Unified SASE for IoT

IoT/OT vulnerabilities

Internet of Things (IoT) and operational technology (OT) devices have become increasingly present in the modern enterprise, enhancing business operations and boosting productivity. However, securing them has unique challenges, as they are deployed in large numbers in varied environments and geographies with security concerns that are distinct from traditional IT security.

Most IoT devices run on a minimal, specialized operating system designed to perform a single task, making them essentially "clientless," so the protections typically applied to a laptop, mobile phone or tablet can't be applied, and they aren't managed by identity and access management (IAM) suites, precluding the application of policy-based controls. These unique characteristics make them attractive targets for hackers, as they frequently sit at the center of controls for critical infrastructure, manufacturing and healthcare systems, and even the most unexciting office network-connected device can serve as a stepping stone for orchestrated ransomware, data theft or DDoS attacks.

Securing IoT devices with unified SASE

Versa's Secure Access Service Edge (SASE) platform unifies networking and security functions into a single service to protect against the inherent risks in IoT – from device and protocol identification to policy controls. It begins with an ability to build visibility into the IoT devices on the network through device fingerprinting and the identification of IoT protocols across the network. Once IoT devices are identified and their flows are mapped, they can be placed in the right microsegments.

Once segmented, the network is protected against lateral movement from compromised IoT devices, and network-based security functions can monitor and control both the entry and exit from each segment. With the application of a full suite of security capabilities, from secure web gateway to CASB controls, IoT devices and their protocols can be monitored for their traffic patterns and any malicious behavior. With identity, device and application-level controls in place, user behavior analytics feed into baselining and anomaly detection.

Zero trust for things

Versa's ability to apply Zero Trust network access (ZTNA) policies to IoT devices, despite their "clientless-ness," adds a compelling dimension to IoT security. The Versa Operating System (VOS), which underpins the SASE service, comes with built-in capabilities to identify and fingerprint over one million types of devices and look at the different attributes of traffic generated by the devices while running inline. With the system armed with detailed information on a per-device basis, security and networking decisions can be implemented at a per-device level of granularity.

Feature Highlights

Elastic NG Visibility & Control

Zone-based stateful firewall policy rules based on:

- Application identification
- URL and content classification
- Domain
- Users and group
- Location/GeoIP

Packet capture ALG support

File Filtering

- Filtering by file signature
- Over 5B file signatures
- Supports HTTP, FTP, SMTP, POP3, IMAP, MAPI
- Whitelist, blacklist
- Decompression support

IDS/IPS Profiles

- Signature/anomaly based detection
- Custom IDS rules
- Packet capture
- Signature updates

URL Filtering Profiles

- Category-based actions
- Reputation-based actions
- Whitelists, blacklists
- Captive portal pages

Elastic L3 to L7 DoS protection

- Anomaly-based detection
- Volumetric DoS detection
- Multi-layer DoS detection
- Custom scripting for actions

Device Fingerprinting

- Device identification using 20+ attributes
- Device fingerprinting database
- Device posture profiling

App Identification

- 3,500 applications/protocols
- Support for user-defined applications

Security Updates

- Full/incremental updates daily
- Real-time updates

HTTP and HTTPS Proxy

Certificate checks, transparent proxy and explicit proxy, DNS and AD integration.

Anti-Virus Profiles

Customize AV scanning based on application/file types.

Lateral Movement Detection

Create firewall rules using templates or for a specific CPE.

Micro- and Macro-Segmentation

Dynamic, software-defined segmentation adapts to security posture changes in IoT devices.

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