INVISINET
Where Zero Trust Begins

Securing Industrial Control Systems and Operational Technology

WHITEPAPER

INVISINET
Where Zero Trust Begins

Staggering Growth in Enterprise OT devices

OT devices are industrial control systems that are used to control, automate and monitor physical processes in industrial and commercial environments, such as manufacturing plants, power plants, healthcare and transportation systems.

Gartner predicts by 2025, **75%** of enterprise-generated data will be created and processed outside of traditional data centers and clouds, mostly at the edge of the network.

This means we will see a proliferation of unmanaged OT devices, such as industrial control systems, smart grid devices, and medical equipment that will generate and process large amounts of data.

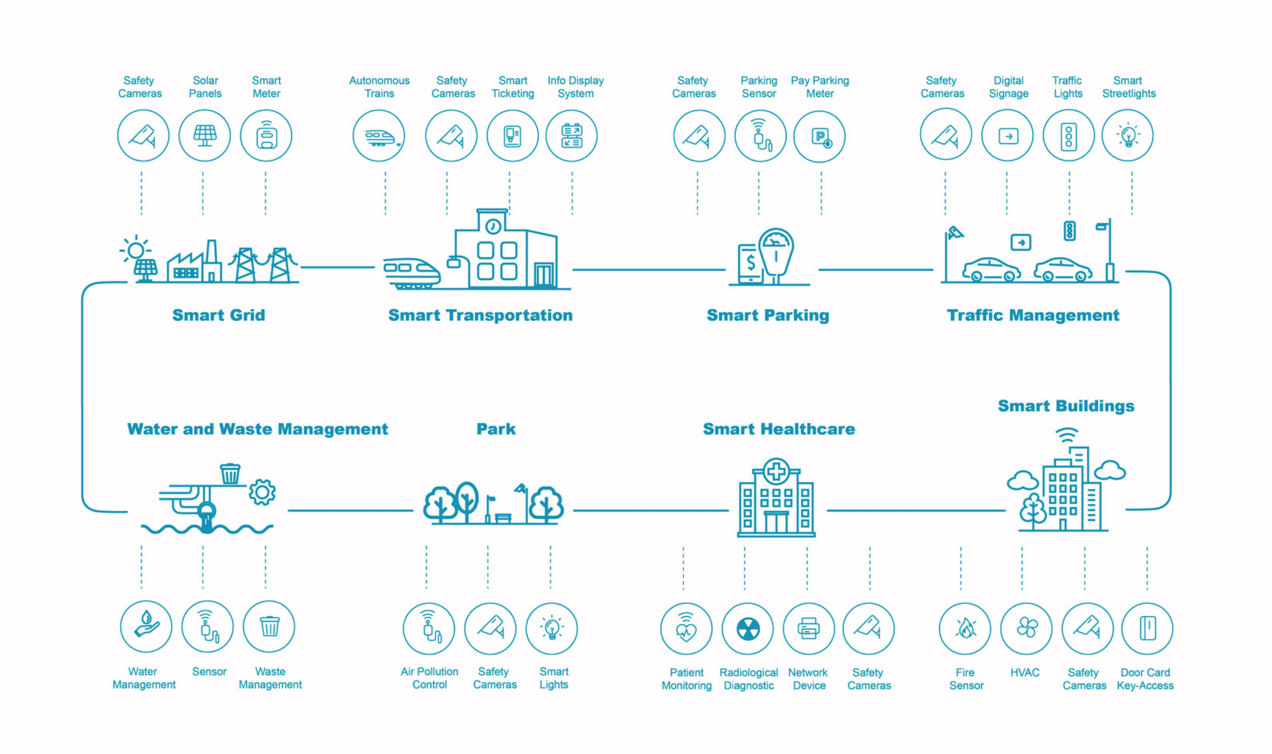

Fig 1

Security challenges with OT footprint

A Forrester study in 2019 highlighted that **66%** of manufacturers had encountered an IoT related security incident in the previous two years. In addition, **84%** of security decision makers were worried about external hackers and **80%** were concerned about viruses, network worms, and other malware threats.[1]

Manufacturers were nervous about attacks against OT environments which would lead to downtime, shutdown of critical services, disruption to business operations, and environmental risks, resulting in significant financial losses. The Mirai Botnet Attack in October 2016 was the largest DDoS attack in history. This attack left much of the east coast of the United States without internet. Attackers scanned the internet to open Telnet ports, and using default passwords, successfully compromised large swaths of CCTV cameras and routers which were then used as a botnet army. Since then, we have seen numerous other attacks where OT devices served as a gateway to access sensitive personal and financial information.

[1] https://www.armis.com/analyst-reports/2023-forrester-top-trends-in-operational-technology-security/

What Makes IoT Security Challenging?

1. IoT Devices Are Unmanaged and Unsecured

IoT device firmware is rarely updated after initial deployment. Updating these devices like a camera or an industrial sensor need physical access which is often restricted. The device owners may not be willing to update and fix a device that is functional. Obsolete operating systems and updated patches make these devices vulnerable to attacks which can be easily prevented on managed devices.

2. Weak Identity and Access Control Measures

The use of default passwords and a lack of strong authentication procedures makes compromising these devices much easier than a managed IT device.

3. Lack of Network Segmentation

Large scale industrial internet of things deployments doesn’t easily lend themselves to the level of network segmentation needed to mitigate cyber threats or prevent the spread of malware.

4. IoT Devices Become Easy Entry Points

IoT devices typically connect to an ecosystem that includes business applications, data centers, IT infrastructure, and the cloud. Because they lack strong cybersecurity controls by default, this makes them easy targets for hackers to use for entry into the rest of the network.

5. Inability to Install Agent-Based Security Software

Many IoT devices are incapable of hosting software security agents. They have limited processing and communication capabilities, in addition to not having “space” to install bulky software.

6. Rogue Deployment of IoT Devices

IoT devices are often deployed without the involvement of IT and/or cybersecurity teams. This can result in devices being in sensitive or insecure areas of the network, making them a much easier compromise because of the lack of additional cybersecurity layers.

Commonly used approaches for securing OT

The NIST Cybersecurity Framework (CSF) is a risk-based framework that helps organizations manage and protect their critical infrastructure and data.

Identify

Understand the types of IoT devices in use in your organization and their associated risks.

Protect

Implement appropriate security controls to protect your network from threats.

Detect

Implement monitoring and detection mechanisms to identify potential cybersecurity threats and vulnerabilities.

Respond

Develop and implement a plan for responding to cybersecurity incidents, finding and isolating affected devices, and communicating about the incident to relevant parties.

Recover

Plan and exercise business continuity strategies for recovering from cybersecurity incidents and restoring affected systems and processes.

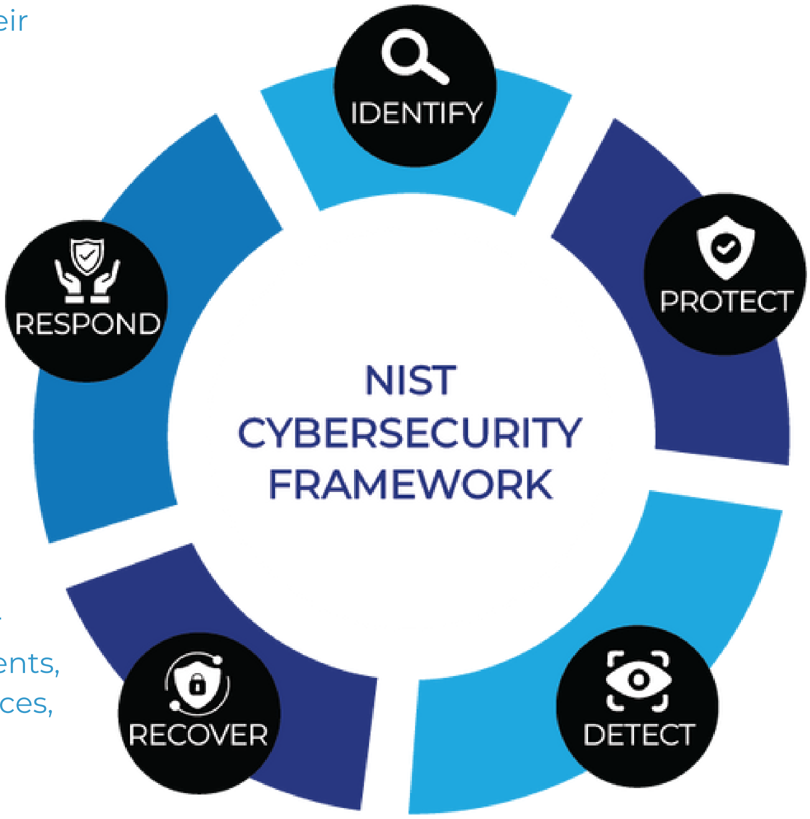

Fig 2: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1

https://doi.org/10.6028/NIST.CSWP.04162018

A Closer Look at the Alternatives to Protect

Let's look at common methods in use to improve security controls and to reduce attack risk in your OT environment.

ALTERNATIVES AVAILABLE TO PROTECT OT DEVICES	PROS	CONS	GAPS
VPN	• Encrypt data between OT device and server • Authenticate and authorize personnel to access OT devices • Enable secure remote access to allow authorized personnel to access and control the devices remotely	• Adds latency and impacts OT device performance • Complex configuration and maintenance of VPN for OT devices as they often have limited resources • A misconfigured VPN server can be a point of entry for attackers. • VPN compatibility across legacy and modern OT devices can be challenging	• Attacker needs to find only 1 weak / misconfigured/ unsecured OT device to access enterprise network
SECURE TUNNELS	• Same as VPN • Easy to use	• Same as VPN	• Incur excessive costs and further strain limited security resources to successfully secure a large OT footprint

FIREWALLS	• Controls network traffic to and from OT devices • Configured to enforce security rules like limiting certain types of traffic, blocking traffic from known malicious IP addresses etc. • Monitor & logging to identify security incidents • Scalable to manage growing number of OT devices	• Limited visibility into OT network traffic and may not detect some attacks or intrusions. • Misconfigurations can create unintended security gaps. • Can be very expensive	• Firewalls cannot be the only layer forsecuring OT devices - needs to be used in combination with other measures
INTRUSION DETECTION	• Detect cyber threats early with continuous network monitoring • Gain visibility into areas of vulnerability	• Can generate false positives • Complex setup and maintenance • Adds latency and impact OT device performance • Expensive	• Not suitable for use with OT devices with real time data processing function • Should be used in combination with other protection measures
ZERO TRUST	• Increased security with granular access to network resources • Flexible architecture • Identity-based authentication ensures only authorized personnel and devices can access OT devices. • Quickly detect andrespond to security incidents	• Complex with high resource and time consumption needed to implement. • Performance impact and latency issues • May create a frustrating user experience and reduce productivity with the needed user authentication and authorization.	• Complexity may deter enterprise-wide adoption especially for challenging OT environments - the weakest link in your enterprise network

INVISINET	• OT devices will remain invisible to unknown users. • Stops attackers at reconnaissance stage • Trusted users can authenticate and access OT devices safely	• User adoption & training	• Improve security posture for OT devices. Provide relief to over-burdened security teams by reducing your enterprise attack surface

INVISINET Transport Access Control

INVISINET Transport Access Control **(TAC)** mutually identifies and authenticates users and devices on the first packet receipt of a TCP/IP session. This First Packet Authentication (FPA) protects applications and network resources from unauthorized access by concealing network services from unidentified and unauthenticated users and devices. TAC can seamlessly augment other security solutions because of its integration at the TCP/IP layer. Authenticated access control provided by TAC is so complete that it even stops port scans and network reconnaissance, rendering protected resources invisible to attackers and intruders.

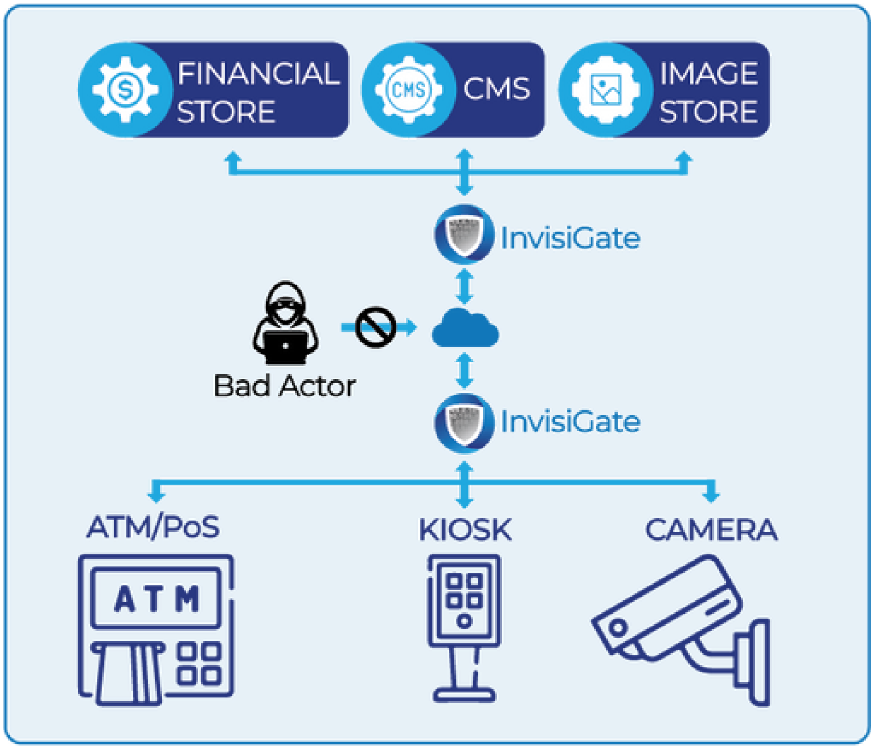

Fig 3: Invisinet TAC

Attackers cannot target and attack what they cannot see. Improve your OT security posture with INVISINET.

IOT SECURITY CHALLENGE	INVISINET SOLUTION	IMPACT
IoT Devices Are Typically Unmanaged and Insecure by Design	IOT devices will not acknowledge or respond to unknown users/ devices	Stops an attack before it can begin
Weak Identity and Access Control Measures	Enforce your IT/ Security approved user and authentication policies	Stops unauthorized and unknown access to OT devices and other critical infrastructure via a compromised OT device
Connected IoT Devices Become Easy Entry Points Measures	Block access to unknown users at the TCP layer itself.	Reduces your attack surface by improving your security controls for OT devices
Lack of Network Segmentation	Deploy a software-based approach to segmentation with identity-based access controls to block or allow network connections	Separates IT/ OT network segments without creating separate physical or logical networks
Inability to Install Agent-Based Security Software	Establish trust with a gateway device to insert identity-based access control	Works across legacy and modern OT devices using TCP/IP based connectivity
Rogue Deployment of IoT Devices	Augment needed security controls for rogue OT devices	Reduces attack risk and shrink enterprise attack surface

INVISINET's TAC technology was developed and deployed for protecting military assets from being discovered and attacked during active military operations. This technology is now available to efficiently secure enterprise OT, government networks, critical infrastructure, and to stay compliant.

Watch a live demo and meet our experts to learn how it can be used to secure your OT environment.

Watch Demo