How to remove IoT & OT from your attack surface

Summary

With IoT and OT (operationalized technology) sprawling across the globe, organizations are able to provide more value to their customers. But for IT security teams, this presents a growing attack surface that's easy for malicious actors to exploit. Weak devices and architectures present teams with a question they need to answer: How can IoT and OT disappear from the attack surface?

Zero Trust security models call for nano-segmentation, which cloaks connected devices. But most solutions lack the ability to limit lateral movement if found out by attackers. ZPE Systems' Nodegrid Mini SR — a smartphone-size device — solves this by creating an overlay network and running preferred security solutions directly on the box. Organizations in manufacturing, healthcare, utilities, and more can use this solution to remove their sprawling IoT/OT from the attack surface and add an extra layer of protection to their critical operations.

Problem – IoT & OT present a big attack surface

IoT and OT are crucial to every industry, with more than half of an organization's devices being considered IoT/OT. These devices include security cameras, building automation systems, pressure sensors, gauge readers, and many others that gather important data or serve critical operations.

According to Ericsson, there were more than 13 billion IoT connections in 2022, and this number is expected to grow to more than 34 billion by 2028. While manufacturers, healthcare companies, smart cities, utility providers, and others see this as a way to deliver more value to their customers, there's one group that sees billions of opportunities to exploit these organizations. That group is cyber attackers.

Thales Group reports that the number one IoT-related security concern is attacks on IoT devices that impact critical operations. With IoT/OT sprawl, attackers are presented with an enormous target. This target is also easy to hit due to a significant weakness inherent to these devices: IoT/OT are not designed to provide their own security.

Gap – IoT/OT devices are easy to hit

The concept of Zero Trust Security — which involves segmenting network access with micro perimeters that restrict lateral movement — is difficult to achieve when so many connected devices are IoT and OT. This is because these devices are not designed to provide their own security, a weakness that stems from three IoT/OT design flaws:

1. IoT/OT devices often remain outdated and unpatched
2. IoT/OT are closed systems that can't run third-party security solutions
3. IoT/OT devices often connect via weak hardware that can't run security tools

This creates a sprawling attack surface that's easy to exploit. Imagine a city's water treatment plant, where day-to-day operations depend on data gathered by IoT/OT sensors. An attacker who comes within range can access and disable these sensors, ultimately shutting down the plant and holding the city's water supply for ransom.

Solution – Cloak devices with nano-segmentation

One solution to secure IoT/OT devices is through nano-segmentation. This is achieved by placing a low-cost appliance, such as an Intel NUC, in front of these devices. This isolates, or cloaks, connected IoT/OT while allowing traffic to be sent/received only to authorized locations

This solution is easy to deploy, but it does not provide total security. This is because these cloaking devices do not come with enough power to run security solutions directly on the box. In the water treatment example above, a savvy attacker can uncover the cloaked Intel NUC and sensors, and potentially move laterally across the network to servers and databases containing customer information.

ZPE Systems' Mini SR cloaks devices and runs security applications

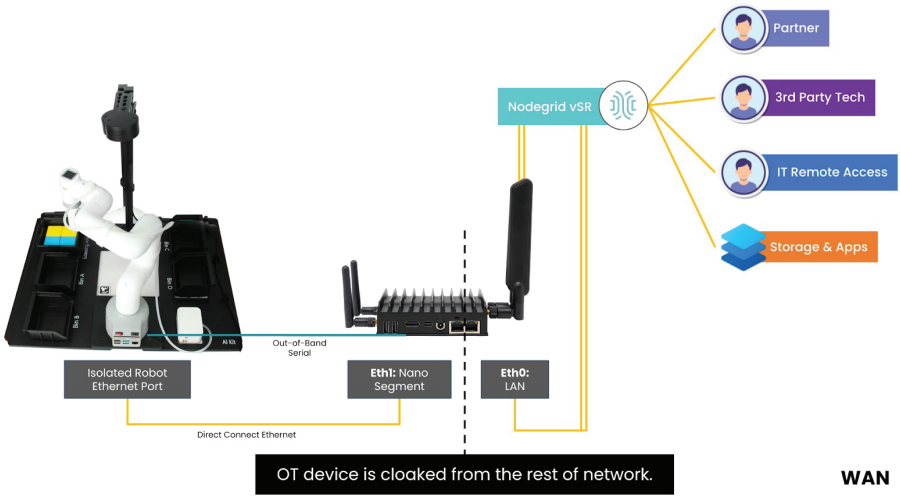
ZPE Systems' Mini SR delivers the closest thing to air-gap isolation for IoT/OT, and runs best-of-breed security solutions directly on the device. The Mini is the size of a smartphone but comes with a multi-core Intel CPU, making it an easy-to-deploy solution with enough power to enforce Zero Trust policies.

NEW

Nodegrid Mini SR

Out-of-band Cloud Gateway for IoT/OT/IoMD applications

Organizations can deploy the Mini between IoT/OT devices and the rest of the network in order to cloak these devices. The Mini creates an overlay network and provides out-of-band management access. Additionally, the onboard Nodegrid OS can run containers and applications, whether custom-built or from best-of-breed security providers. The Mini SR essentially cloaks all connected IoT/OT, and hosts its own safeguards to seal out breaches if revealed by a savvy attacker.



Secure your IoT & OT infrastructure with ZPE Systems

Closing your organization's attack surface is critical to protecting operations from cyber attacks. As IoT & OT infrastructure continues to grow, achieving a modern, Zero Trust security posture is difficult to accomplish due to inherent device weaknesses. ZPE Systems helps you secure your distributed environments with the Nodegrid Mini SR.

To see how you can secure your IoT/OT devices, set up a personalized demo or POC at zpesystems.com/contact. We'll pair you with an engineer to walk you through the cloaking architecture, and show you how to defend against an attack by running security right on the box.

zpe