Internet of Things (IoT)

Internet of Things (IoT) devices are becoming increasingly present in modern enterprises and have transformed the way we work. While they can be used to enhance productivity and business operations, their unique characteristics also present an avenue for threats to enter your infrastructure and quickly move to a point of impact.

Many organizations connect IoT devices to their infrastructure without fully understanding the security risk.

IoT Vulnerabilities

Because most IoT devices run on a minimal operating system and are programmed to perform a single task, you can't apply the same embedded protections as you would with a laptop, mobile phone or tablet. Many aren't even managed by Identity and access management (IAM) software suites, precluding the application of traditional policy-based controls.

The broad nature of IoT/OT or network attached devices make them valuable targets for hackers. They are often at the center of controls for critical infrastructure, enabling manufacturing processes or used to deliver life-critical healthcare. These factors contribute to the severe impact of breaches that begin with an IoT compromise.

The uniqueness of these systems provides an opportunity for adversaries to compromise IoT devices as a launching point to orchestrate attacks – including phishing, data theft and distributed denial-of-service (DDoS) attacks. At a minimum, compromises provide stepping stones for lateral movement across the infrastructure.

Securing IoT devices

Securing IoT devices must focus on identifying, classifying, and enforcing proper controls. Versa's Unified Secure Access Service Edge (SASE) platform unifies IoT and network security functions into a single service to secure 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 with device fingerprinting, and identifying 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, your network is protected against lateral movement from compromised IoT devices and their flows. You can then monitor, and control both the entry and exit from each segments using the appropriate network-based security functions. With these controls in place, IoT devices and their protocols can be monitored for their traffic patterns and for malicious behaviors. Techniques like UEBA allows baselining and anomaly detection.

And with Identity, device and application-level controls, the Versa Unified SASE platform can reduce the impact of compromise through threat detection and prevention.

Feature Highlights

Elastic NG Visibility & Control

Zone based stateful firewall Policy Rules based on

- Application Identification
- URL and Content Classification
- Domain-based
- 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

Micro and Macro Segmentation

VERSA NETWORKS

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