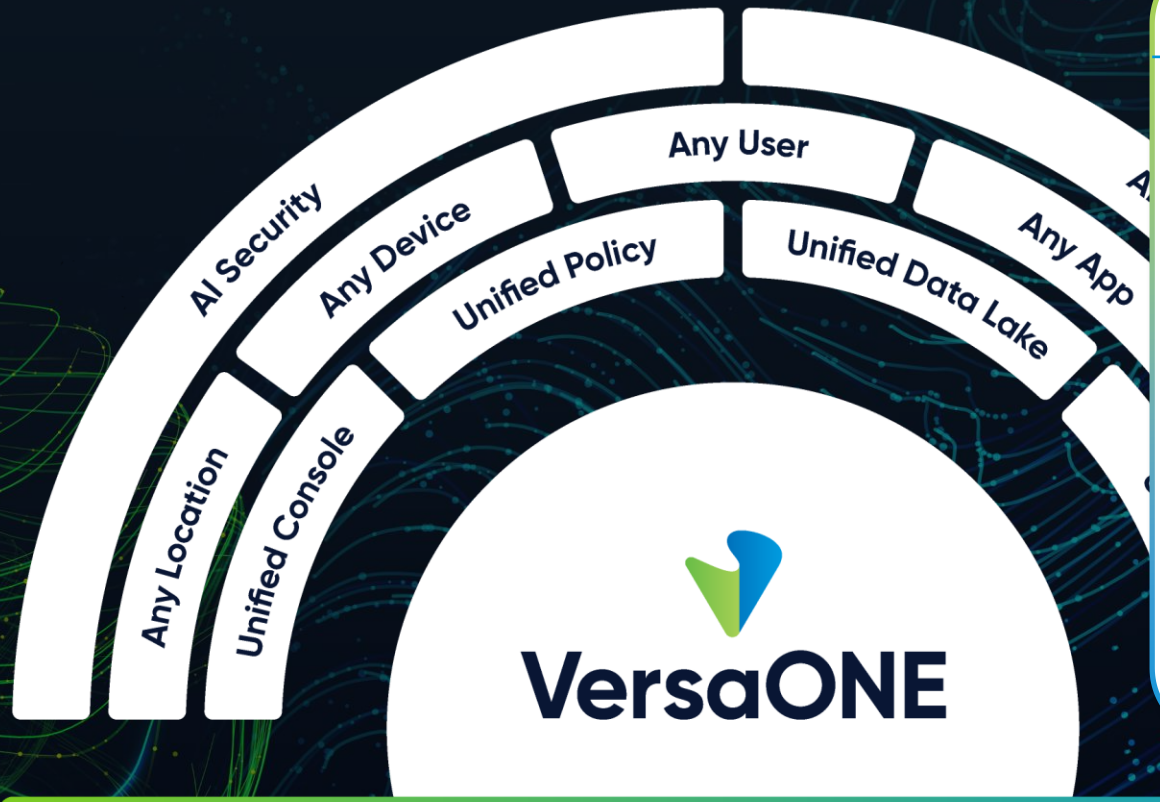


Threat Prevention against exploits and evasions using CyberRatings exploit repository.

Versatility 2025

VERSA

VersaONE Universal SASE Platform



Next Generation Firewall

- Layer 7 Aware & Control
- ZTNA for Micro-Segmentation
- IoT Security/OT Security
- IPS/IDS
- GenAI Firewall
- AI for Security
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)*
- Advanced Threat Protection (ATP)*

INTEGRATIONS

- Identity Providers
- EPP / EDR
- MDM
- Threat Intelligence

Artificial Intelligence

Zero Trust

Scalable multi-plane architecture

High availability | API | Agent / Agentless | Observability | Multi-tenancy

Real-time message bus | Traffic Engineered Fabric | Automation | Appliances (L2/L3/L4-L7)

INTEGRATIONS

- SSE / SD-WAN
- Multi-Cloud
- Security Analytics
- Network Monitoring/Mgmt
- Automation
- Service Desk

Versa Next Gen Firewall

Different deployment options

Enterprise NGFW

On-premise deployment for hands-on control over network security. (On-prem)

Cloud NGFW

Native integration and deployment on cloud environments. (e.g. AWS)

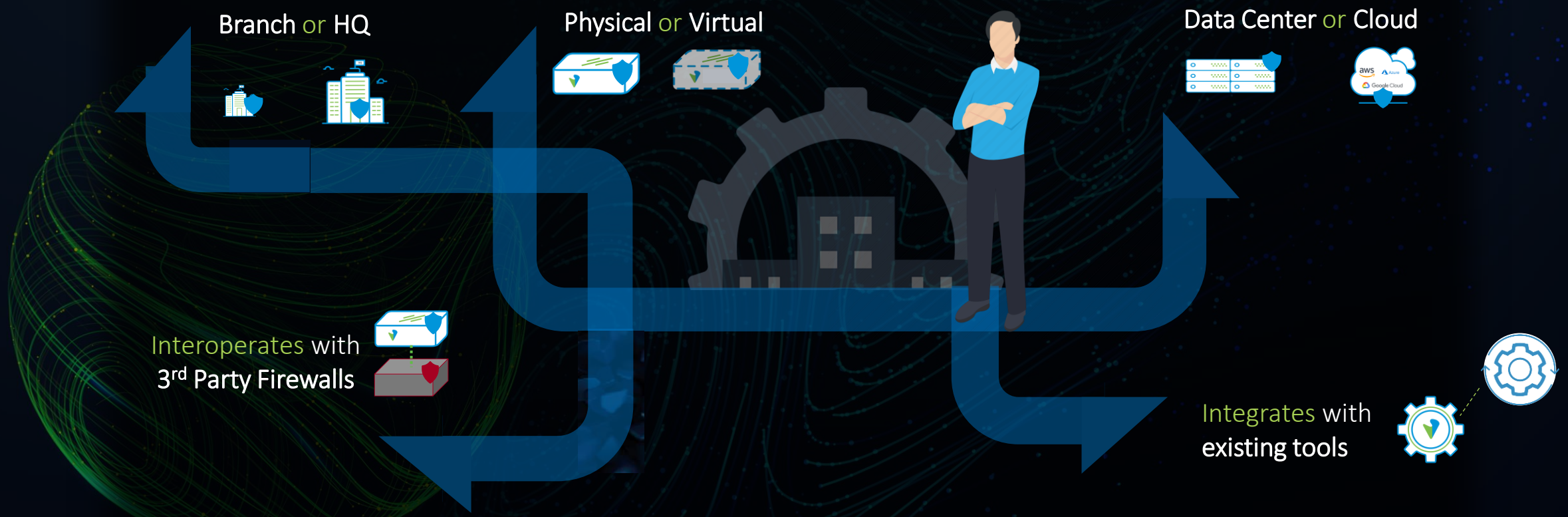
Firewall as a Service

Cloud-delivered "as a service" to secure across locations & devices. (SSE)

VERSA

Seamlessly Fits into any Environment

- Flexibility to meet your enterprise needs



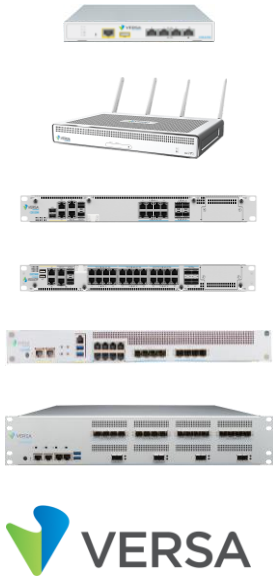
Versatility 2025

VERSA

Versa's Hardware & Hypervisor Agnostic Approach

Reducing complexity and costs with flexible options to meet your needs

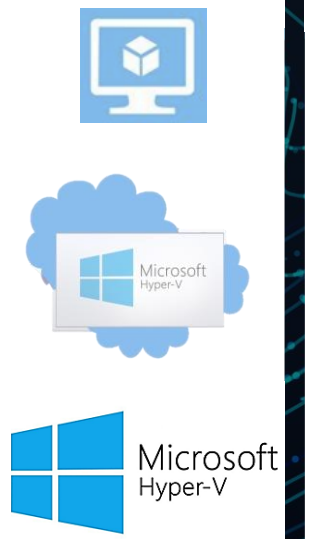
Versa CSG
Appliances



Dell VEP
Appliances

Hypervisor
VMs

Microsoft
Hyper-V



IaaS
Platforms

Designed to run directly on bare metal Versa CSG appliances

Also runs on certified & preconfigured:

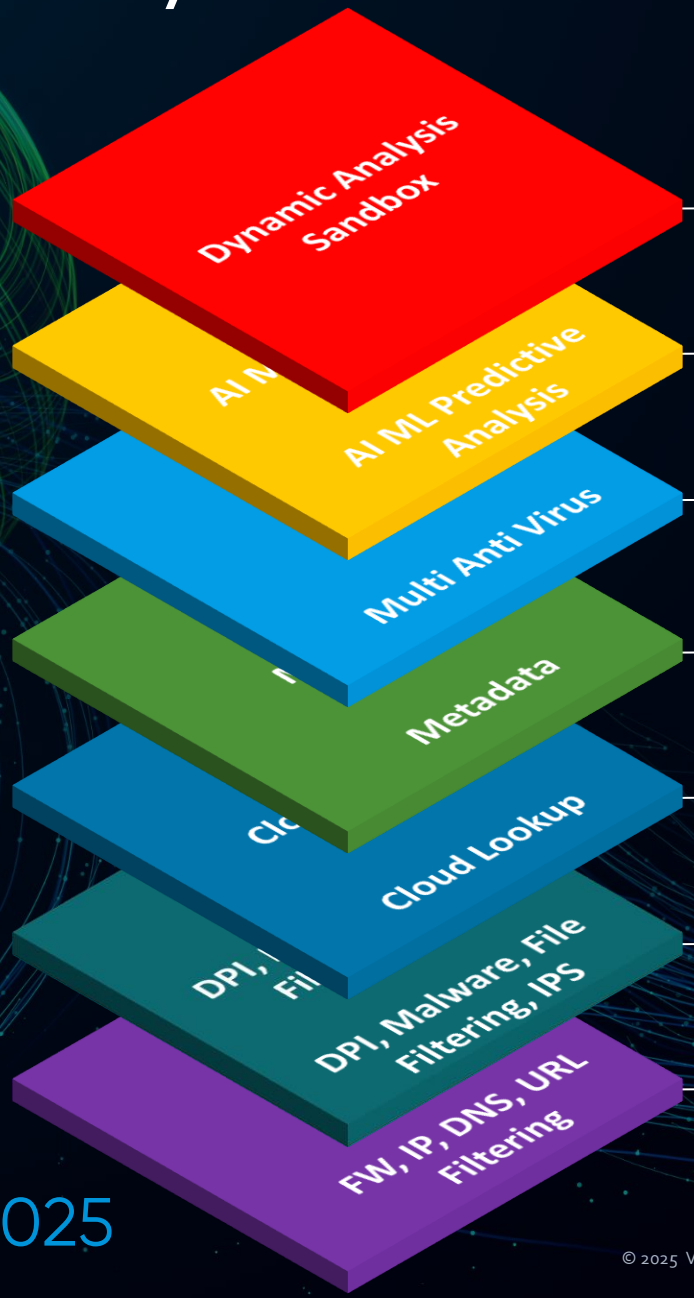
- Dell VEPs
- Hypervisor VMs (VMware ESXi, KVM Xen)
- Microsoft Hyper-V
- IaaS platforms (Amazon, Google and Microsoft)

VERSA

Foundational Functions of Versa NGFW

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 Security	On-prem ZTNA	Cloud Access Security Broker
Data Loss Prevention (DLP)	Advanced Threat Protection (ATP)	Remote Access ZTNA

Versa ATP Layered Threat Defense



Advanced Threat Protection (ATP)

Secure Web Gateway, FWaaS, Zero Trust Network Access, Intrusion Prevention System

- Detonates file in sandbox
- Uses non-signature-based AI ML models
- **Static Analysis:** Uses Multiple engines to check for AV signatures
- **Static Analysis:** File metadata attribute checks
- **Static Analysis:** Checks for known bad file hashes
- **Content filtering:** Scans web, email traffic & files, application risk classification, matches signatures
- **Web/FW filtering:** No decryption IOC match

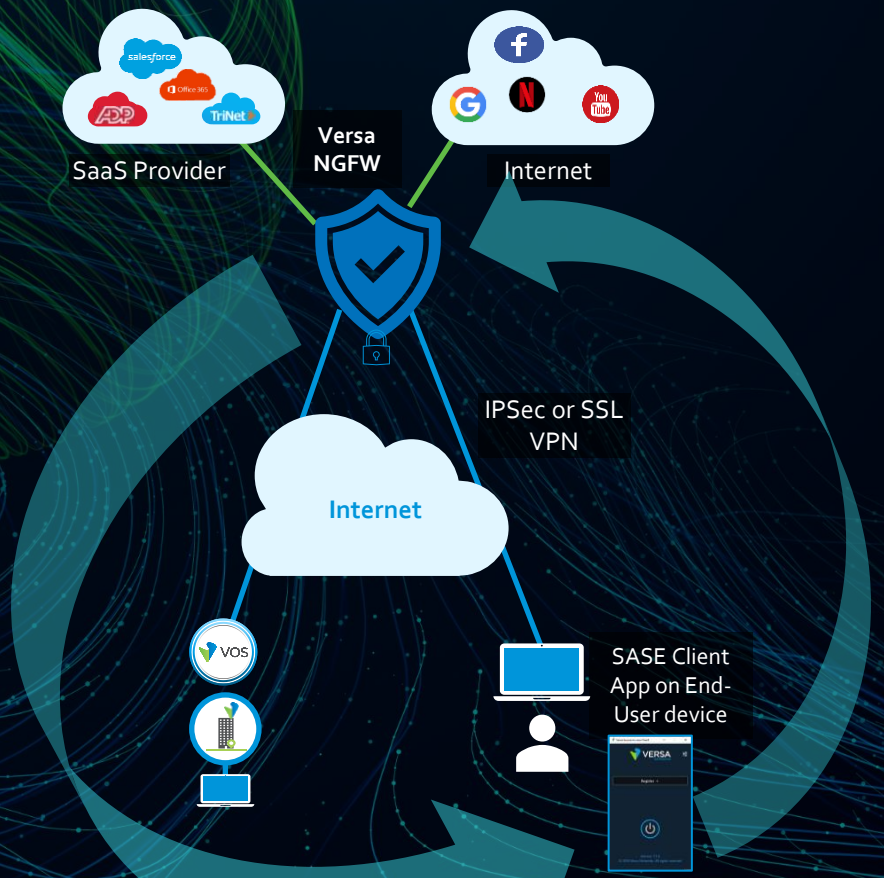
Requires TLS Decryption

Versatility 2025

VERSA

Zero Trust Network Access

With continuous risk assessment and adaptive access control



4 Continuous posture checks configurable as low as every 5 seconds

3 Gateway enforces security policies based on EIP posture received

2 SASE client app publishes the End-client machine's profile and user-profile to portal & gateway

1 User authenticates to portal and receives EIP-agent configuration from portal

Supported software categories

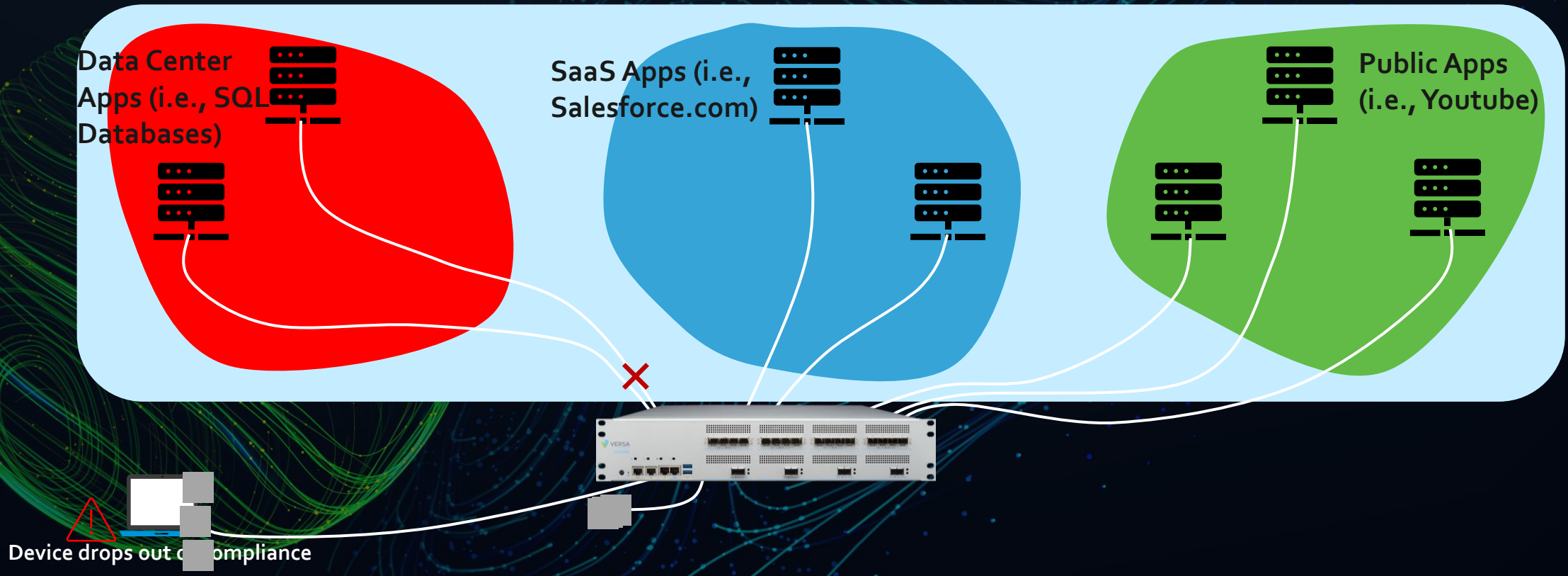
- ✓ *Antimalware*
- ✓ *Antiphishing*
- ✓ *Firewall*
- ✓ *Browser*
- ✓ *Messenger*
- ✓ *DLP*
- ✓ *Patch-management*
- ✓ *Disk encryption*
- ✓ *Cloud storage*
- ✓ *Disk backup*
- ✓ *Virtual machine*
- ✓ *Health Agent*
- ✓ *Public File Sharing*
- ✓ *Remote Control*
- ✓ *Custom (Files, Windows Registries)*
- ✓ *General (OS, user-name, domain)*
- ✓ *Management status*

Versatility 2025

VERSA

Software Defined Microsegmentation

Using continuous risk assessment and applying adaptive access control

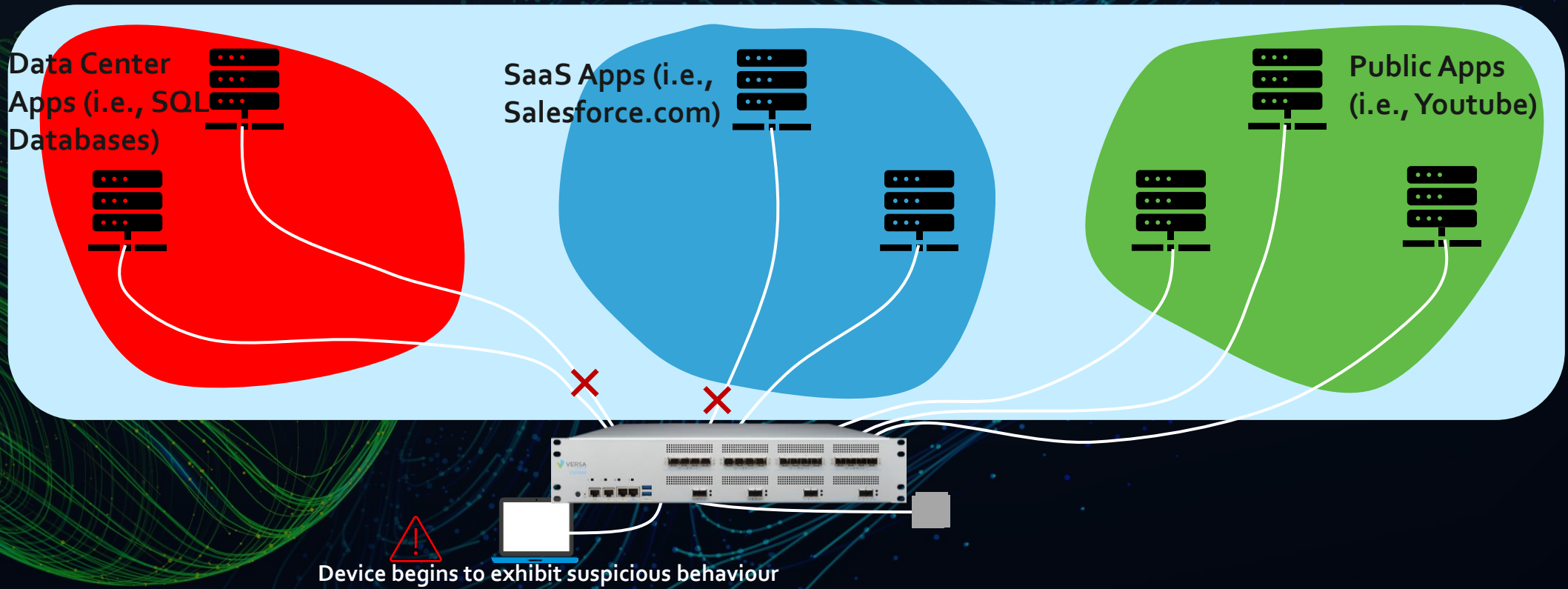


Versatility 2025

VERSA

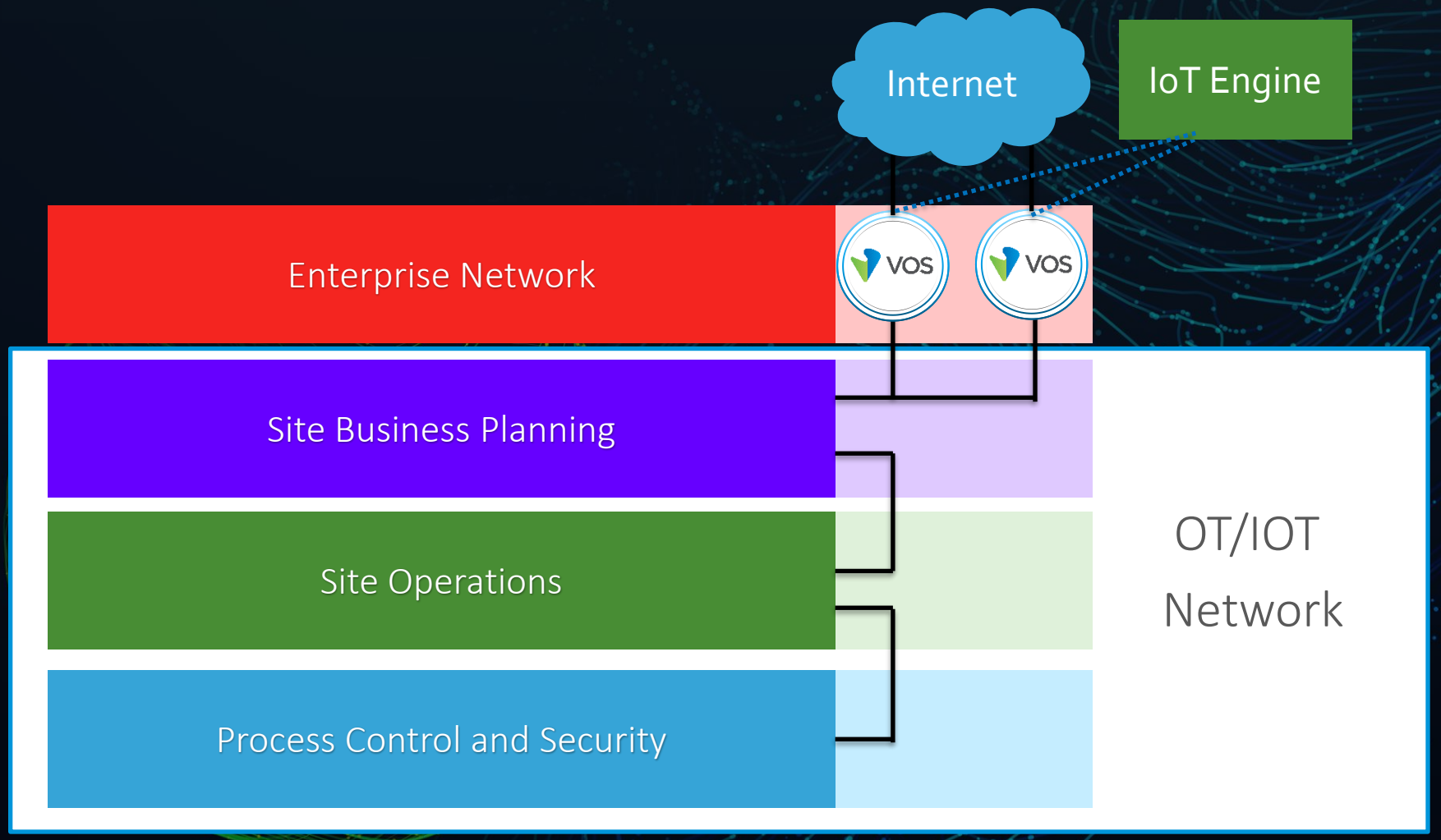
Software Defined Microsegmentation

Using continuous risk assessment and applying adaptive access control



VERSA

IoT Device Fingerprinting

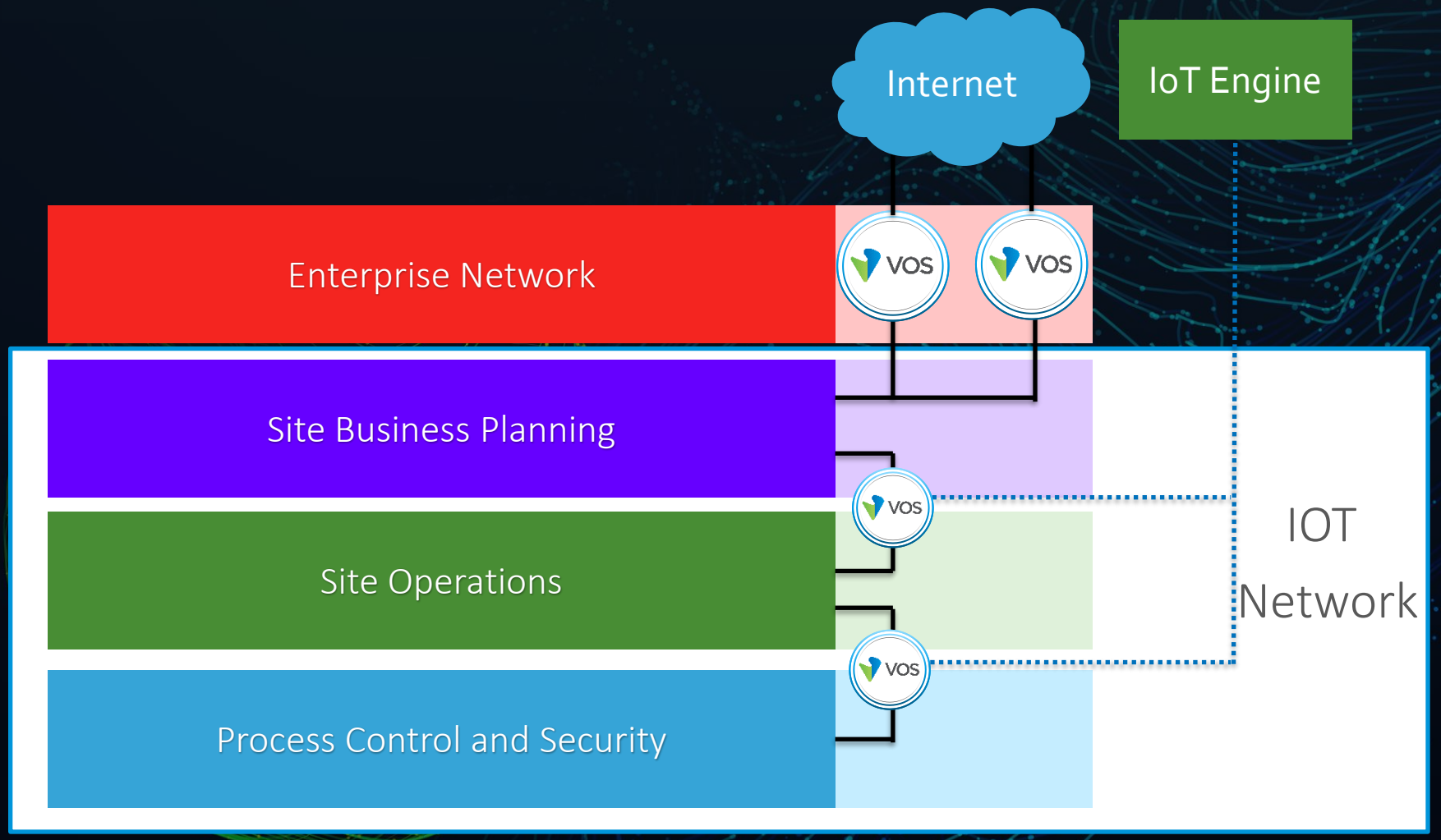


- Device fingerprinting enabled on Secure SDWAN or NGFW device
- Detection of IOT/OT devices traversing VOS
- VOS queries Cloud Engine to detect IOT devices

- Uses 20+ parameters to detect the device type, manufacturer, firmware version.
- Estimates device risk

VERSA

IoT Device Fingerprinting



NGFW deployed deep inside the IOT/OT network to detect devices and to secure the network

VERSA

Market Leading Identification Capabilities

Device Fingerprinting (Dev-ID)

- Inline Analysis of traffic flows for IoT/OT (and Corporate, BYOD/personal) devices
- Device Fingerprint DB – Leyer 2 to Layer 7
- Low Latency Rule-based Engine
- Match based on device class for consumption of policies, analytics, and others

Deep Pocket Inspection (DPI)

- Support for Applications identification of 3,500+ applications/protocols
- Rich set of IoT protocol and application signatures – jSCADA, MQTT, DNP3, CAP, OPC and many more..
- Support for user defined Applications & Filters
- Support for Allow, Block, Rate-Limit and Classify network traffic based on identification and policies

URL Based Traffic Identification

- Web Traffic Analysis - 460+ million domains and 13+ billion URLs scored and classified
- 83 Predefined URL categories
- URL database updated on a regular basis via Security Package Updates
- Custom URL categories

VERSA

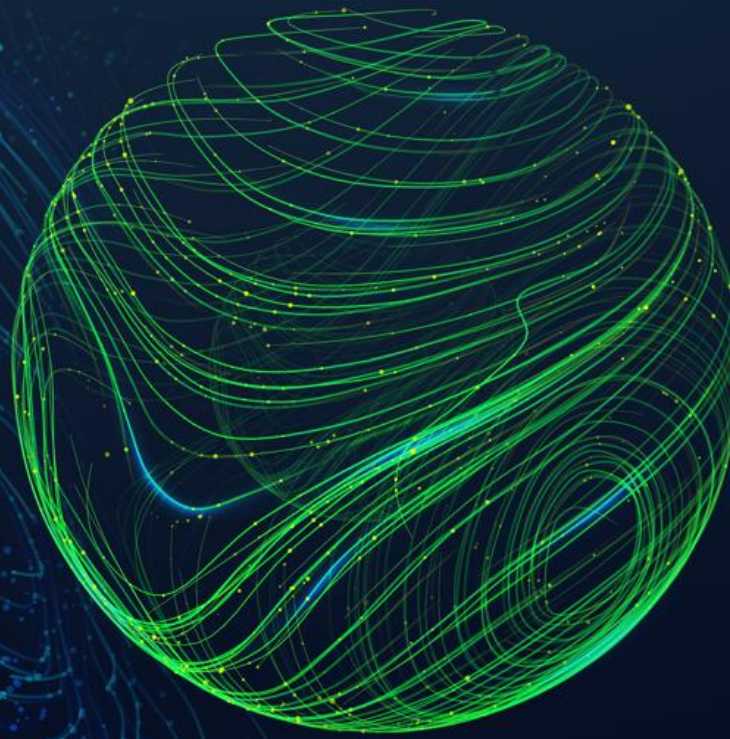
Sample IoT Protocols Recognized by Versa IOT Engine

IoT Protocol Examples	Description
Distributed Network Protocol	DNP3 (Distributed Network Protocol) is a set of protocols used between components in process automation systems (SCADA).
MQ Telemetry Transport	MQTT (MQ Telemetry Transport) is a machine-to-machine (M2M)/"Internet of Things"connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.
Constrained Application Protocol	CoAP (Constrained Application Protocol) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things.
OPC Unified Architecture	OPC is the interoperability standard for the secure and reliable exchange of data in the industrial automation space and in other industries. This plug-in classifies the OPC Unified Architecture (UA) binary protocol over TCP.
Modbus Remote Terminal Unit	Traffic related to Modbus Remote Terminal Unit (RTU), a distributed control system used in industrial process control (Emerson Process Management).
PC-cubed	PCCC stands for "Programmable Controller Communication Commands", it is used to control software running in Programmable Logic Controler (PLC). PCCC traffic can be hardware specific, this plugin addresses traffic generated by Rockwell/Allen-Bradley to talk to SLC5, PLC5E and MicroLogix PLC for service.
IEC 60870-5-104	IEC 60870-5-104 protocol (aka IEC 104) is a part of IEC Telecontrol Equipment and Systems Standard IEC 60870-5 that provides a communication profile for sending basic telecontrol messages between two systems in electrical engineering and power system automation.
Gige Vision Control Protocol	GVCP stands for Give Vision Control Protocol a standard for industrial cameras supported by several companies. This plugin classifies GVCP traffic related to control and discovery.

Device ID/Fingerprint Based Traffic Control for IoT/OT

- Traffic decision by type or class of devices
- Action: accept, deny, forward, log and more..
- Eliminates the need to authenticate the machine, provides automated device traffic management
- Example:
  - Network Connected Thermostat
  - Passive / inline detection of the device
  - Placement of the thermostat in the right network
  - Access restrictions to thermostat from other computers
  - Logging, monitoring and big data analytics of traffic coming from the Thermostat

Thank you



Versatility 2025

VERSA