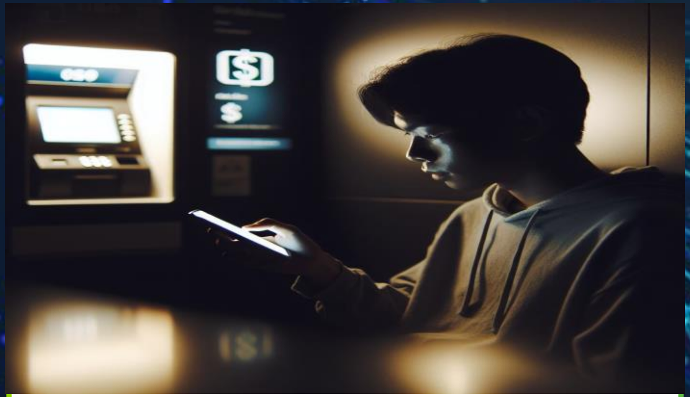
Versatility 2025

xOT Security with Versa Solution

VERSA

xOT Security: What are we securing?



IT Systems

- BYOD devices and visitor devices add to the risk

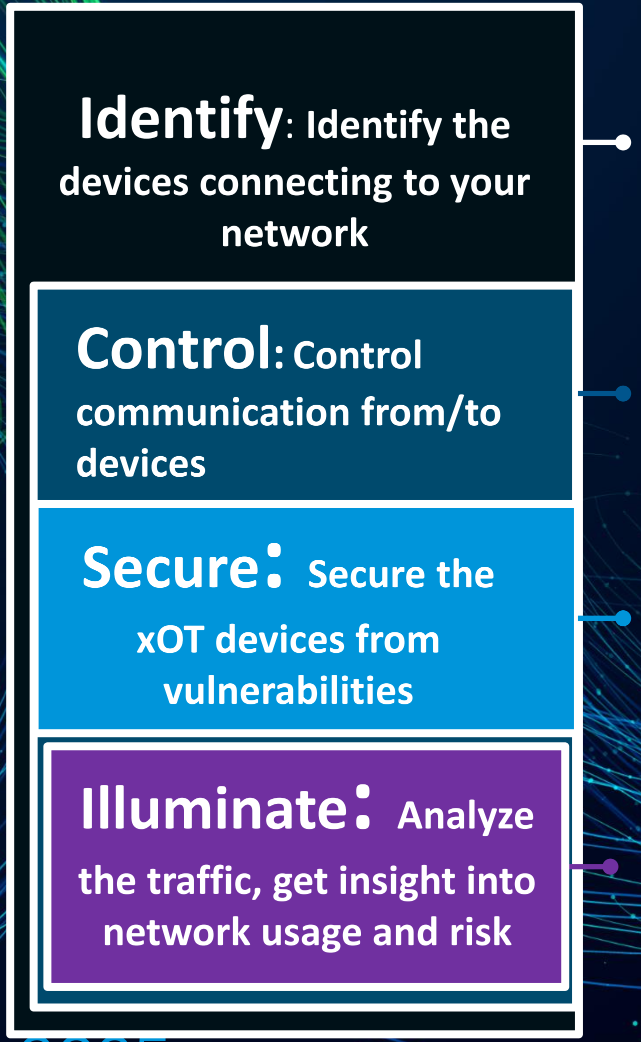
IOT devices

- Printers, cameras, temp sensors use proprietary OS and irregular patching systems

OT devices

- Manufacturing machines, control systems, factory floor devices have long life and run EOL software

Wholistic Approach to xOT security



Identify: Identify the devices connecting to your network

Control: Control communication from/to devices

Secure: Secure the xOT devices from vulnerabilities

Illuminate: Analyze the traffic, get insight into network usage and risk

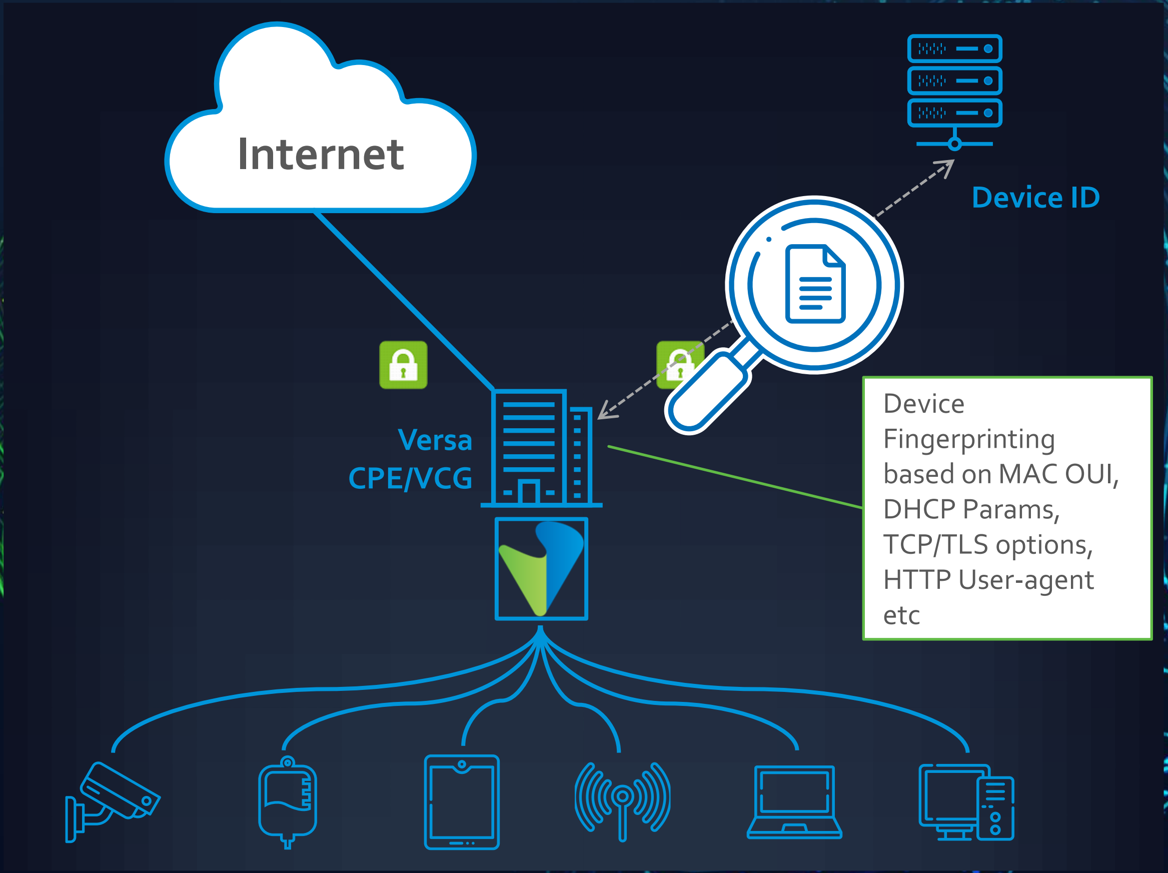
Device Fingerprinting: Uses Network Metadata, Active Probes, Integration into CM DB, Deep Packet Inspection ☑

Micro-segment and Control: Uses Zero Trust Micro-segments, App Firewall, DPI ☑

Network Security: Leverages IOT Specific Signatures. Prevents Lateral Moment ☑

Analytics: Uses AI/ML to identify traffic patterns, Anomalous patterns, Alerts the admin ☑

Identify: Device Identification & Fingerprinting



Device Fingerprinting based on MAC OUI, DHCP Params, TCP/TLS options, HTTP User-agent etc

Manual catalogues are resource intensive and never complete.
Strict Segmentation Strategy based on VLANs fail in majority of organisations

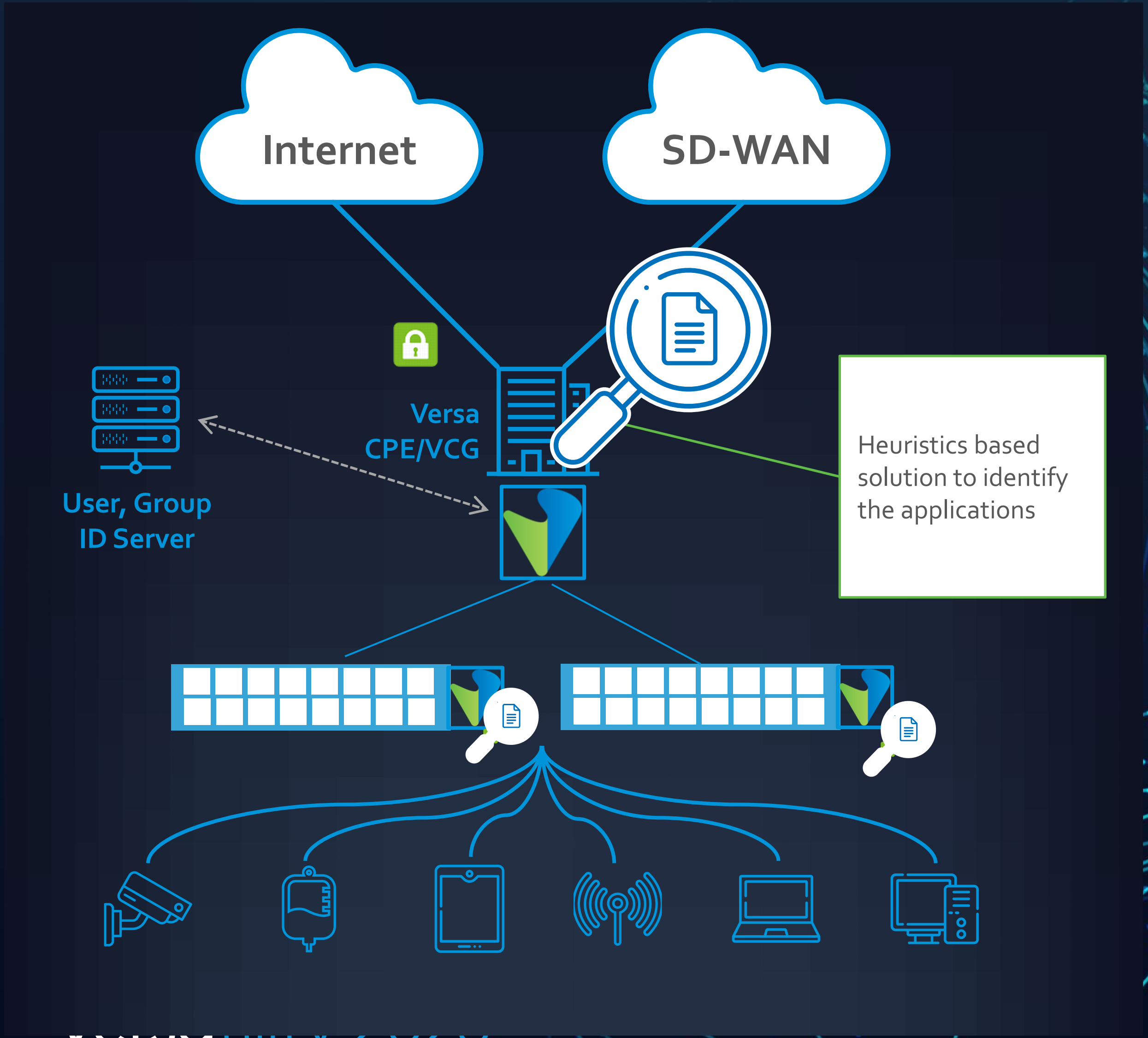
Network based Device Fingerprinting

Uses 20 plus parameters are extracted to identify the device. Completely transparent to the end device

Deep Packet Inspection

Specific signatures for SCADA, DNP3, MQTT, and other IOT Protocols

Control: NGFW, Micro-segmentation,



Application Firewall and Control

L7 based policies based on Applications (e.g., a device from IT segment should not be able to communicate with "IOT Protocols".

Dynamic Policy based on Device Type, Device Risk

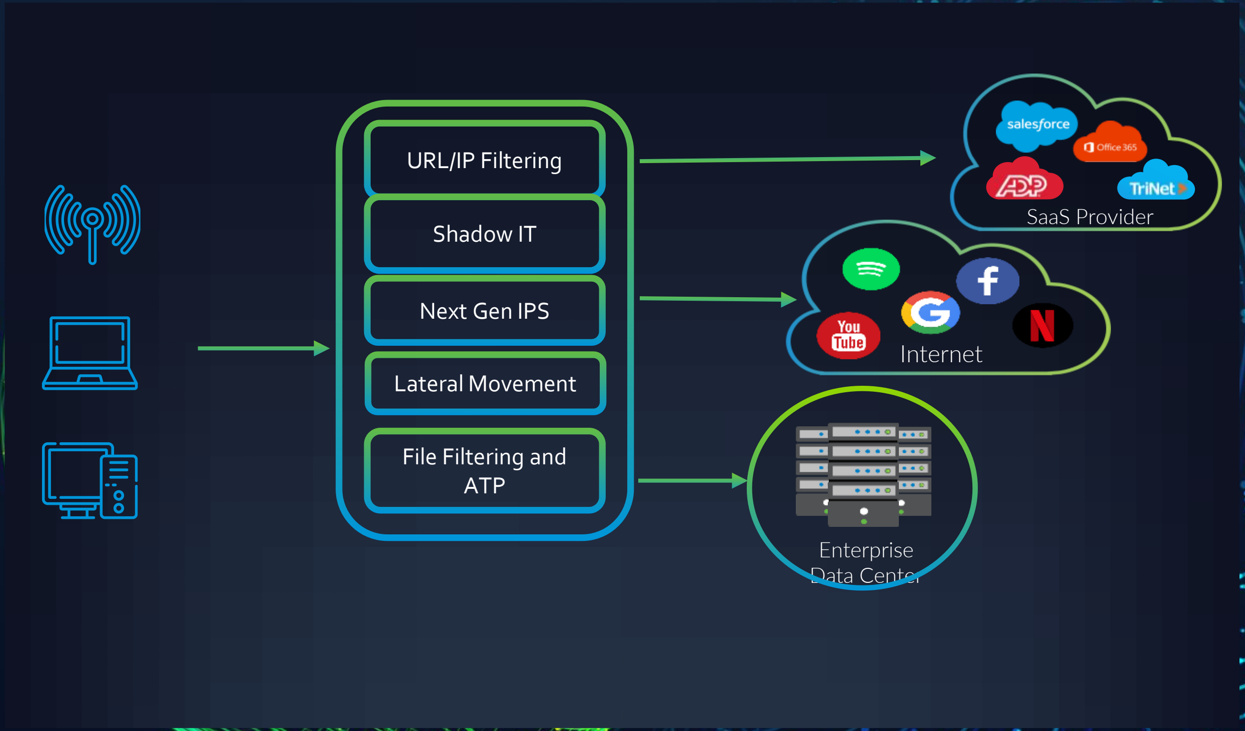
Dynamic Micro-segmentation

Control the hosts and zones who can communicate with IOT devices. 802.1x, NAC provisioning and Device ID Dynamically update the micro-segment based on detected device posture, user defined tags, 3rd party Change of Authorization (including Cisco ICE)

URL Filtering:

Allow only reputable destinations to communicate with the devices. Identify and block newly created domains, limit based on URL categories

Secure:

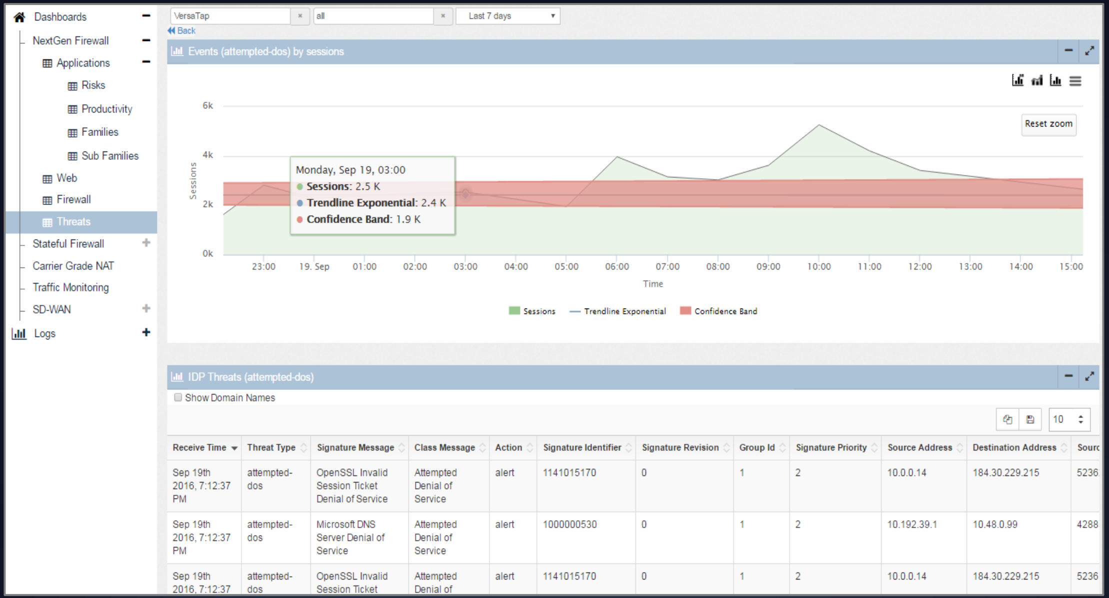


1. **Shadow IT:** Automatically block risky SaaS applications. Risk rating is dynamically updated.
2. **Next Gen IPS and Lateral Movement:** Specially designed signatures to detect threats to xOT devices. Detect Command and Control traffic. Detect lateral movements
3. **File filtering and ATP:** Advanced Threat Prevention by scanning the traffic for malware
4. **Packet Captures: Trigger based PCAP**

Versatility 2025

VERSA

Illuminate: Anomaly Detection



Monday, Sep 19, 03:00
● **Sessions**: 2.5 K
● **Trendline Exponential**: 2.4 K
● **Confidence Band**: 1.9 K

□ Show Domain Names

Receive Time	Threat Type	Signature Message	Class Message	Action	Signature Identifier	Signature Revision	Group Id	Signature Priority	Source Address	Destination Address	Sourc
Sep 19th 2016, 7:12:37 PM	attempted-dos	OpenSSL Invalid Session Ticket Denial of Service	Attempted Denial of Service	alert	1141015170	0	1	2	10.0.0.14	184.30.229.215	5236
Sep 19th 2016, 7:12:37 PM	attempted-dos	Microsoft DNS Server Denial of Service	Attempted Denial of Service	alert	1000000530	0	1	2	10.192.39.1	10.48.0.99	4288
Sep 19th 2016, 7:12:37	attempted-dos	OpenSSL Invalid Session Ticket	Attempted Denial of	alert	1141015170	0	1	2	10.0.0.14	184.30.229.215	5236

Automated Baselining: Zero-configuration base lining to determine what is “normal”

Detect Anomalies: AI/ML based algorithm to detect anomalies in the network

Visibility and Reporting: Get visibility into network operations and security environment

Alerts and Triggers: Set triggers for automated alerts based on network events

Benefits of Versa xOT Security

- Seamless integration of xOT security for your current Secure SD-WAN, NGFW and/or SSE solution
- Zero delay/Zero Day inline threat assessment
- Discover devices deployed in your network along with Risk rating and vulnerabilities
- Automatically block “unnecessary” communication based on device type. Automates policy enforcement
- Secure and Clean communication channel from IOT devices to Private or SaaS applications
- Detect zero day attacks based on file scanning, Anomalous traffic detection

Leveraging IOT Security in your network

- Versa Secure SD-WAN and Versa SSE customers can enable xOT Security
  - May require an additional license
- Seamlessly enable Versa xOT security in brownfield deployments
- Works with any SD-WAN, SD-LAN and SSE appliance/Service

Demo

Versatility 2025

VERSA

Thank you