VERSA

Do's & Don'ts

of IoT Security

Table of Content

Don’ts of IoT Security

Do’s of IoT Security

©2024 Versa, Inc.

Understanding IoT Security Risks

The rapid proliferation of the Internet of Things (IoT) devices has transformed business operations in nearly every industry. From smart home devices to industrial sensors, IoT solutions are changing how businesses operate, manage resources, and deliver services. However, this hyper-connected landscape also introduces significant security challenges.

First and foremost is the staggering number of devices being brought online – nearly 19 billion IoT devices. These devices don't just include your smart TVs, cameras, printers, or other typical connected office equipment. "IoT" now includes a breadth of industry-specific connected devices.

For example:

- Industrial IoT (IIoT) and operational technology (OT) devices connect industrial control systems, supervisory control and data acquisition (SCADA) systems, and other controls used in utilities, power grids, manufacturing plants, and industrial environments.
- The plethora of Internet of Medical Things (IoMT) includes everything from hospital equipment to wearable sensors, such as glucose monitors, to injectable sensors for robotic surgery.

Yet despite their advanced technologies and innovative uses, IoT devices and the networks they run on are highly susceptible to cyberattacks. The large number of IoT devices expands the attack surface or organization across sectors. These devices often operate on legacy infrastructure, which may be more vulnerable to attacks. Many also run outdated or purpose-built software, making it near-impossible to apply regular updates or patches, especially if devices are deployed in remote locations or patient homes.

Even when devices are physically located on an organization's premises, due to the sheer number of devices, IT administrators frequently lack visibility into which IoT devices are connected to the network. This makes them prime entry points for attackers to gain a surreptitious hold on the network. Risks compound once attackers gain access to a single IoT device, as they can move laterally across the network, jeopardizing other sensitive systems and data.

The stakes are even higher with OT and IoMT devices. These devices control critical infrastructure or medical equipment. In the event of a breach, resulting downtime can impact public safety or patient health, and lead to life-threatening consequences.

Given these challenges, it's essential to rethink how IoT security is approached. This eBook outlines key do's and don'ts to help organizations strengthen their IoT defenses.

Don’ts of IoT Security

Let’s start with what not to do when it comes to securing IoT devices.

1. Don’t Rely on Perimeter-Based Security

Traditional security models are built on perimeter-based defense, where the network is segmented into “trusted” internal zones and “untrusted” external areas. However, this approach fails with modern business practices where devices on the inside and outside of the organization are constantly communicating with each other. In fact, with cloud computing and work-from-anywhere, the idea of a perimeter has become obsolete.

Even if an IoT device resides full-time on the company premises, it typically is still able to communicate with the “outside.” Whether it’s allowing communication with the manufacturer to push down updates or allowing remote management through a portal, perimeter-based security models cannot protect these dynamic, interconnected systems.

What to do Instead

Embrace Zero Trust, utilizing Zero Trust Network Access (ZTNA) as a foundation. ZTNA operates under the assumption that no user or device should be implicitly trusted by default, regardless of whether they are inside or outside the network perimeter. It emphasizes strict access controls, continuous authentication, and minimal access privileges to ensure that only authorized users can access specific resources, thereby reducing the risk of unauthorized access and data breaches.

Applied to IoT, Zero Trust principles further advocates device verification, micro-segmentation, and continuous monitoring of device interactions to ensure secure communications across the entire network.

2. Don’t Rely on Manual Processes

One popular IoT management strategy is to create a dedicated “IoT VLAN.” In theory, all IoT devices are placed in that segregated VLAN so that policies can be applied to IoT devices without affecting the rest of the network and other client-based devices like laptops.

However, modern enterprise environments are highly dynamic, and manual device management is both inefficient and risky. With potentially thousands of devices per site, manually identifying, onboarding, and segmenting each one creates significant operational overhead and increases the likelihood of human error. It’s easy to miss a device or apply the wrong policy to another, for example. Manually segregating IoT devices can therefore lead to blind spots and vulnerabilities, leaving potential entry points for attackers.

Moreover, modern organizations are constantly in flux. New devices, systems, and processes are frequently introduced, and everything must be “turned on” as soon as possible. As a result, despite the best efforts to segregate IoT devices to their own part of the network, networks tend to end up as mixed used networks eventually. This in turn presents challenges to enforcing consistent security policies.

What to do Instead

Automate device discovery. Use an IoT security platform that automatically detects and classifies devices on the network significantly reduces manual effort and human error.

Use dynamic risk analysis. Risk levels of a device can change as time goes on. Static policies cannot account for changes in risk. Modern Zero Trust security platforms leverage AI and machine learning (AI/ML) to detect anomalies in the network and device behavior. These capabilities allow different policies to take effect when risk levels change, ensuring appropriate policy application and enforcement based on current risk levels.

3. Don’t Overlook OT Devices

OT devices, once isolated from traditional IT networks, are now increasingly interconnected and connected to external networks or the cloud. Many organizations have integrated older, legacy OT machinery into their digital networks for efficiency and performance improvements. However, these OT devices were not designed with modern cybersecurity in mind and run on legacy or custom software. In many cases, compromises in OT networks can lead to access into IT networks.

Further, OT devices control critical infrastructure in industries like manufacturing, energy, and transportation. A successful attack on an OT system can lead to production halts, operational downtime, or worse—physical harm to employees or the public. Yet, many organizations overlook OT in their security strategies, leaving these critical systems exposed.

What to do Instead

Integrate OT devices into your IoT security strategy. Treat OT systems as part of the broader network, ensuring that they are subject to the same monitoring and protection measures as other devices. Use advanced security features real-time threat detection and micro-segmentation and to protect OT systems from cyberattacks and limit attack impact.

Do’s of IoT Security

We’ve covered what not to do – now here’s what to do instead for IoT Security.

1. Know What’s Connecting to Your Network

One of the biggest challenges with IoT security is maintaining visibility over the vast number of devices that are connecting to your network. From smart cameras to industrial sensors, each device poses a different security risk to the network. If administrators are unaware of what is connecting to their networks, they cannot effectively secure those devices.

We’ve noted that manual onboarding and management of devices is not sustainable. With thousands of devices in large organizations, the process of identifying and securing each one would be labor-intensive and error prone.

How to Achieve This

Automate device discovery. Use a security platform that can automate device discovery. These solutions allow organizations to automatically detect new devices in real-time when they’re added to the network. This continuous process ensures that previously connected devices are also recognized and managed securely. A robust solution will also provide metadata about each device such as device class, operating system, and model number, allowing admins to get a sense of device risk with a casual glance.

2. Categorize Devices and Define Risks

Not all IoT devices pose the same risk to the organization. Some, like industrial control systems, carry a much higher level of risk than office IoT devices like smart printers. To effectively secure IoT environments, organizations must categorize their devices based on risk and implement appropriately tiered security policies that reflect these distinctions.

Just as higher-risk IoT devices, such as critical control systems, need stricter security controls, incident response for those devices must be similarly appropriate to their risk level. To continue our example, an industrial control device showing signs of suspicious behavior warrants a different response than that of a smart printer. An appropriate policy for the printer may be to require credentials for employees and prevent visitors from accessing the printer. An appropriate policy for the industrial control device, on the other hand, may be to end existing sessions, prompt for credentials, and immediately block access to other devices and the internet. In addition, locking down OT devices requires additional processes to prevent downtime – any equipment the industrial control device controls must still be operational and controllable. The printer, on the other hand, would not need additional processes and could be simply segmented from the network.

Without proper categorization, organizations run the risk of applying one-size-fits-all security policies, which can leave high-risk devices inadequately protected and reduce usability in lower-risk devices.

How to Achieve This

Categorize devices based on risk. Use a security platform that can organically categorize and fingerprint IoT devices. Once you know what device types are on your network, determine their varying risk levels, and create policies for each risk level. Make sure you also create policies that can be enforced if a device's risk level increases. These policies should be automatically applied to existing and new devices connecting to the network.

Use dynamic risk scoring. Device risk levels may change due to vulnerabilities or changes in usage. Using dynamic risk scoring helps adjust security measures in real-time so there is no gap in protection. Once a device's risks score increases over a pre-defined threshold, stricter policies should be automatically applied and enforced.

3. Apply Zero Trust to IoT Connections

As organizations continue digital transformation, more resources are being allocated to the cloud, creating new possibilities and benefits. Organizations are now able to move costly datacenters to the cloud and connect OT devices to cloud resources. And even historically air-gapped networks, including everything from manufacturing plants to oil rigs, can now be connected to the cloud and interconnected to each other.

The benefits are many. Besides cost savings, connecting to the cloud brings greater accessibility to resources, strengthens internal communication, and even reduces physical risk as in-person deployments to dangerous locations can be minimized.

However, just as Zero Trust is being adopted in traditional IT systems, security for IoT environments must follow suit. IoT devices communicating with outside cloud resources are highly susceptible to attacks. The application of Zero Trust principals to IoT devices ensure those devices have strict controls over what they can access, are micro-segmented to minimize impact of compromises, and have ongoing monitoring to catch security threats early.

How to Achieve This

Implement dynamic micro-segmentation. Use a security solution to apply dynamic micro-segmentation to IoT devices. This provides several benefits: 1. Devices can be automatically segregated by device category and risk, reducing management overhead, 2. Granular policies can be applied to each device category for precise control, and 3. Impact to the rest of the network is limited in the case of a compromised device.

Apply advanced security controls. The advanced security features used in other parts of the network should also be applied to IoT environments. Next-generation firewalls (NGFW), URL filtering, and intrusion prevention systems (IPS), this approach provides granular control over IoT connections and mitigates the risk of unauthorized access. Using AI/ML-assisted behavior analytics can surface abnormal or risky behavior early in IoT devices. This early alerting is critical for IoT devices as most are client-less so tell-tale signs of compromise, such as delayed device response, are not easily apparent.

4. Continuously Monitor Devices

Security is not a one-time activity. An IoT device's security posture can change over time, making continuous monitoring essential. Static security policies cannot account for shifts in risk levels, such as when a vulnerability is discovered in the OS or a previously secured device becomes compromised. Without continuous, real-time monitoring, organizations risk having policies that do not align with a device's actual security posture, leaving them exposed to threats.

How to Achieve This

Use AI-powered behavior analytics. Deploy AI-driven device behavior analytics to continuously assess device behaviors and activities. By analyzing patterns and baselines, AI tools can assist with baselining normal behavior, detect anomalous behavior, and correlate events. Predictive analytics can also help anticipate future threats, allowing organizations to act preemptively.

5. Secure Partner Integrations

IoT ecosystems are increasingly extending beyond organizational boundaries to those of vendors, service providers, and business partners. As business partners offer new managed IoT services, ensure these integrations do not introduce new security risks. Organizations must take steps to secure partner integrations and clearly define partner access.

How to Achieve This

Use a multi-tenant platform. Use a multi-tenant platform with granular security controls to reduce management complexities while securing B2B connectivity. By managing partner integrations through a single, unified platform, can ensure that each partner's access is limited to only what is necessary. This reduces the risk of a partner's vulnerability affecting your own organization.

Versa's Approach to IoT Security

Versa provides a fundamentally different approach to IoT security by focusing on a holistic approach. Rather than deploying sensors across your organization, Versa leverages our comprehensive network and security platform to extend advanced security and protection to all devices. With granular, real-time visibility and protection, organizations can secure their IoT ecosystem without manual overhead typically associated with device management.

Key features of Versa's IoT security strategy include:

Automatic device discovery and fingerprinting: Versa enables administrators to automatically identify all connected IoT devices, eliminating the need for manual onboarding. All devices are automatically categorized and assigned default risk levels for a plug-and-play solution.

Zero Trust enforcement: With Versa, organizations can implement Zero Trust security measures across all IoT devices, ensuring that every connection is validated and secured.

Advanced security capabilities: Versa's IoT solution includes NGFW, URL filtering, IPS, ATP, and other advanced features that protect against a wide range of threats. Detailed logging and monitoring keep admins up-to-date on device actions and behaviors.

Dynamic detection and response: Versa uses dynamic risk analysis and scoring so every device's security posture is assessed in real time. Combined with our dynamic micro-segmentation and lateral movement detection capabilities, administrators can take immediate action to automatically isolate compromised devices, reducing the impact of attacks.

Strengthening Your IoT Security

Securing IoT environments requires a thorough, proactive approach that incorporates modern security practices such as Zero Trust protections. Taking advantage of automation, dynamic protections, and AI can further streamline IoT management and security. By implementing these strategies, organizations can protect take advantage of IoT benefits while staying safe from emerging threats.

Versa's comprehensive IoT security solutions provide organizations with the tools they need to effectively manage and protect IoT ecosystems, ensuring a seamless integration of devices without compromising security.

Next steps

Schedule a demo to see how to secure your IoT environment with Versa.

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

© 2024 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and VOS are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners. Part# SB_VCFW-01.0