Versa IoT Security

Zero Trust for devices

IoT and OT technologies are transforming day-to-day business operations but pose security risks and management challenges rooted in their sheer numbers, diversity, and autonomy.

- For BYOD devices attaching to the network are beyond the control of enterprise administrator and may potentially contain malicious code or weakness in security which can be exploited by the attackers to infiltrate into the enterprise domains.
- Many IOT devices run outdated software some of which are many decades old. The lifecycle of IOT devices is much slower than standard software lifecycle. This results in these devices operating for decades after the last security patch has been issued by the software vendor.
- Many IOT devices run custom operating systems where patching over the network may not be supported or is complicated consuming precious admin resources.
- And, since the IOT devices are typically autonomous (i.e., there is no human actively interacting with it), many of the symptoms of attack (like device slowness) are not apparent. Hence the attack can go unnoticed for months or years.
- The IT and OT devices in an enterprise network far out number the employees and contractors in most organizations. The devices are challenging to identify, catalogue and maintain.
- Enterprise users are connecting sanctioned or unsanctioned devices to the network. IT organizations are unaware of all devices that are network connected, which makes segmentation and protection tasks more difficult

The basic task of identifying and cataloguing all of them can be its own challenge for IT. Their purpose-designed, custom operating systems don't support standard security agents and are complicated to patch and update in a timely manner. These characteristics makes them softer targets for staged cyberattacks.

Versa IoT Security is a single, integrated, inline solution that automates the identification and classification of IoT/OT devices, applications and secures them through end-to-end segmentation and real-time, full-stack advanced edge security. Versa IOT security solution integrates seamlessly and can be deployed with Versa Secure SD-WAN, SD-Security, SD-LAN and SSE products. Most fundamentally, Versa's platform extends Zero Trust security to "things," applying least privilege access to even "client-less" devices and dynamically reevaluating their security posture, while supporting the complete IoT/OT device management lifecycle across discovery, control, security, and monitoring

Discovery

The discovery phase provides a completely automated, scalable mechanism for your security team to identify and get complete visibility into the devices installed in your network, including any unsanctioned devices, and plan network security strategy accordingly. Devices are identified according to key parameters (device category, manufacturer, firmware version, serial number, etc.) using a combination of AI/ML based device fingerprinting and protocol analysis engine. Inline identification of devices and classification eliminate the lag between device detection and granular, device-specific policy enforcement. Instantaneous, inline policy enforcement improves the security posture by further eliminating opportunity for the intrusion.

The device identification and classification can identify hundreds of thousands of device types along with serial number, device category, manufacturer, device risk and other details. These metrics can be used to apply granular device specific policies to protect the network from external threats.

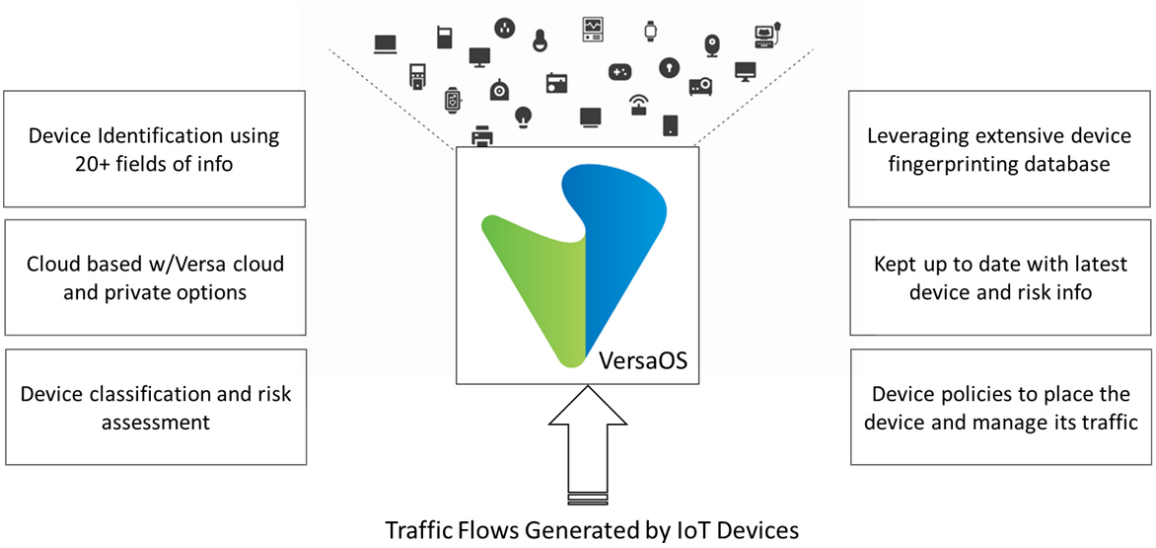
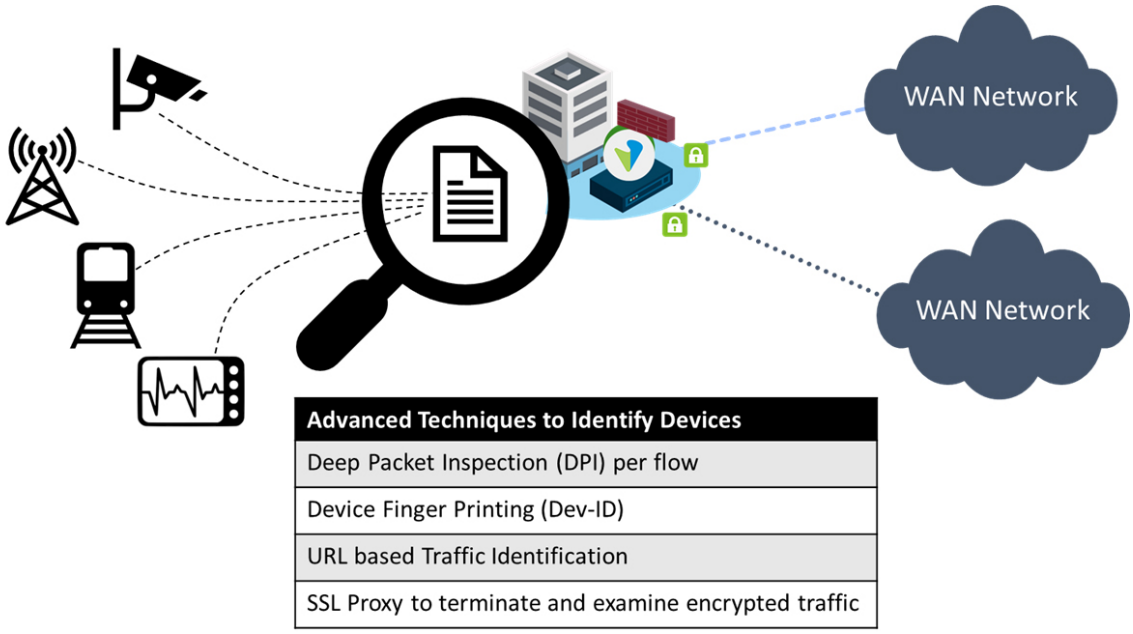


Figure 1- Cloud-based IoT and OT device discovery

Versa's market-leading AI/ML-based App Identification Engine analyzes traffic flow to identify and gain insight into the activity of the applications and resources accessed over your network. It recognizes over 4,000 applications, including market leading IoT/OT applications and commonly used SCADA protocols like MQTT and CoAP.



Advanced Techniques to Identify Devices
Deep Packet Inspection (DPI) per flow
Device Finger Printing (Dev-ID)
URL based Traffic Identification
SSL Proxy to terminate and examine encrypted traffic

Figure 2 - Automated discovery of IoT/OT devices on the network

Control

The application of isolation and strict policies controlling who can communicate – and what they can communicate -- with the IoT devices are basic principles underlying Versa's approach. Versa is able to enforce device-level policies through two main mechanisms:

1. Dynamic micro-segmentation to create siloed channels based on the device's type and risk profile
2. A policy-based application firewall that applies application-based DPI, URL filtering, and other security measures.

Dynamic micro-segmentation

Versa dynamically microsegments IoT devices to protect them from external interference, prevent lateral movement, and minimize the blast radius in the event any device is compromised. When an IoT device connects to the network, its access is controlled to allow only specific users and applications to communicate with it, allow the device to reach only specific internal resources and/ internet-based destinations. Versa provide the ability to create micro-segments based on the device's identity, device class, risk profile and context. The newly discovered and classified IoT device is automatically allocated to a micro-segment which provides least privilege access for the devices.

While Versa supports VLAN based macro-segmentation, Versa's micro-segmentation is implemented dynamically and is more granular than the usual static segmentation based on VLAN tags. Versa uses standards-based Secure Group Tags (SGT) to provide micro-segmentation. SGT tags can be prepended to the traffic that is destined to and from the IoT/OT devices to separate such traffic from the rest of the network traffic.

Standards-based Secure Group Tags (SGT) are prepended to IoT/OT device traffic and their values are assigned from a centralized system or taken from a customer's third-party policy server. Use of SGT tags on IoT/OT traffic flows also allows consistent implementation of policy-based traffic management, segmentation, and security functions across the network so it is effectively a network-wide solution instead of a node-specific solution.

Policy-based application firewall

Versa's NGFW is able to apply application-specific policies to the hundreds of automatically detected applications and protocols identified by the App Identification Engine. Additionally, customers can define their own applications and restrict the type of applications and data being exchanged by the devices.

Security

Versa's Next Gen Firewall secures devices by scanning both encrypted and unencrypted traffic and detecting and preventing attacks at every network edge. Advanced security features like URL filtering, NG IPS, Anti-Malware, ATP etc. URL filtering and categorization is used for detecting traces of command-and-control traffic, providing an early warning of compromise.

Versa's Next Gen IPS scans both north-south traffic and east-west traffic to detect IOCs and provides signature-based and anomaly-based detection. The solution identifies any attempts to exploit vulnerabilities and automatically blocks access, including use of specialized signatures for IoT-specific vulnerabilities. In addition to micro-segmentation, Versa's specialized lateral movement detection algorithms prevent the spread of any compromise. Anti-malware and anti-virus protection apply multi-layered techniques such as heuristics, signature matching, and Advanced Threat Protection, which includes sandboxing.

Underpinning Versa's IoT defenses is a dynamic Device Risk Score algorithm. The risk score reflects all activity and incidents related to each device, enabling administrators to make informed quarantine decisions.

Monitoring

Versa Secure IoT provides single-pane-of-glass, near-real-time visibility into and management of network activity, traffic, events and alerts through Versa Analytics, which performs baselining, correlation, and prediction, all optimized by an AI-powered data lake feedback loop, while providing practical administrative tools like historical search, reports on usage metrics, performance metrics, trends, security events, and alerts. The automatic baselining of traffic patterns, destinations and active times is used by device behavior analytics to detect anomalous activities (e.g., devices communicating with an unusually large number of destinations or experiencing unusually high data volume).

Licensing and pre-requisites

Versa IoT Security is an optional add-on license with Secure SD-WAN, Secure SD-LAN or SD-Security licenses. Please reach out to your Versa account team for further licensing information.

Features

Device discovery, fingerprinting, & monitoring

- Agentless, real-time discovery and continuous asset inventory
- DPI to identify IoT applications and protocols
- Device fingerprinting based on 20+ attributes and patterns
- Extensive device profiling and classification
- Device behavioral monitoring and analysis
- Dynamic risk assessment with AI/ML

Network access and traffic control

- 802.1x-based Network Access Control (NAC)
- Policy-based traffic management and prioritization
- Zero trust network access (ZTNA) for IoT and OT devices
- Segmentation and micro-segmentation into controlled zones
- Inline identification of IoT application traffic and protocols

Security

- Next-Gen Firewall (NGFW) protection tailored to IoT devices
- URL filtering, IP reputation, geo-location filtering
- Next-generation IPS against Zero-Day attacks
- Advanced threat protection (ATP) with multi-sandboxing
- Continuous threat intelligence updates
- SSL proxy for encrypted traffic inspection

Analytics & reporting

- Network traffic and performance analytics
- Integrated security and compliance reporting
- Customizable dashboards and alerts

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