COMCAST BUSINESS | MASERGY

WHAT YOU'LL LEARN

- How to monitor endpoints vs. "things"
- Key security considerations for IoT
- How network segmentation applies

E - GUIDE

The truths and lies of IoT security: monitoring connected devices

As the Internet of Things (IoT) accelerates the pace of the enterprise with data-driven decision making, CEOs, CIOs, and CISOs are making the dash for the IoT playing field. But how do they get in the game while not jeopardizing security? Yesterday's security techniques and legacy networks don't always transition well into the new world of IoT. To expose the certainties and the snare traps of IoT, let's play a game of "truth or lie."

Truth or Lie?

Monitoring the security of thousands of connected devices is the same as monitoring thousands of endpoints.

THE ANSWER: Lie

Many assume that end-point detection tools can be applied to connected IoT devices, making it easy to monitor hundreds or even thousands of connected things. But that's a fallacy.

These models cannot be practically applied to IoT. Why? Because of the lack of standardization. Not every connected device is running on the same operating system, which causes logistical and scalability challenges. The end-point detection and response tools we have today aren't fit for IoT because:

- Devices use a variety of communication protocols,
- Potential vulnerabilities come from disparate proprietary systems, and
- Security patches are not easily available or deployable (much less available for testing and quality assurance)

Therefore, we can't apply monitoring standards across all devices and manage that complex operation from a central system. Our technology simply isn't there yet.

Truth or Lie?

Network segmentation techniques are effective in securing an endless number of connected devices.

THE ANSWER: Truth, but...

Yes, enterprises should isolate IoT devices on their own network, separating device traffic from other critical network infrastructure. But, it's important to note that segmentation is just one of many security strategies that should be deployed with IoT.

Network segmentation is highly effective for IoT, because it's a primary approach for security and isolating threats from within. As one of the strongest techniques for security, it improves access control, monitoring, response to incidents, and containment. Creating isolation zones (discrete virtual networks and Layer 3 VPNs) puts layers of protection in place with incremental gates that help limit the attack surface in the event that a connected device is compromised. Isolated zones are helpful because IT teams can write security policies and rules for each one depending on the type of traffic originating. This helps create granular controls that can be applied only to those connected devices.

Key security considerations for IoT:

- Corporate security policies for connected devices
- Network design flexibility and separate network instances to support IoT infrastructures
- Deep network visibility to efficiently investigate suspicious behavior
- Monitoring backed by machine learning and behavioral analytics
- Risk from vulnerability exposure to help protect against botnets searching for target IoT devices
- Patches and updates for all the connected devices

Additional resources

- IoT Necessities: Getting Your Network and Security Ready
- ZK Research Buyer's Guide for SD-WAN
- Friction in the IT Helix: How to Create Harmony between Network Design and Security
- True Network Security Depends On More Than Perimeter Defenses
- The Managed Security Services Provider Survival Guide
- There's Help for CISOs Overwhelmed By Security Threats

About Masergy

Masergy is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled application performance across the network and the cloud with Managed SD-WAN, UCaaS, CCaaS, and Managed Security solutions. Industry-leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.