Is IT Ready for OT and the Industrial Internet of Things (IIoT)?

We read a lot about the rampant growth of the Internet of Things (IoT) as everything from doorbells and TVs to cars and entire cities become smarter and more connected. We hear less about the fast-growing Industrial Internet of Things (IIoT), which is introducing a fresh batch of cybersecurity risks such as the Triton malware and Stuxnet virus.

The migration of unfamiliar, fundamentally different devices onto the data network instantly expands your attack surface. With deployments of IIoT set to skyrocket, experts are scrambling to extend cybersecurity infrastructures and give organizations full visibility to all industrial devices.

Your information technology (IT) and security teams need new strategies for securing the IIoT as quickly as possible. This paper looks at the trends, challenges, and key elements of a high-level strategy for gaining visibility and control.

Visibility Solution Highlights

- provides 100% visibility to defend IT, OT, and IoT
- addresses unique needs of oil and gas, utility, manufacturing, smart city, and maritime network infrastructures
- alerts users to anomalies indicative of malware, ransomware, and zero-day attacks
- provides a fully integrated solution that speeds response times and optimizes operations

KEYSIGHT TECHNOLOGIES

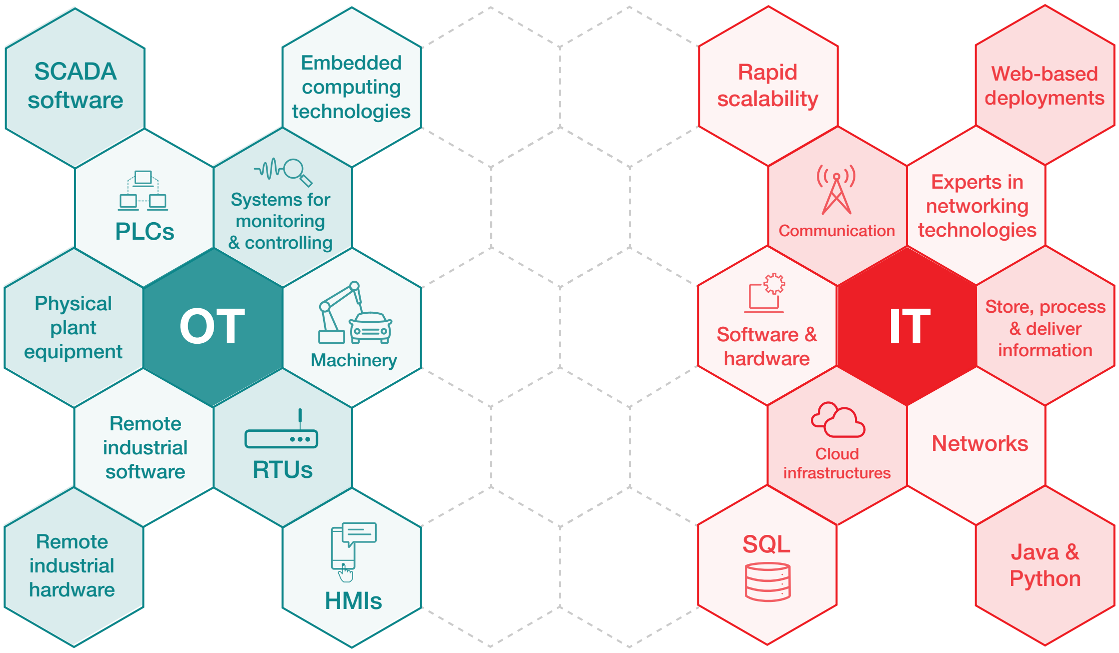
How Big Is IIoT?

The potential for attacks targeting nontraditional devices connected to the internet may be virtually limitless:

- The overall IIoT market could reach $124 billion in 2021 with a compound annual growth of 7.3% through 2020, according to *Forbes*.
- IIoT could have an additional $14.2 trillion impact on the global economy by 2030, Accenture predicts. [1]
- The three industries that analyst firm International Data Corp. predicts will spend the most on IoT in the near term are manufacturing ($189 billion), transportation ($85 billion), and utilities ($73 billion).

IIoT and operational technology (OT) networks span a broad swath of industry sectors and applications:

- industrial control systems (ICS) in which specialized monitoring devices control plants and machinery
- connected cities, including traffic management, water distribution, waste management, public safety, lighting, environmental monitoring, and parking systems
- utility systems and power substations that use remote terminal units (RTUs), compressors, and meters to generate, send, or meter power usage
- transportation hubs such as railway stations, airports, and seaports
- energy/oil and gas companies with ruggedized industrial probes and other devices deployed at remote or hard-to-access locations


SCADA software
Embedded computing technologies
PLCs
Systems for monitoring & controlling
Physical plant equipment
OT
Machinery
Remote industrial software
RTUs
Remote industrial hardware
HMIs
Rapid scalability
Web-based deployments
Communication
Experts in networking technologies
Software & hardware
IT
Store, process & deliver information
Cloud infrastructures
Networks
SQL
Java & Python

Source: i-scoop.eu

Figure 1. OT vs. IT

Why now?

Bringing transformers, valves, pumps, sensors, and other industrial devices online for the first time presents new opportunities to achieve savings and operational efficiencies by doing the following:

- adding predictive maintenance
- improving operating margin in highly competitive and price-sensitive industries — manufacturing, oil and gas, public utilities — with unprecedented performance and productivity
- enabling centralized troubleshooting without dispatching technicians to oil rigs and other remote locations
- delivering greater access to OT data that further reduces effort, cost, and time to market

At the same time, the greater interconnection between OT and IT networks confronts IT with formidable new challenges. Extending cybersecurity to include IIoT tops the list.

Highlights

Triton is malware first discovered at a Saudi Arabian petrochemical plant in 2017. It can disable safety instrumented systems, which can then contribute to a plant disaster. It has been called “the world’s most murderous malware.”

Stuxnet is a malicious computer worm, first uncovered in 2010, thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran.

How Great is the Risk?

Attacks on any or all sectors listed above could devastate individual businesses. But while attacks on manufacturing plants and other facilities might disrupt production and result in significant loss of revenues or reputation, attacks on critical infrastructure have the potential to compromise public safety and society as a whole.

Thousands of OT networks that used to be separate from traditional IT infrastructures now represent prime targets for criminals seeking to access privileged data or centralized resources. The crux of the problem is a lack of visibility from the security operations center that gives bad actors a formidable advantage.

The attacks against Ukraine's power grid in 2015 showed that the threat is real. And, more recently, a ransomware attack shut down a natural gas compressor station for two days, causing a "loss of productivity and revenue," according to an alert from the U.S. Cybersecurity and Infrastructure Security Agency. [2]

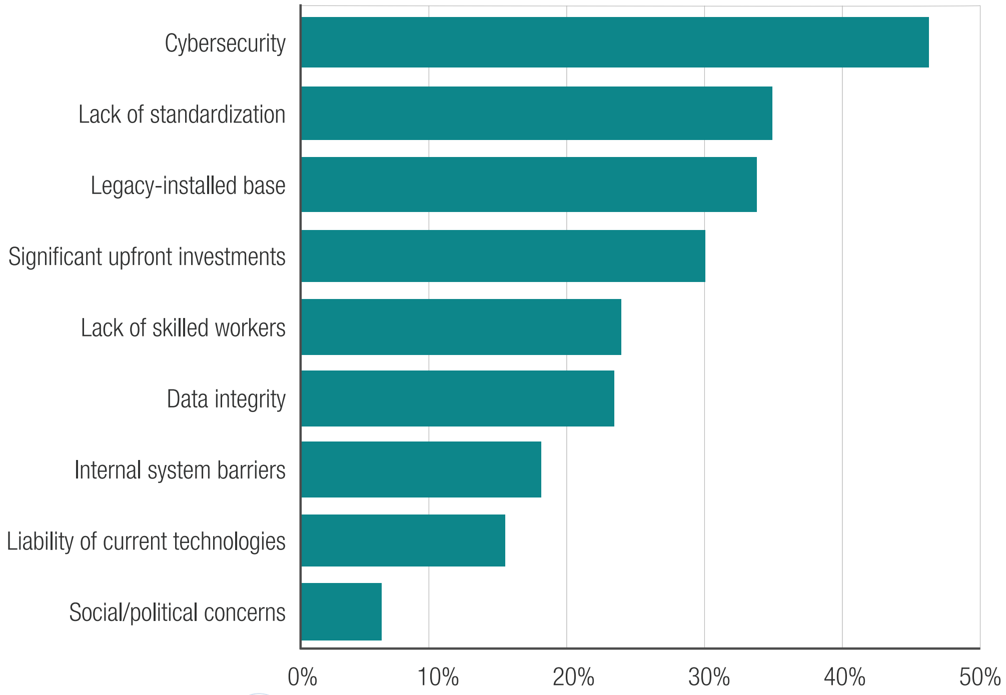
> "If IIoT products haven't received updates, or are still equipped with default passwords and login credentials, they provide attackers with an easy backdoor into networks that are already known to be lucrative targets when it comes to confidential data."
>
> -ZD.net

What causes the blind spots?

Many factors contribute to the risk:

- Remote locations often lack IT/cybersecurity expertise.
- Physical vulnerabilities, as noted above, exist. Hackers might have a field day with meters, sensors, and other structures left unlocked, unguarded, and in plain sight.
- Companies may display “cyber ignorance” of newly connected industrial devices that lack the cybersecurity safeguards built into IT or consumer devices. OT devices may be running older operating systems, Industrial Ethernet, or other specialized communications protocols such as Ruggedized that do not communicate with firewalls and other devices providing edge security and deep packet inspection (DPI). These devices cannot be patched to prevent new threats.
- Records of devices deployed over decades may be incomplete.
- The use of external service provider networks, managed network infrastructures, or the cloud requires extra steps to maintain integration, visibility, and control of OT and IT operations.
- High cost or shortage of resources and expertise may stand in the way of updating or revising processes.
- Use of external service provider networks, managed network infrastructures, or the cloud require extra steps to maintain integration, visibility, and control of OT and IT operations.

Challenges to IIoT adoption



Source: Morgan Stanley

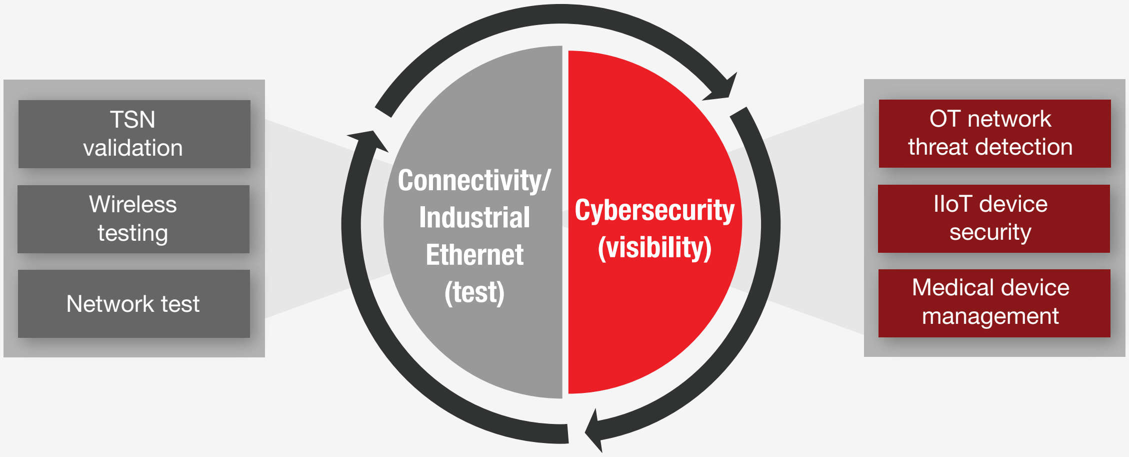
What Can You Do About It? Two Key Elements of IIoT Security

Efforts to streamline security operations should include all phases of networking — from planning and deployment through day-to-day operation. During the planning stages, activities center on testing and improving the ability of systems to communicate, interoperate, detect, and shut down threats. During operation, regular testing continues but complete visibility and as much automation as possible must augment the testing.

Strategy 1: Test and keep testing

Conduct testing at every stage — rollouts, migrations, upgrades, troubleshooting, expansion to new sites, and as you add new vendors and technologies to the mix. Keysight's network test and network visibility solutions offer industry-leading solutions for validating networks, devices, and security, providing the ultimate user experience.

Keysight ISG solutions for industrial IoT


TSN validation
Wireless testing
Network test
Connectivity/ Industrial Ethernet (test)
Cybersecurity (visibility)
OT network threat detection
IIoT device security
Medical device management

As with any network, again, testing should be continuous and combined with complete visibility.

Strategy 2: Extend visibility and monitoring across the hybrid IT/OT network

Keysight works closely with IIoT security innovation leaders such as Nozomi Networks, Darktrace, Zingbox, and Armis to deliver integrated visibility solutions for defending hybrid IT, OT, and IIoT infrastructures. Many ICS security partners solutions require actual data packets from the network, while other tools (for example, Indegy and Claroty) use a combination of passive packet data and active (nonpacket) data.

Passive monitoring at the IT/OT network edge discovers devices (using MAC addresses). Active techniques (polling, data logs, agents) probe the OT side to gather more detailed information about specialized OT protocols, proprietary ICS protocols, and other aspects unique to OT.

End-to-end visibility solutions must take in all necessary data sources and work with all types of monitoring tools to equip you to do the following:

- discover every dormant or active asset
- unearth malware and other threats
- achieve real-time threat detection and automated incident response across industrial environments
- model device behavior across geographically dispersed sites

OT network monitoring solutions should provide security teams with detailed cyber-risk assessments that highlight vulnerabilities and policy violations, and aid in forensics. These risk assessments include the following:

- asset discovery and detailed data about which ports are active, what software versions are running, and when updates occurred
- network traffic information about communication protocols, throughput, and latency
- DPI and threat and anomaly detection
- visualization of entire networks and all remote sites
- risk monitoring
- trend data

> “Continuous OT network monitoring has become an essential part of every industrial/OT cybersecurity strategy. It provides the asset and connectivity information users need to build strong defenses. It also alerts users when defenses may be breached.”
>
> -ARC Advisory Group [3]

How visibility works

In modern IT/OT operations, RTUs, PLCs, and ICS units deployed in the field send traffic to an operational technology control network (Levels 0 and 1 in the diagram below) comprising sensors that generate data about temperature, vibration, speed, composition, you name it. These sensors then forward traffic to a process network (Level 2 in the diagram below) to provide insight into the performance of each device for predictive maintenance.

Traffic then flows to the traditional IT infrastructure depicted in Levels 4 and above on the diagram below. At this point, network and security monitoring solutions featuring artificial intelligence, machine learning, and other emerging techniques help detect cyberthreats in real time.

Intelligent network visibility provides precisely the right data from hybrid networks for use in threat analysis and response. Keysight's Visibility Architecture includes all the necessary components.

Taps provide easy access

Intelligent network visibility starts with using physical and virtual taps, sometimes called "test access points," to capture and copy traffic from any IT or OT network — at each layer and every site. Compared with establishing data collection points from your network switches using SPAN ports to mirror data, taps offer an easier, safer, less costly alternative:

- Viability: OT devices typically connect to probes that do not perform switched port analyzer, or SPAN, functions.
- ROI: SPAN ports typically cost more than taps and may be scarce. Deploying taps at remote locations, on network links, and in the cloud also promotes full visibility while eliminating costly truck rolls.
- Scalability: You can add taps quickly as the network expands and easily manage them from a central location.

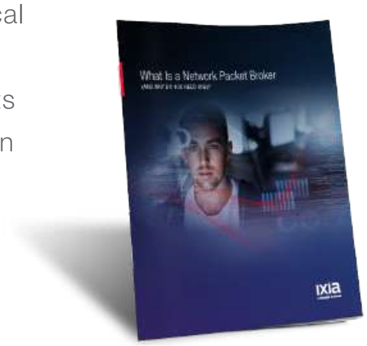
However, as networks scale, connecting every tap or SPAN port directly to monitoring and security tools (recorders, firewalls, forensics solutions) becomes unwieldy, if not logistically impossible. The Keysight Visibility Architecture overcomes this challenge by inserting Vision network packet brokers (NPBs) between taps and tools to add efficiency and scale and reduce cost and complexity.

Packet brokers save time and speed response

Securing networks amid relentless change requires real-time, proactive, and historical analysis. Most companies rely on a mix of network and application performance monitoring solutions to optimize performance and troubleshooting. Their counterparts on security teams use firewalls, intrusion prevention systems (IPS), data loss prevention (DLP), anti-malware, and other point solutions to find and shut down threats.

All of these specialized or high-end security and monitoring tools have three things in common:

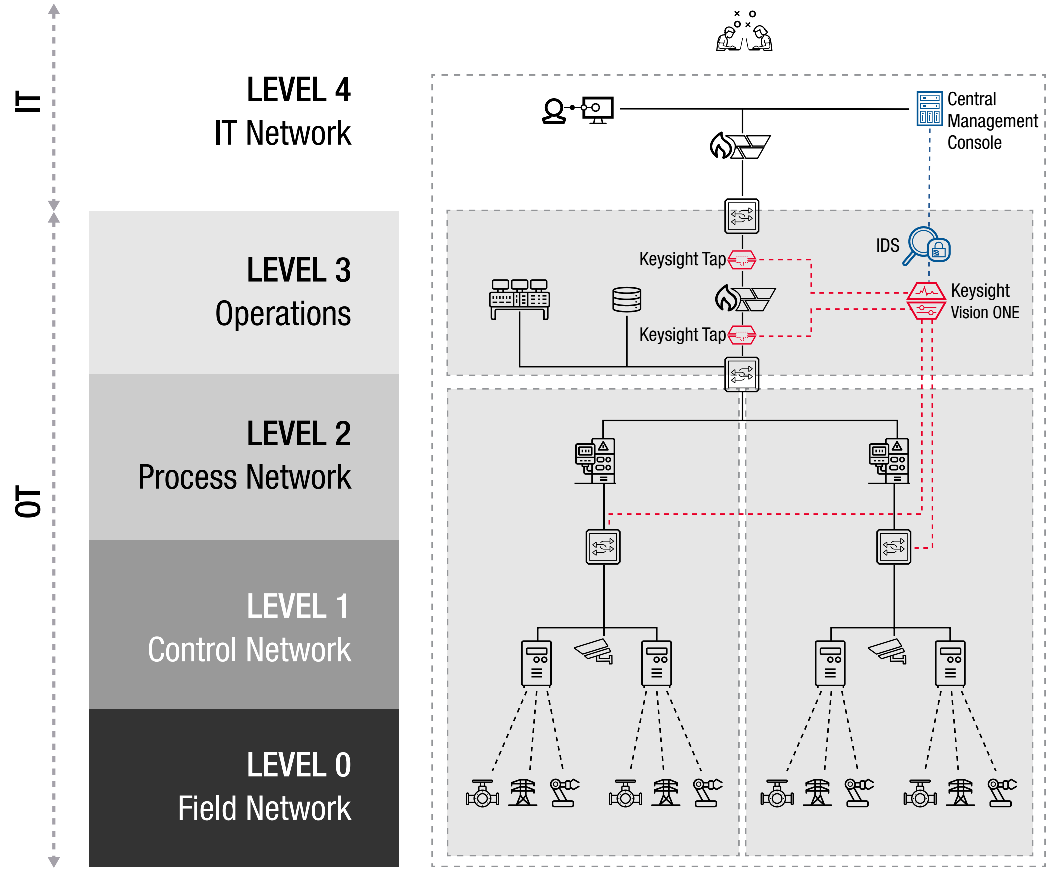
- They require specialized resources and expertise.
- They need to know exactly what is happening in the network.
- Their output is only as good as the data they receive to analyze.



What is a Packet Broker – and Why Do You Need One?

SCADA Level

ICS/OT Security Visibility Reference Architecture



Intelligent NPBs help you achieve all three. NPBs efficiently funnel the right data from the network to every analysis tool that needs it by adding an abstraction layer of intelligence between taps and tools.

NPBs remove duplicate packets, strip out unnecessary headers, mask privileged information so only the right tools can see it, and decrypt traffic once for use by a suite of security tools deployed inline. This pivotal preprocessing of traffic from IT and OT networks promotes the following:

- Better decisions based on better data: Advanced filtering capabilities serve to organize and streamline data for use by monitoring, performance, and security tools. NPBs can also aggregate multiple data streams such as data flows and network packets.
- Stronger security: Firewalls, IPSs, and other defenses see all relevant data, all the time.
- Faster problem resolution: "Problem identification is IT's biggest challenge," says Zeus Kerravala, principal analyst at ZK Research. NPBs automatically add context regarding the geographic location of outages, the root cause, and solutions presenting issues.
- Detailed context about applications, users, devices, operating systems, and location.
- Load balancing of traffic to extend the value of IT investments: For example, as you upgrade data center networks to 10 Gbps, 40 Gbps, or higher speeds, NPBs can downshift the flow of data to distribute the higher-speed traffic across a pool of lower-speed monitoring tools for analysis. Doing so allows you to avoid costly rip-and-replace upgrades.

Choosing the right packet broker

Three important characteristics distinguish high-performing NPBs:

- ease of use and streamlined single-pane-of-glass management
- 100% reliability — no packets dropped while running advanced features
- high-performance architecture combining hardware and software for advanced processing and speed

As the de facto standard visibility fabric for monitoring and security applications, Keysight taps and packet brokers deliver complete access and intelligence to save you time and money while averting danger.

> "Packet loss in a network visibility tool should be unacceptable. Visibility is supposed to enable clear insight into network data, not degrade the data that the analytics tools require."
>
> -Tolly

Act Now to Bridge the IoT/IIoT Gap

Until now, companies have primarily used data within OT networks for managing performance and improving uptime. They still do, but as communication between IT and OT networks grows, you can no longer ignore the risks inherent in these networks.

Organizations need to be thinking about establishing the proper visibility and building a sound, all-inclusive cybersecurity practice. In some cases, this means extending what the IT infrastructure already does. In other cases — and for those starting from scratch — it means designing visibility in from the very beginning.

The basic visibility challenge — providing each expert and analysis tool with precisely the right data – remains the same. And like traditional IT networks, industrial networks may be quite large and may change often with new devices — and threats — appearing anytime.

New visibility solutions must address both IT and OT, streamline deployment, and bridge gaps in processes and expertise. Keysight and its IIoT security partners work together to ensure your team of full visibility to all networking, security, and industrial systems.

Contact us to explore your unique security needs and begin devising cyber defense strategies that seamlessly integrate enterprise and industrial environments.

[1} Petrov, Christo. "40 Internet Of Things Statistics From 2020 To Justify The Rise Of IoT." Tech Jury. Last modified January 17, 2020. https://techjury.net/stats-about/internet-of-things-statistics/#gref.

[2] Walton, Robert. "Natural Gas Ransomware Attack Offers Critical Lessons for Electric Utilities, Analysts Say." Utility Dive. Last modified February 24, 2020. https://Utilitydive.com/news/natural-gas-ransomware-attack-offers-critical-lessons-for-electric-utilitie/572798/

[3] Snitkin, Sid. *Users Need Enhanced OT Network Monitoring*. ARC Advisory Group and Nozomi Networks, 2019. https://www.arcweb.com/blog/users-need-enhanced-ot-network-monitoring-capabilities-support-future-requirements.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at:
www.keysight.com/find/contactus

KEYSIGHT
TECHNOLOGIES