WHITEPAPER

ICS Visibility Guide

MANUFACTURING

How to Provide Secure Visibility to Mitigate Production Downtime and Risk

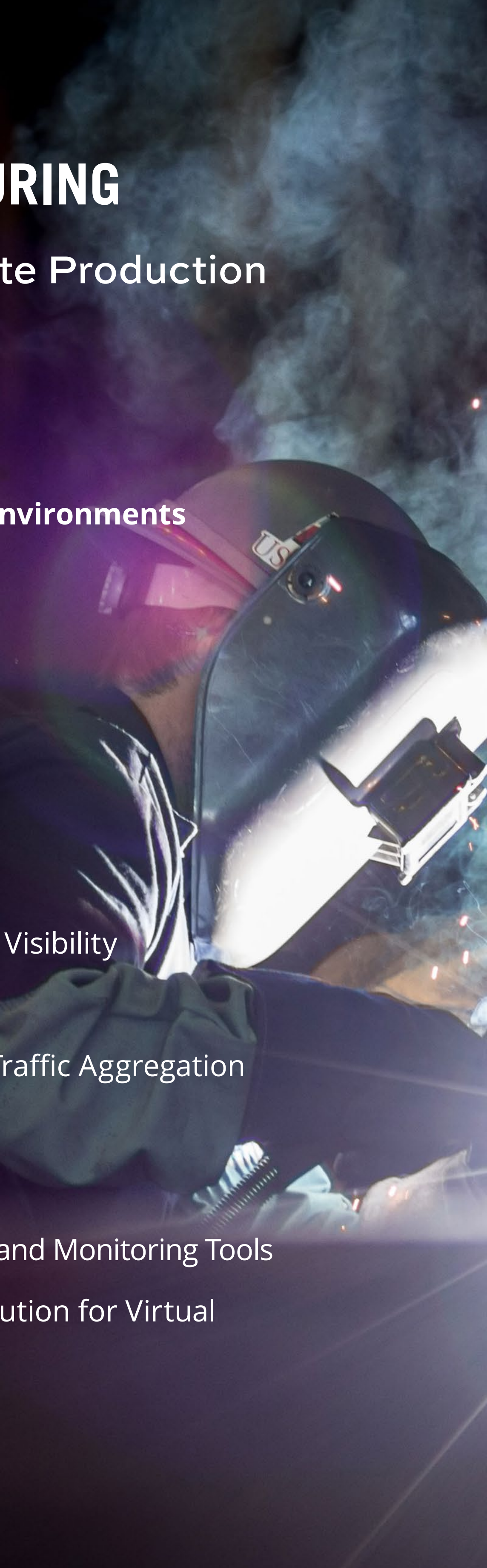
GARLAND TECHNOLOGY

See every bit, byte, and packet®

TABLE OF CONTENTS

ICS VISIBILITY GUIDE: MANUFACTURING

How to Provide Secure Visibility to Mitigate Production Downtime and Risk



INTRODUCTION

Today's critical infrastructure industries include the manufacturing and distribution of goods such as aerospace and defense, electronics, chemicals, pharmaceuticals, automobiles, food and beverages and more.

Manufacturing networks in operational technology (OT) environments utilize Industrial Control Systems (ICS), and the various other systems like supervisory control and data acquisitions (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLCs) typically found in the industrial sectors and critical infrastructures.

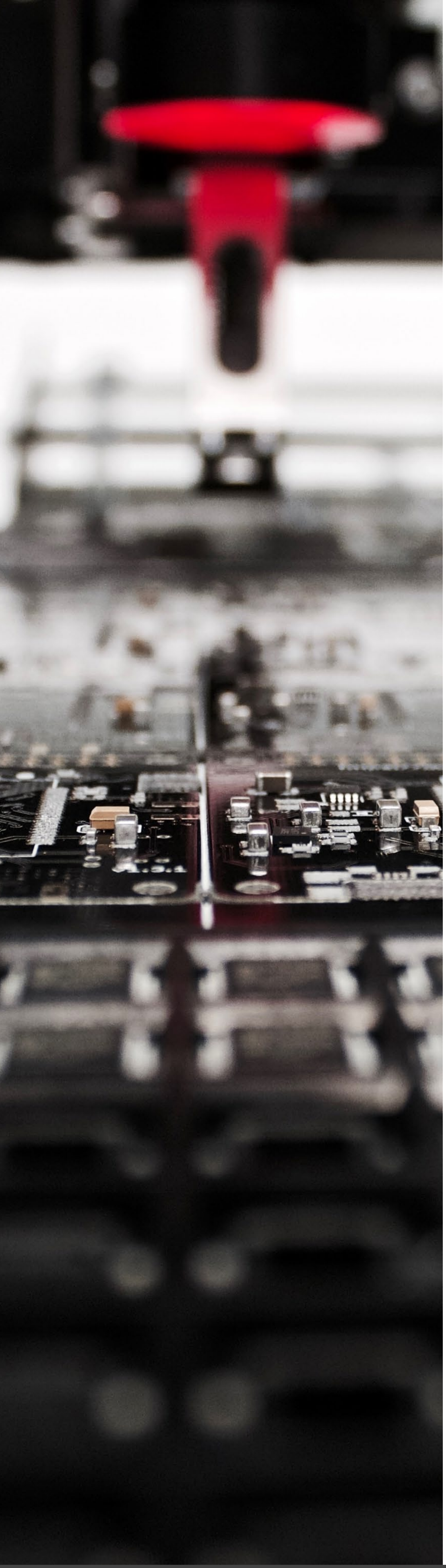
These manufacturing systems are categorized as either process-based or discrete-based (or a combination). Process-based manufacturing utilizes two main process types:

- Continuous Manufacturing are processes that run continuously, often in phases to make different grades of a product, and can be seen in steel and paper manufacturing plant, petroleum in a refinery, and distillation in a chemical plant.
- Batch Manufacturing are processes that have distinct steps, conducted on a quantity of material, and can be seen in food, beverage, and biotech manufacturing.

Discrete-based manufacturing typically performs a series of operations on a product to create the end product, and can be seen in electronic, machining and mechanical parts assembly.

Both process-based and discrete-based manufacturing utilize similar types of control systems, sensors, and networks. Some facilities are a hybrid of discrete and process-based manufacturing.[1] But the bottom line for all process based manufacturing is to mitigate production downtime and risk.

This guide is designed for ICS engineers to navigate network visibility options, best practices and use cases for deployments and upgrades.



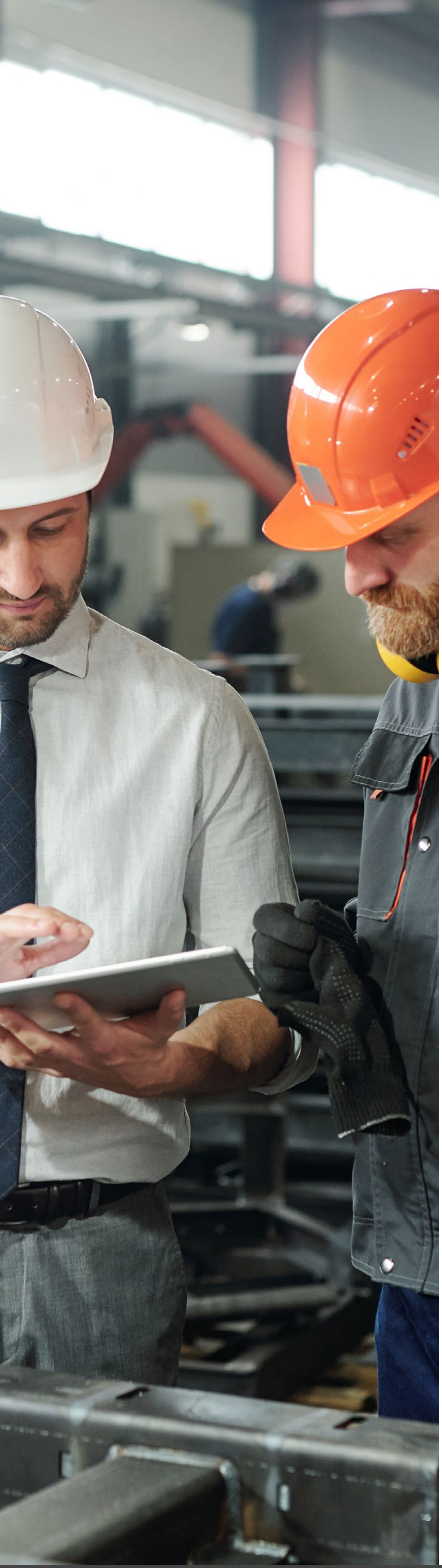
THE CONVERGENCE OF OT AND IT IN MANUFACTURING ENVIRONMENTS

For decades OT systems relied on processes, proprietary protocols and software that were manually managed and monitored. Being siloed from the world, these manufacturing systems were relatively insignificant targets for hackers, as they would have to physically breach the facility to access the terminals.

IT networks of course have been steadily growing in sophistication of computer systems, hardware, software, and networks related to the processing and distribution of data.

Fast forward to the 21st century and there is no question why digital transformation has been incorporated into these previously non-connected systems. This IT-OT convergence gives manufacturing organizations a complete view of both industrial systems and process management solutions, as well as the various industrial internet of things (IIoT) devices and the manufacturing equipment itself. All with the goal of better managing accurate information on users, machines, switches, sensors and devices in real-time.

Million Insights predicted[2] in a recent report that the value of the global IIoT market would reach US$922.62 billion by 2025, up from almost nothing 20 years ago, and this figure may prove to be overly conservative. The coronavirus (COVID-19) pandemic has given manufacturers new reasons to adopt connected systems by creating incentives for remote monitoring and control, and major technology providers such as Microsoft have responded[3] by expanding their involvement in IIoT solutions.



What's driving this expansion is evidence that connected monitors and sensors have the potential to save costs and add value to manufacturing in a variety of ways, including improvements in safety, predictive and preventative maintenance, more accurate tracking of personnel and inventory, and updating of legacy systems and equipment. According to a study published last year by McKinsey[4], IIoT applications have the potential to generate an additional US$1.2-3.7 trillion worth of economic value to manufacturers by 2025.

These connected systems bring risks as well as rewards. Every point of connection – every monitor, every sensor, every terminal, every remote access option, every patch installed on legacy devices, every link to corporate information technology (IT) systems, every server set up to run the system – has some degree of vulnerability to cyberattacks.

Manufacturers must work to minimize this risk. If they don't, they could fall victim to malware or ransomware attacks, which cause business continuity to be lost, production interrupted, equipment damaged, and/or raw materials wasted, resulting in billions of dollars in losses and clean-up costs.

They could also leave themselves open to corporate espionage incidents involving the loss of intellectual property, trade secrets, and/or proprietary formulas, designs, and processes via connected devices – and this isn't just a theoretical risk. Verizon's Cyber-Espionage Report[5], published last November, concluded that attacks on manufacturers account for 22% of all cyberespionage incidents, second only to the public sector at 31%.

Unfortunately, the Industrial IoT digital transformation leaves the OT infrastructure side vulnerable, as they tend to be poorly protected against cyber attacks, and most ICS being used today were developed decades ago. Companies are left to face several OT / IT challenges:

- Many IT security solutions are ill-adapted to protect legacy control systems like SCADA
- How to secure emerging technologies, such as cloud computing and the internet of things (IoT)
- The growing likelihood of malware and ransomware attacks
- Proliferation of unsecured shadow OT devices that are running in the background

CYBERSECURITY THREATS FOR MANUFACTURING

As companies evolve with the Industry 4.0 digital transformation, manufacturers need to invest in cybersecurity to mitigate the threats and risks that come along with it.

Small and medium size manufacturers are considered bigger targets for cyber attacks because they often have more to lose than larger manufacturers. These manufacturers are often seen as an easy entry point into larger businesses and government agencies.

Manufactures offer a larger attack surface. With the many benefits digitalization brings an organization, there are more connections and entry points through which hackers can gain access to your production network.

Pharmaceutical and chemical companies are a recent focus of Ransomware attacks aimed at disrupting production. Disruption for these manufacturers results in downtime, production disruption and lost revenue. Because these risks can have large-scale environmental impact and safety concerns, these organizations typically standardize critical processes to ensure the strict adherence to quality standards.

5 STEP CYBERSECURITY FRAMEWORK

To help manufactures develop modern security strategies to combat these threats, both CISA[6] and NIST[7] encourage a 5 step Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.

1 - Identify

Identify physical and software assets within the organization to establish the basis of an Asset Management program, as well as identifying the business environment the organization supports including their role in the supply chain, and the organization's place in the critical infrastructure sector.

2 - Protect

The ability to limit or contain the impact of a potential cybersecurity event to ensure delivery of critical infrastructure services, including protections for Identity Management and Access Control within the organization including physical and remote access.

3 - Detect

The ability to identify the occurrence of cybersecurity anomalies and events, and what their potential impact is.

4 - Respond

The ability to take action on a detected cybersecurity incident, with capabilities to contain the impact of a potential cybersecurity incident.

5 - Recover

Maintaining plans for resilience and restoring any capabilities or services that were impaired due to a cybersecurity incident, supporting timely recovery to normal operations to reduce the impact from a cybersecurity incident.

ICS SECURITY SOLUTIONS FOR MANUFACTURING

ICS security solutions are designed to resolve these network and security challenges. Also, ICS security solutions allow you to manage these threats efficiently so you can properly detect, respond, and recover from threats and breaches. Most ICS security solutions focus on visibility, threat detection, compliance, and asset management to help manufacturers gain full visibility and practice risk management in their OT networks while incorporating Industrial IoT technologies.

THREAT AND NETWORK VISIBILITY

One fundamental ICS security best practice is having real-time visibility into cyber attacks, risks, and incidents. This focuses on having proper access to all traffic flowing through the network and those analytics to identify assets, network communications, and activities, including protocols and equipment status. The goal is to know what is on your network, and who is on your network.

OT & IOT ASSET DISCOVERY AND MANAGEMENT

Part of having complete visibility is extending security and monitoring across all your assets. With manufacturing companies, this includes large attack surfaces, with a very complex network of devices and equipment. Accurately identifying and managing all assets in OT & IoT environments are critical. Today's solutions provide asset discovery and network visualization to monitor these devices and the activities, including firmware updates and availability.

THREAT DETECTION AND MONITORING

Imperative to modern ICS security strategies is threat detection, also known as an intrusion detection system (IDS), with the goal to identify cyber threats, risks, and anomalies providing the ability to quickly respond and reduce mean-time-to-detection (MTTD).

Threat detection takes the network visibility (packet data and devices) and provides complete IT-OT monitoring, essential to preserving the availability, integrity, and safety of manufacturing operations. Most threat detection and monitoring solutions incorporate the MITRE ATT&CK Framework8 and ICS Matrix, which is an overview and database of tactics and techniques that threat actors have used while carrying out attacks against industrial control system networks.

ICS VISIBILITY CHALLENGES WITHIN OT ENVIRONMENTS

Securing and monitoring your network is the ultimate goal. But OT teams face complex challenges when it comes to architecting connectivity throughout these large and sometimes aging infrastructures that weren't initially designed with network security in mind. These challenges include:

- Relying on legacy switch SPAN ports for visibility, that aren't secure, reliable, or available
- Face different media or speed connections between the network and various tools
- Network sprawl with a need to reduce network complexity
- Require unidirectional connectivity for their monitoring tools
- Require a secure air-gapped solution for virtual environments

Fortunately, these challenges have solutions. Optimized security and performance strategies start with 100% visibility into network traffic. And visibility starts with the packet.

A common access point for network visibility in OT environments has been from SPAN ports on a network switch, many times engineers will connect directly to intrusion detection systems (IDS), or network monitoring tools.

But now there are two options to access network packets for security and monitoring solutions to properly analyze threats and anomalies, as well as performances and regulatory conditions — network TAPs and SPAN ports. We'll review these two options in-depth in the next section.

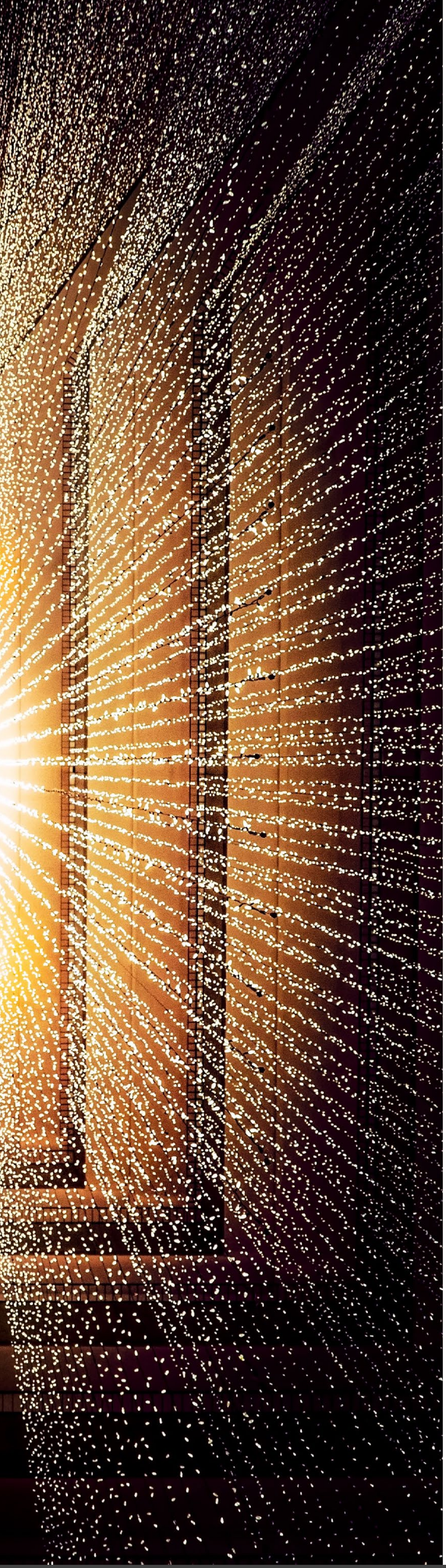
LEGACY NETWORKS & SWITCHES

Legacy OT networks pioneered the concept of redundancy. Born out of the necessity that these critical infrastructure network's cannot go down, redundant network segments were designed to last decades and provide production and infrastructure maintenance windows to address any issues or upgrades.

Even with redundancy in many OT environments, the fact remains that aging technology is a constant challenge for many legacy networks:

- Many networks are still running at either 10M or 100M with 100BaseFX or 100BaseTX cabling
- Many networks run older operating systems such as Windows 95 and Windows XP due to security concerns, even after the legacy operating systems are no longer supported
- Adhering to static production traffic regulations. Many changes to the machine environment require recertification and calibration

Large legacy switch providers have been the bedrock for OT network infrastructure for decades. As these environments were built to last for a long time, 20+ years, it makes sense that these switches are still in use. Many legacy switches use very little data, typically 10M, 100M, up to 1G.



Connectivity Challenges in OT Environments

When bridging the gap between legacy infrastructure and modern security solutions, engineers run into two connectivity challenges:

- Speed variations - Need to connect tools with a different speed than the live network
- Media incompatibility - Need to connect tools with different media connections than network appliances

Most security solutions may not support legacy 1Gbps OM1, 100Base-FX fiber or 10/100M copper connections. How do you connect a security platform, utilizing 1Gbps copper links to enable faster detection and response to ICS/SCADA risk?

Achieving Unidirectional Data Compliance

Some manufacturing environments face challenges to protect network segments from incoming threats through the network infrastructure designed to protect them. These situations require a one-way data transfer between segments or facilities. Unidirectional or one-way data flow is designed to secure OT network from external threats and maintained business continuity, adhering to NIST cybersecurity compliances.

- NERC CIP v5 regulations[9]
- NRC guidelines

This is achieved by using data diode devices that eliminate inbound data flow and ultimately threats to OT networks, while providing the outbound data flow needed.

Implementing Air Gap Networks

As OT systems and infrastructure are being connected to corporate IT environments, such as cloud computing, big data analytics, artificial intelligence (AI), and the internet of things (IoT). With the benefit of added efficiency and compute power comes added security vulnerabilities and widening threat vectors.

One way to bridge the OT and IT convergence is implementing an air gapped network where needed. This security measure physically isolates a secure network or appliance from unsecured networks, such as the public Internet or an unsecured local area network. This ensures the network has no network interfaces connected to other networks, ultimately providing the benefits of digital transformation while reducing the security threats connectivity brings.

ICS VISIBILITY BEST PRACTICES

Security Solutions Need Visibility. “You cannot secure what you cannot see.” This is a common mantra in security circles because:

- Security solutions are only as good as the data they analyze
- Blindspots hide threats and anomalies

It’s a fundamental best practice in OT security to have a system inventory of all the networked devices and ICS being monitored so that users can determine what facilities are connected to their networks and who is active on their networks.

The goal of network, security, compliance and application managers require full visualization of the network and the packets therein. Real visualization is everything. If you cannot see an issue, like an attack, misusage, inefficiency, how are you going to understand it and resolve it?

It’s this reason most modern ICS strategies incorporate a visibility fabric.

For security threat detection or monitoring tools — providing a cohesive visibility fabric of network TAPs and packet brokers, improves the tool performance tasked with solving various security strategies.

When you implement a visibility infrastructure within an OT environment, you’re able to:

Maintain uptime: Ensure minimal network downtime for deployment and upgrade windows, and guarding against unintentional downtime due to a breach or outage

Improve Risk Assessment: Being able to guarantee total visibility into your network traffic and data flows makes it easier to spot vulnerabilities and manage changes to the protect surface

Reduce Network Complexity: Network TAPs and NPBs make it easier to maximize tool utilization through traffic aggregation load balancing, packet filtering, and other features. These features minimize the number of tools you need to deploy to maximize visibility, reducing complexity in sprawling OT environments

Streamline Infrastructure Upgrades: A visibility layer creates more access points to your network and an ability to implement inline or out-of-band security and monitoring tools. Instead of taking the network down for extended periods of time to upgrade infrastructure components, you can maintain data flows while making changes to the architecture

Better Tool Performance: The only way for your security and monitoring tools to deliver the best results is for them to see every necessary packet of traffic. Your network visibility layer ensures each tool is fed with every bit of data it needs

Reduce Compliance Violations: When your monitoring and security tools can see all data packets, you can stay ahead of problems that would otherwise build until the network becomes out of compliance

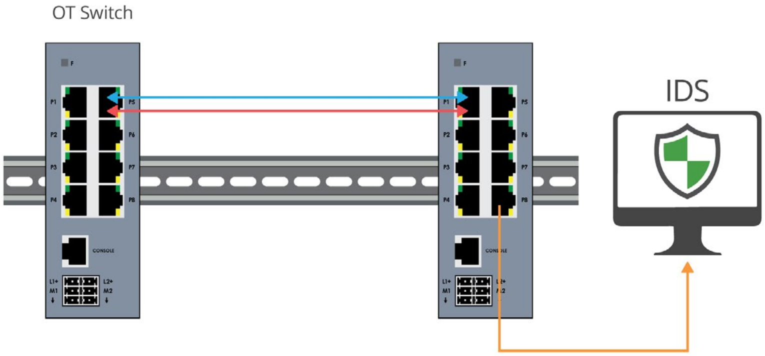
TAP VS SPAN IN OT ENVIRONMENTS

Determining where you use SPAN ports or network TAPs comes down to a multitude of issues. And many times a combination of both is a visibility architecture reality. But there are some significant differences which affect the integrity of the traffic that is being analyzed, as well as the performance of the network traffic. Let's review some of the pros and cons of each to help you decide what works best for your network.

Switch SPAN ports

A common visibility use case is to route mirrored traffic from a SPAN port on the switch to a security or monitoring tool. Port mirroring also known as SPAN (Switch Port Analyzer), is a designated port on a network switch that is programmed to mirror, or send a copy, of network packets seen on a specific port (or an entire VLAN), where the packets can be analyzed.

- Provides access to packets for monitoring
- SPAN sessions do not interfere with the normal operation of the switch
- Configurable from any system connected to the switch



The concept is simple enough — the switch is already architected into the environment. Just hook up your security solution. Done. But many times the simplest path isn't the best path.

High-level SPAN challenges include:

- SPAN takes up high value ports on the switch
- Some legacy switches do not have SPAN ports even available
- SPAN ports can drop packets, an additional risk for security and regulation solutions

One of the fundamental reasons security teams do not like to use SPAN is because of dropped packets. This usually happens when the port is heavily utilized or oversubscribed. In OT environments, network switches tend to run 10M, 100M, up to 1G so you may think this may not happen. Unfortunately, ICS switches are prone to drop packets at a lower level, even when network links are not saturated. This can happen for a variety of reasons:

- Packets sometimes can't be stored because of a memory shortage
- 'PAUSE' frame attack. A bad actor can flood the SPAN disguised as a loopback, hiding bad data and forcing dropped packets
- Packets showing a broken CRC will be dropped
- Frames smaller than 64 bytes or bigger than the configured MTU can be dropped because of an ingress rate limit

If dropping the packets isn't an eye opener, did you know SPAN:

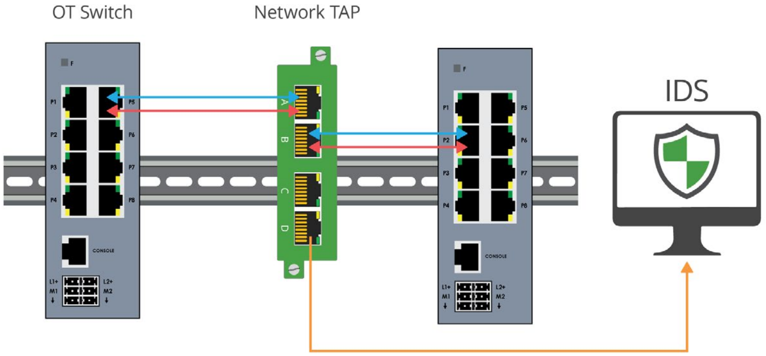
- Will not pass corrupt packets or errors
- Can duplicate packets if multiple VLANs are used
- Can change the timing of the frame interactions, altering response times

The SPAN concept may have sounded easy because it was available, but after weighing packet loss and altered frames, additional SPAN security considerations include:

- Bidirectional traffic opens back flow of traffic into the network, making switch susceptible to hacking
- Administration/programming costs for SPAN gets progressively more time intensive and costly

Network TAPs

The industry best practice for packet visibility are network TAPs (test access points). Network TAPs are purpose-built hardware devices that create an exact full duplex copy of the traffic flow, continuously, 24/7 without compromising network integrity. Instead of connecting two network segments, such as routers and switches, directly to each other, the network TAP is placed between them to gain complete access to traffic streams. TAPs transmit both the send and receive data streams simultaneously on separate dedicated channels, ensuring all data arrives at the monitoring or security device in real time.



- Network TAPs make a 100% full duplex copy of network traffic
- Network TAPs do not altering the data or dropping packets
- Network TAPs are scalable and can either provide a single copy, multiple copies (regeneration), or consolidate traffic (aggregation) to maximize the production of your monitoring tools

TAPs VS SPAN

TAPs

- 100% full duplex copies of network traffic
- Enables faster troubleshooting
- Ensures no dropped packets, passing physical errors and supports jumbo frames
- Does not alter the time relationships of frames
- Passive or failsafe, ensuring no single point of failure (SPOF)
- TAPs are secure, do not have an IP address or MAC address, and cannot be hacked.
- CALEA (Commission on Accreditation for Law Enforcement Agencies) approved for lawful intercept, providing forensically sound data, ensuring 100% accurate data captured with time reference
- Data Diode TAPs provide unidirectional traffic to protect against back flow of traffic into the network
- Scaleable for traffic optimization and can aggregate multiple links down to one
- Plug and play; easy configure and deploy

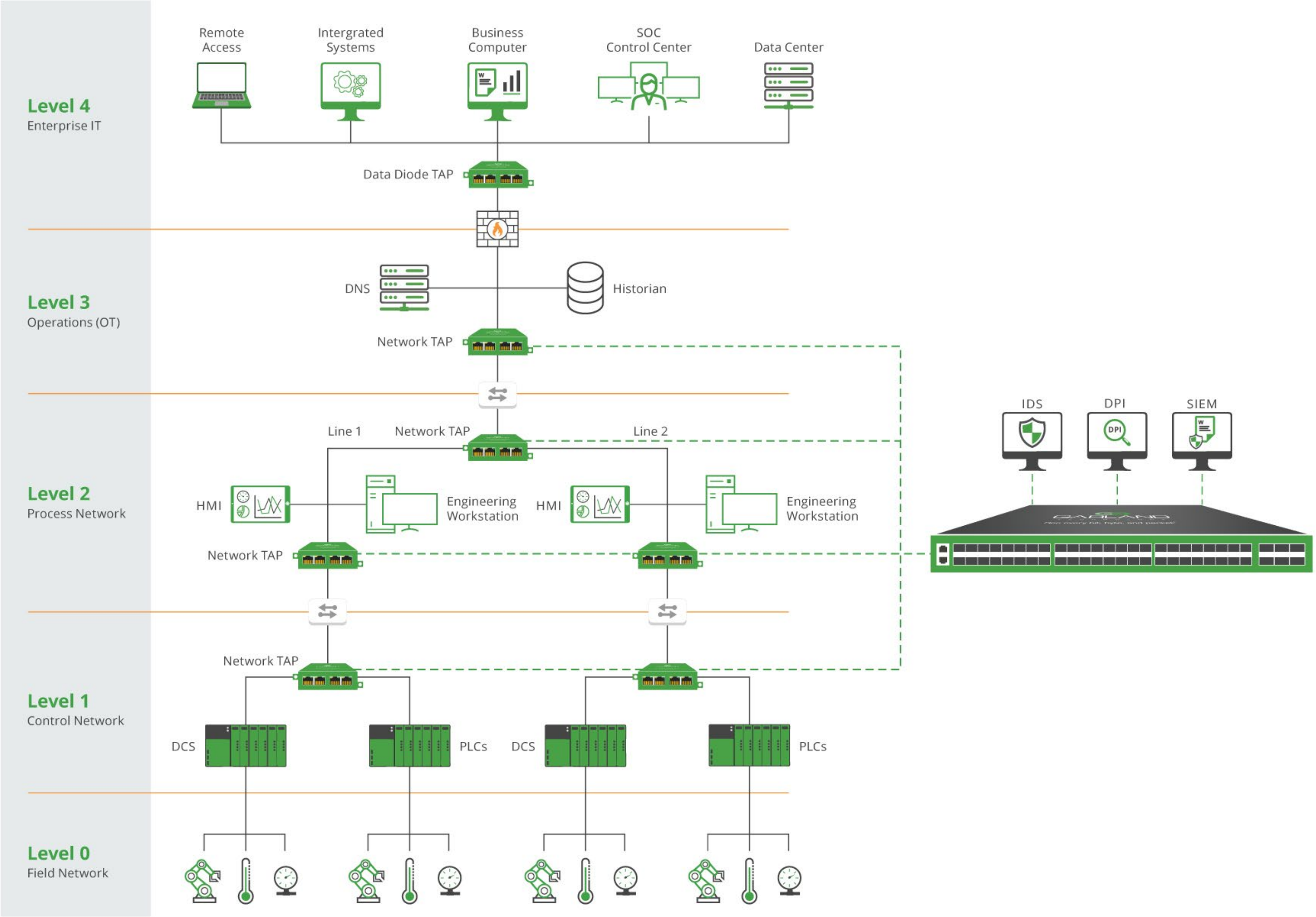
SPAN

- Provides access to packets for monitoring
- Can take up high value ports on the switch
- SPAN traffic is the lowest priority on the switch
- Some legacy switches do not have SPAN available
- SPAN ports drop packets, an additional risk for security and regulation solutions
- Will not pass corrupt packets or errors
- Can duplicate packets if multiple VLANs are used
- Can change the timing of the frame interactions, altering response times
- Bidirectional traffic opens back flow of traffic into the network, making switch susceptible to hacking
- Administration/programming costs for SPAN can get progressively more time intensive and costly

Following critical infrastructure's guiding principles — you want your network to be built to last, while ensuring minimal to no network downtime. These concepts rest on the network infrastructure and visibility architecture. Being built by incorporating best practices are what's going to help you achieve these goals.

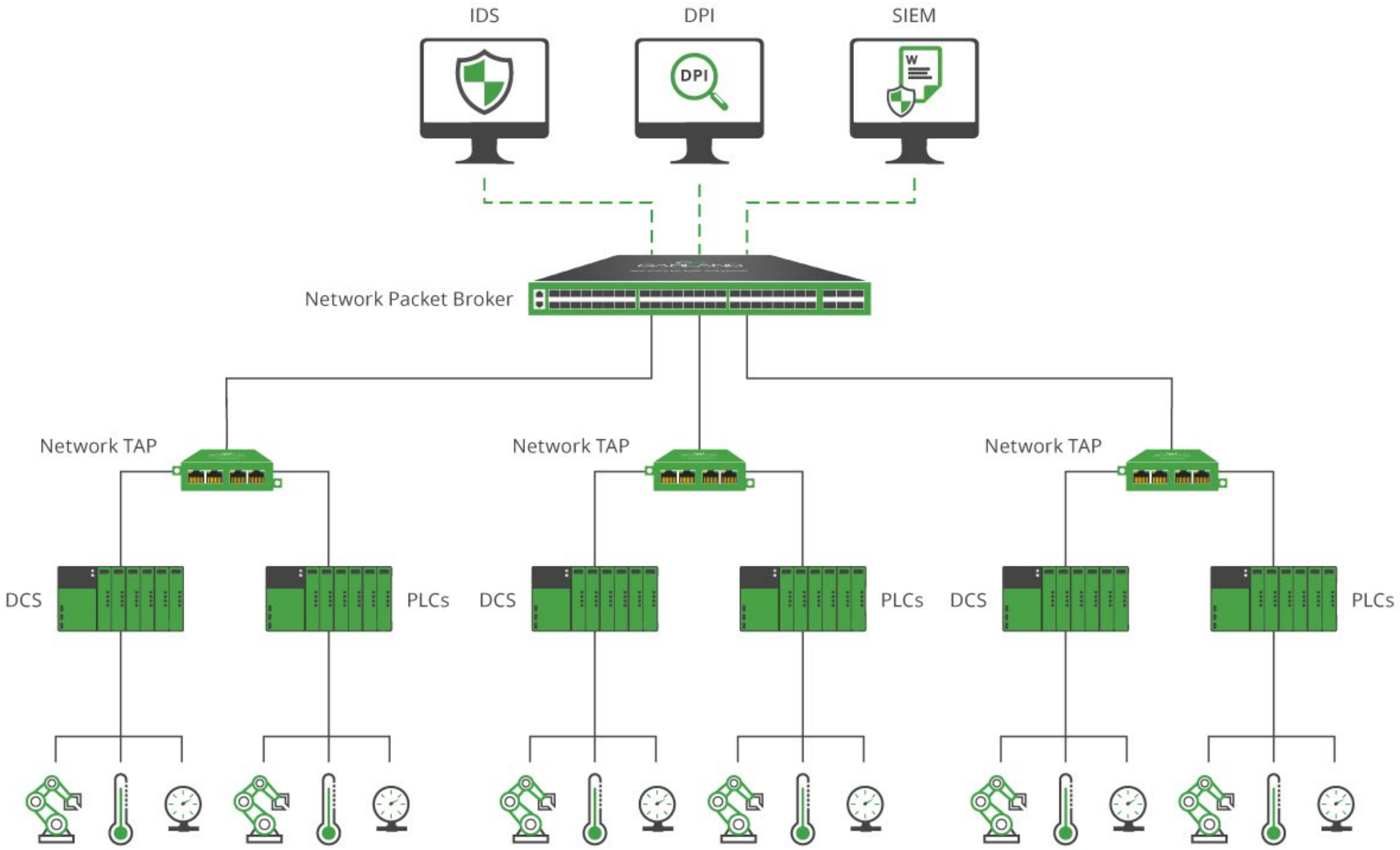
ICS VISIBILITY SOLUTIONS

Today's ICS network requirements for security, monitoring, management, compliance and auditing of your manufacturing network requires real-time access to the packets that flow through our network.



In this high level network diagram, manufacturing companies properly access ICS visibility with network TAP technology, the most viable and reliable technology for that job, as SPAN ports expose many challenges and added security risks.

For larger deployments that have many network TAP and SPAN connections, adding network packet brokers offers a scalable visibility solution with advanced aggregation, filtering and load balancing, that will streamline traffic flow, reduce network complexity and improve security and monitoring tool performance.



Utilizing network TAPs and packet brokers within ICS architecture also solves many of the visibility challenges engineers face, including:

- Providing ICS Security tools 100% packet visibility
- Eliminating Blind Spots
- Improving Tool Performance
- Reducing network complexity through traffic aggregation
- Ensuring unidirectional connectivity
- Providing a secure air gap solution for virtual environments

Let’s review the various visibility use cases.

HOW TO PROVIDE ICS SECURITY TOOLS 100% PACKET VISIBILITY

Many times, ICS teams run into challenges when hooking up packet visibility to their security solutions. Chances are your IDS security or your assets management tools must rely on eliminating blind spots before they become an issue. And it is critical to optimize the investment on security, monitoring and compliance tools to work as needed.

1 - Eliminate Blind Spots

"Blind spots" refer to the inability to analyze the data between certain segments in a network, that may seem "hidden" to your monitoring tool and can compromise network performance and security. These blind spots happen for a variety of reasons, including:

- There has been an addition of new network tools, equipment or applications. The additions haven't been properly architected for visibility, or the security tools are not accessing the packets needed in the segment.
- SPAN ports present a host of opportunities for blind spots – SPAN port contention issues, dropping packets and creating a loss of information, improper SPAN port programming – all resulting in incorrect or missing data captures.

2 - Improve Tool Performance and Efficiency

Network security tools need packet data to properly analyze and detect any threats. Teams are typically tasked with getting more out of their existing tool investments, which becomes challenging with growing traffic volumes and legacy architecture.

- Network and security tools can themselves be oversubscribed.
- Traffic growth outpaces existing tool capacity leading to reduced throughput and effectiveness.
- Dropped packets present an additional risk for security and regulation solutions, as not getting a complete picture of the packet data.

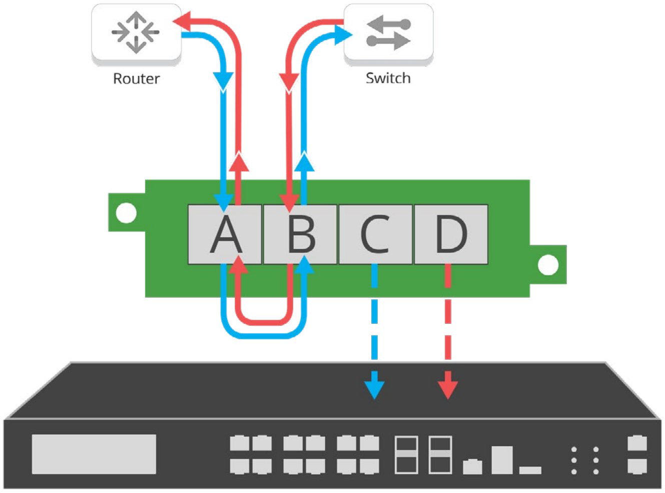
SOLUTION

NETWORK TAPS GUARANTEE TOOLS COMPLETE PACKET DATA VISIBILITY

Network TAPs, an industry best practice over SPAN ports, provide the ability to capture network monitoring data without compromising the network, removing blind spots.

ICS teams use Network TAPs to easily monitor all network data. A network TAP is a purpose-built hardware device that are typically placed between network devices like switches and routers, creating an exact copy of both sides of the traffic flow, continuously 24/7/365. The duplicate copies can be used for monitoring, security, and analysis, while the network flow continues uninterrupted. TAPs do not introduce delay, or alter the data. They are either passive or "failsafe," meaning traffic continues to flow between network devices if power is lost or a monitoring tool is removed, ensuring it isn't a single point of failure.

TAPs enhance tool performance by ensuring no dropped packets if oversubscribed and no duplicate packets or altered frames. Network TAPs provide 100% full duplex copies of the traffic you are analyzing. Better data provides better tool performance and added value.



Recommended Products

Copper Network TAP

10M/100M/1000M (1G) | Portable | Breakout

Model # P1GCCB

Copper OT Network TAP

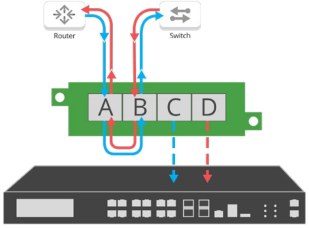
10/100/1000M (1G) | Portable

Breakout | Fixed DC power

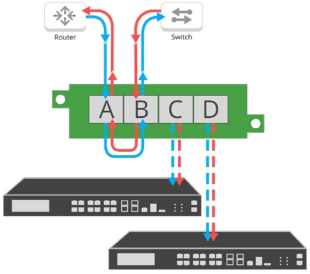
Engineered for temperature

variations -40C to +85C / -40F to +185F

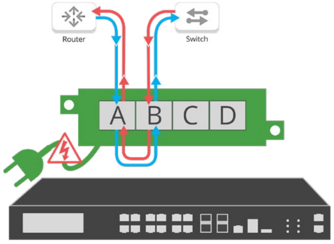
Model # P1GCCB_OT



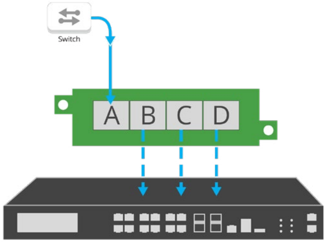
TAP 'Breakout' Mode



Aggregation Mode



Failsafe



Regeneration / SPAN mode

HOW TO UTILIZE MEDIA AND SPEED CONVERSION

Teams facing connectivity challenges in OT Environments when bridging the gap between legacy infrastructure and modern security solutions, sometimes include needing to connect tools with a different speed or media types than the live network.

What do you do if your network analyzer or IDS runs copper gigabit, and you need to connect a 100Base-FX link? There are no 100Base-FX NIC cards for your security or performance monitoring device.

SOLUTION

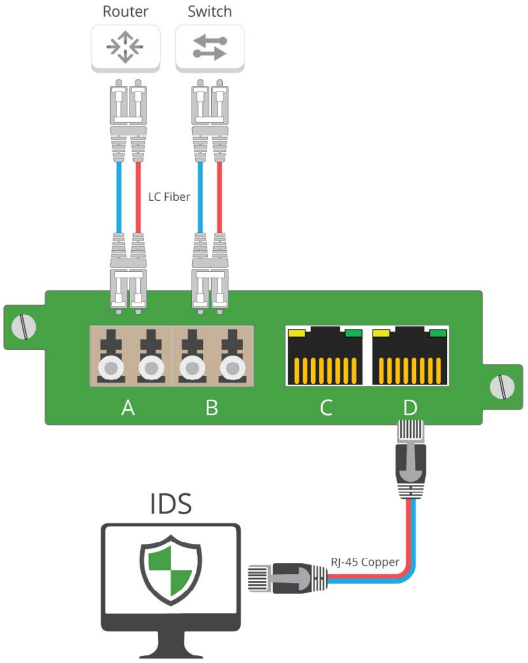
NETWORK TAPS PROVIDE VARIOUS MEDIA CONVERSIONS OPTIONS

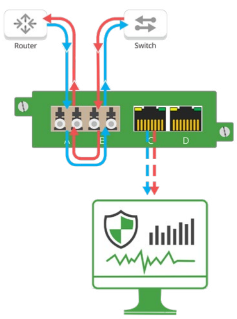
Not only do network TAPs bridge the gap between various media types, solving connectivity issues without having to upgrade existing infrastructure. But network TAPs provide one thing other media converters do not: complete packet data, ensuring security platforms perform at peak performance without dropping packets.

- Media conversion from SX and LX fiber to RJ45 copper or SFP
- Media conversion from 100Base-FX and 100BASE-LX to RJ45 copper

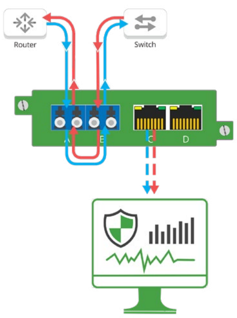
Unlike common media converters:

- Failsafe technology recognizes power outages and automatically reconnects the link
- Collect traffic from two sources and aggregate it to a single link
- Reducing critical infrastructure risk with zero impact to operations by achieving 100% network visibility
- Additional monitoring ports for future expansion

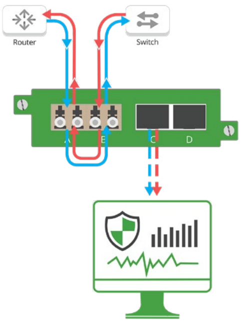




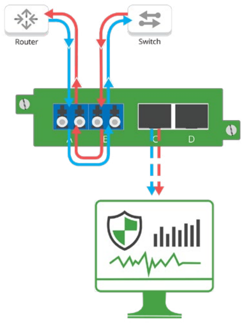
Multi-mode fiber to Copper



Single-mode fiber to Copper



Multi-mode fiber to SFP



Single-mode fiber to SFP

Recommended Products

AggregatorTAP: Fiber
SX or LX to copper conversion
SX or LX to SFP conversion
Portable | Aggregation, tap 'Breakout' & Regeneration/SPAN modes
Model # P1GMCA | P1GMSA | P1GSCA | P1GSSA

AggregatorTAP: 100Base-T
100BASE-T to copper conversion
Portable | Aggregation and tap 'Breakout' modes
Model # P100CCA

AggregatorTAP: 100Base-FX
100BASE-FX to copper conversion
Portable | Aggregation and tap 'Breakout' modes
Model # P100FXCA

AggregatorTAP: 100Base-LX
100BASE-LX to copper conversion
Portable | Aggregation and tap 'Breakout' modes
Model # P100LXCA

SOLUTION

MINIMIZING TRANSMISSION ISSUES WITH LINKS SPEED SYNCHRONIZATION

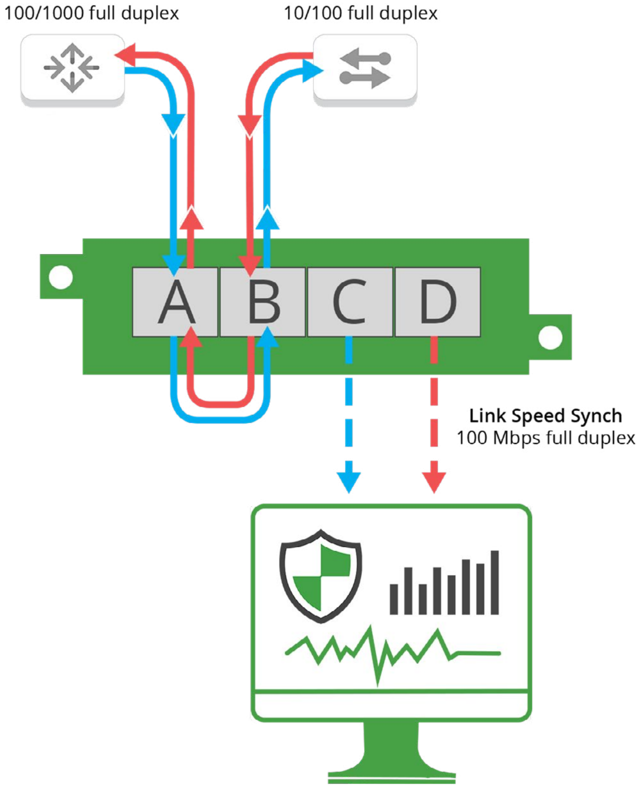
Link Speed Synchronization is included on Garland's copper network TAPs to allow the TAP to automatically negotiate issues to ensure the best possible rate of transmission between copper-based network traffic streams and all connected devices. With auto-negotiation, two devices advertise all their communication parameters (port speed and duplex state) so they can automatically connect at the highest common denominator.

- Auto-negotiation: Automatically connects at the highest common speed on all ports

That means that a switch advertising 10/100/1000 full duplex and a router advertising 10/100 full duplex will communicate at 100 Mbps at full duplex, because the TAP is smart and knows the highest speed the switch and router would select if they were connected to one another.

The TAP uses the auto-negotiation function to interrogate both attached devices to find out their individual capabilities, and keeps a table of the data to automatically determine the best transmission rates for each connection.

e.g., If someone logged into the router and changed it from advertising 10/100 full duplex to 10/100/1000 full duplex. Garland's Link Speed Synchronization function will ensure that the transmissions happen at 1000 Mbps at full duplex – all without manual intervention.



Recommended Products

Copper Network TAP
10M/100M/1000M (1G) | Portable | tap 'Breakout' mode
Model # P1GCCB

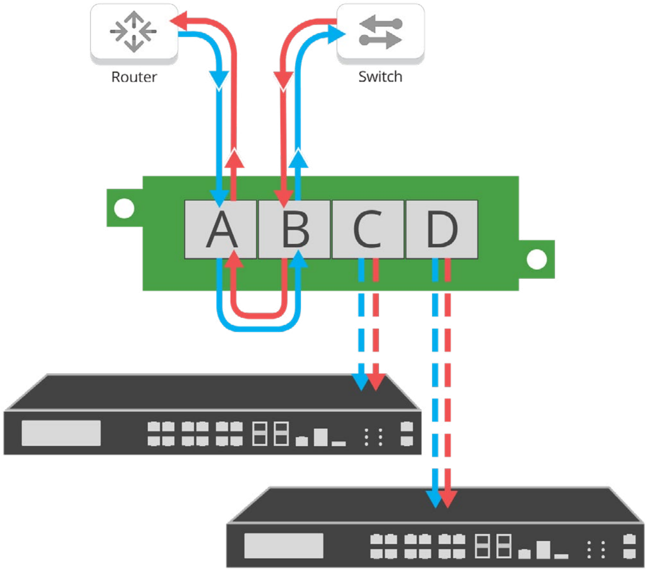
AggregatorTAP: Passive
100M | Portable | Aggregation mode
Model # P100CCA

AggregatorTAP: Copper
10/100/1000M (1G) | Portable | Aggregation, tap 'breakout' and regeneration/SPAN modes
Model # P1GCCAS

Copper Modular Network TAP
10/100M and 10/100/1000M | 1U or 2U | tap 'Breakout' mode
Model # M1GCCB

Military-Grade Industrial Network TAP
10/100/1000M(1G) | Modular 1/2 rack Portable Chassis
tap 'Breakout' mode
Model # M1GCCBm

HOW TO REDUCE NETWORK COMPLEXITY THROUGH TRAFFIC AGGREGATION



Expanding industrial networks who deploy various tools, multiple systems and devices within legacy infrastructure, often find themselves inundated in complexity and network sprawl. Many companies running a majority of their traffic off of SPAN ports often see a tangled web to manage, leading to SPAN port contention that can result in:

- Slower processing speed
- Loss of data and oversubscription
- Slower MTTR and threat hunting
- Data silos

SOLUTION

TRAFFIC AGGREGATION FOR VISIBILITY OPTIMIZATION

Traffic aggregation can be achieved in a multitude of ways. TAP aggregation accomplishes two goals:

- Streamlines traffic allowing teams to reduce the number of security tools needed
- Enhances scalability, to increase visibility and deploy new devices in the future

A single portable TAP can provide full duplex traffic on a single link, or even reduce three SPAN links down to one. A half rack 1U TAP can reduce four full duplex links or eight SPAN links down to 1, and the 2U chassis can aggregate 11 TAP links down to a single link.

Adding in network packet broker traffic aggregation further scales the traffic as needed, taking 24 TAP links down to one, and more.

Recommended Products

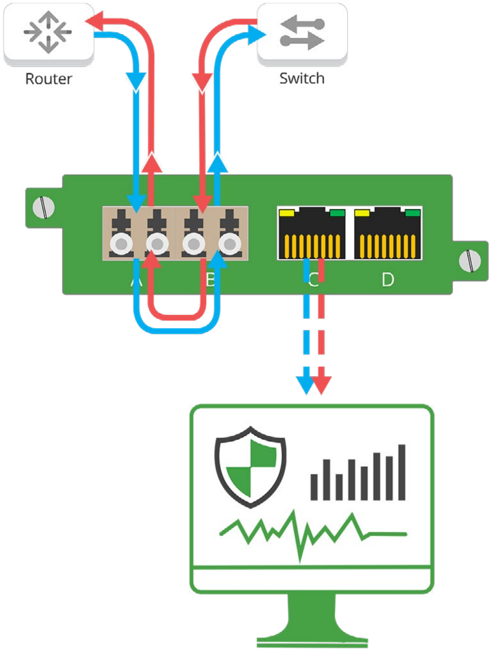
AggregatorTAP: Copper High Density
1G | 1U 1/2 rack | Aggregation & Regeneration/SPAN modes
Unidirectional Data | Diode Circuitry Design
Model # INT1G10CSA | INT1G10CSA-DC | INT1G10CSASP
INT1G10CSASPDC

XtraTAP™: All-In-1 Modular Packet Broker
10/100/1000M (1G) | 1U or 2U modular chassis | Remote Management
Filtering, Aggregation, Breakout & Regeneration/SPAN modes
Model # M1G1ACE | M1G2ACE | M1GC | M1GCCF

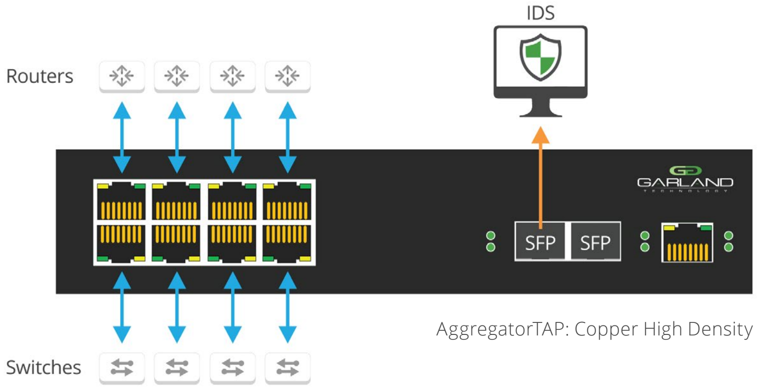
PacketMAX™: Advanced Aggregator
1G | High Density Aggregation | Filtering | Load Balancing
Model # AA1G52ACv2

PacketMAX™: Advanced Features
1/10G | High Density Aggregation | Filtering | Load Balancing
Tunnel Encapsulate [GRE, L2GRE]
Tunnel Decapsulate [GRE, L2GRE, ERSPAN, VxLAN]
Model # AF1G40AC | AF1G40DC

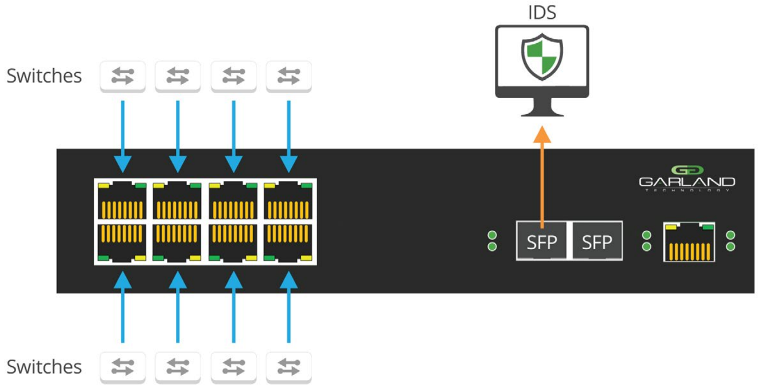
TAP AGGREGATION USE CASES



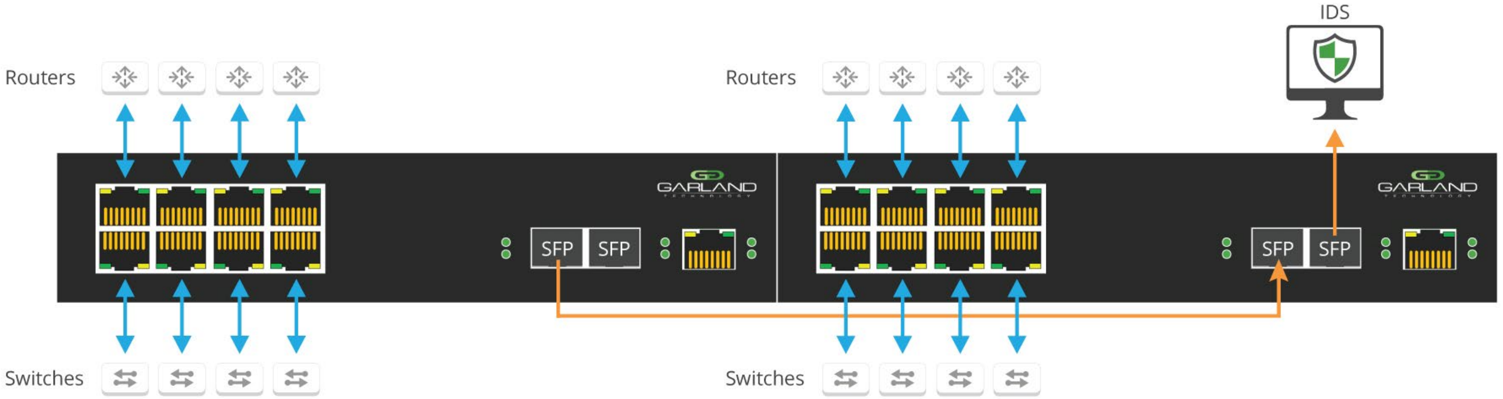
In this scenario, you are able to TAP one link and aggregate down to one monitoring port.



In this scenario, you are able to TAP 4 links and aggregate down to one monitoring port.

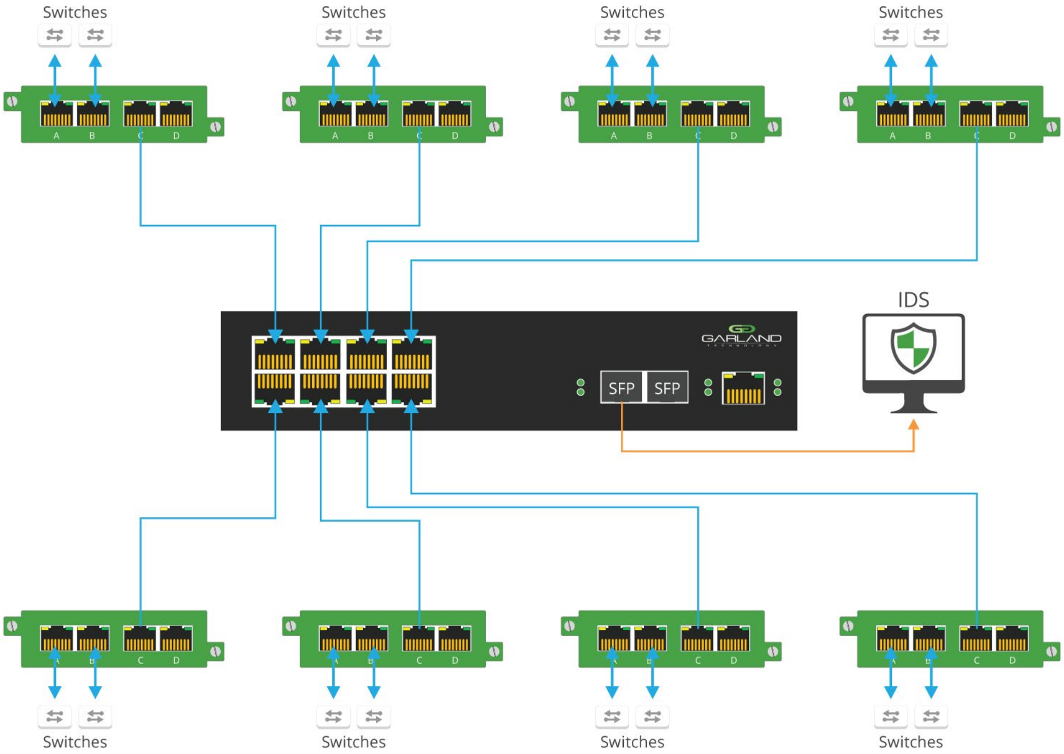


In this scenario, you are able to SPAN 8 links and aggregate down to one monitoring port.

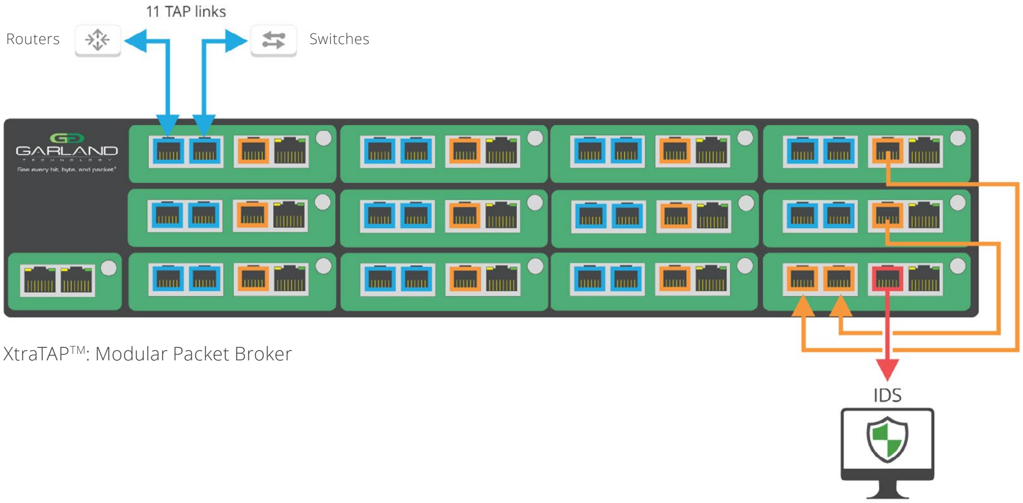


In this scenario, you are able to TAP 8 links and aggregate down to one monitoring port. Combining two units allows you to aggregate the first four links over to the second unit's 4 links and down to a single monitoring port.

SCALING TAP AGGREGATION USE CASES

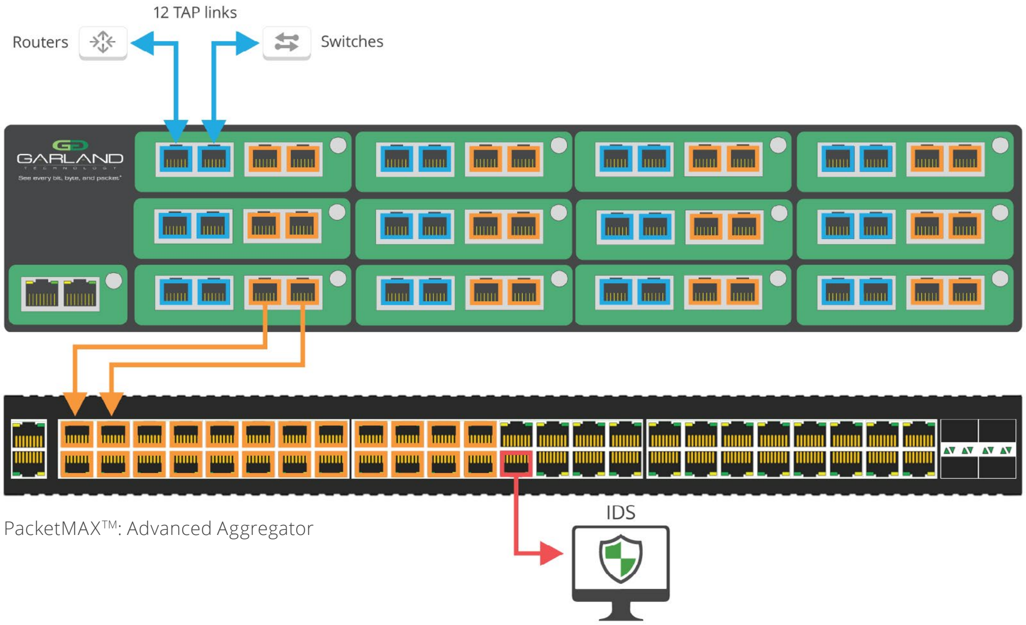


In this scenario, you are able to TAP 8 links in different locations and aggregate down to one monitoring port. Utilizing 8 passive 10/100 portable TAPs (P100CCA), allows you to TAP various locations into the AggregatorTAP aggregating down to a single monitoring port.

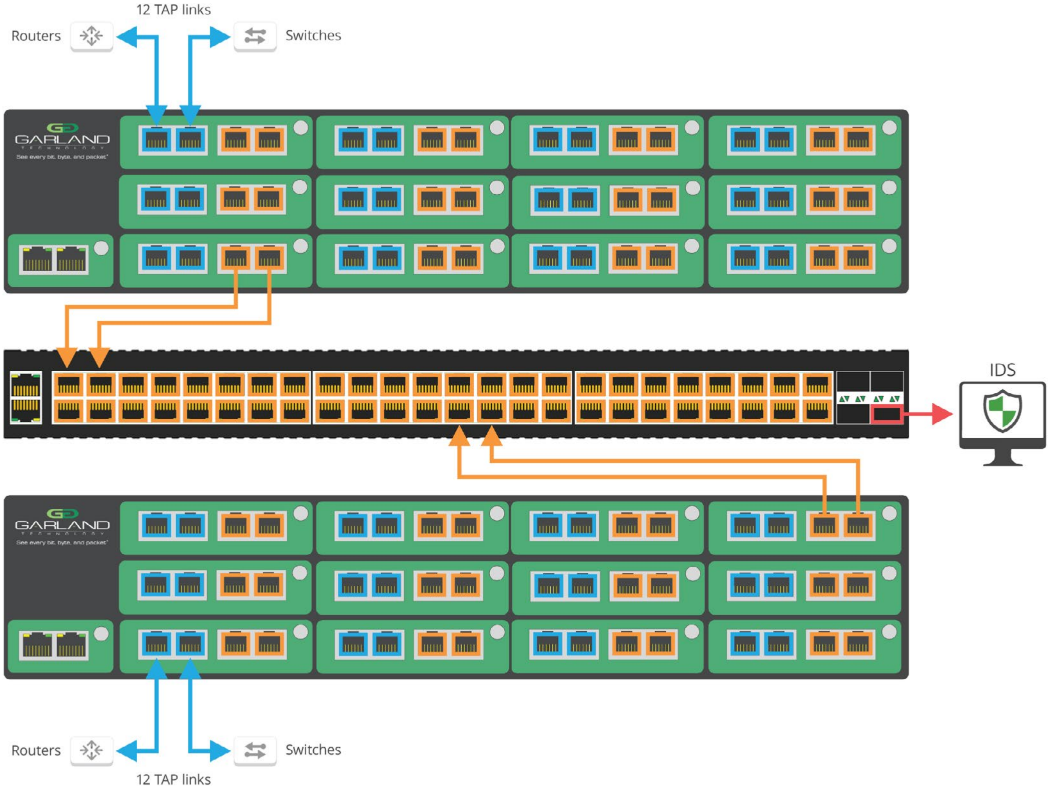


XtraTAP™: Modular Packet Broker

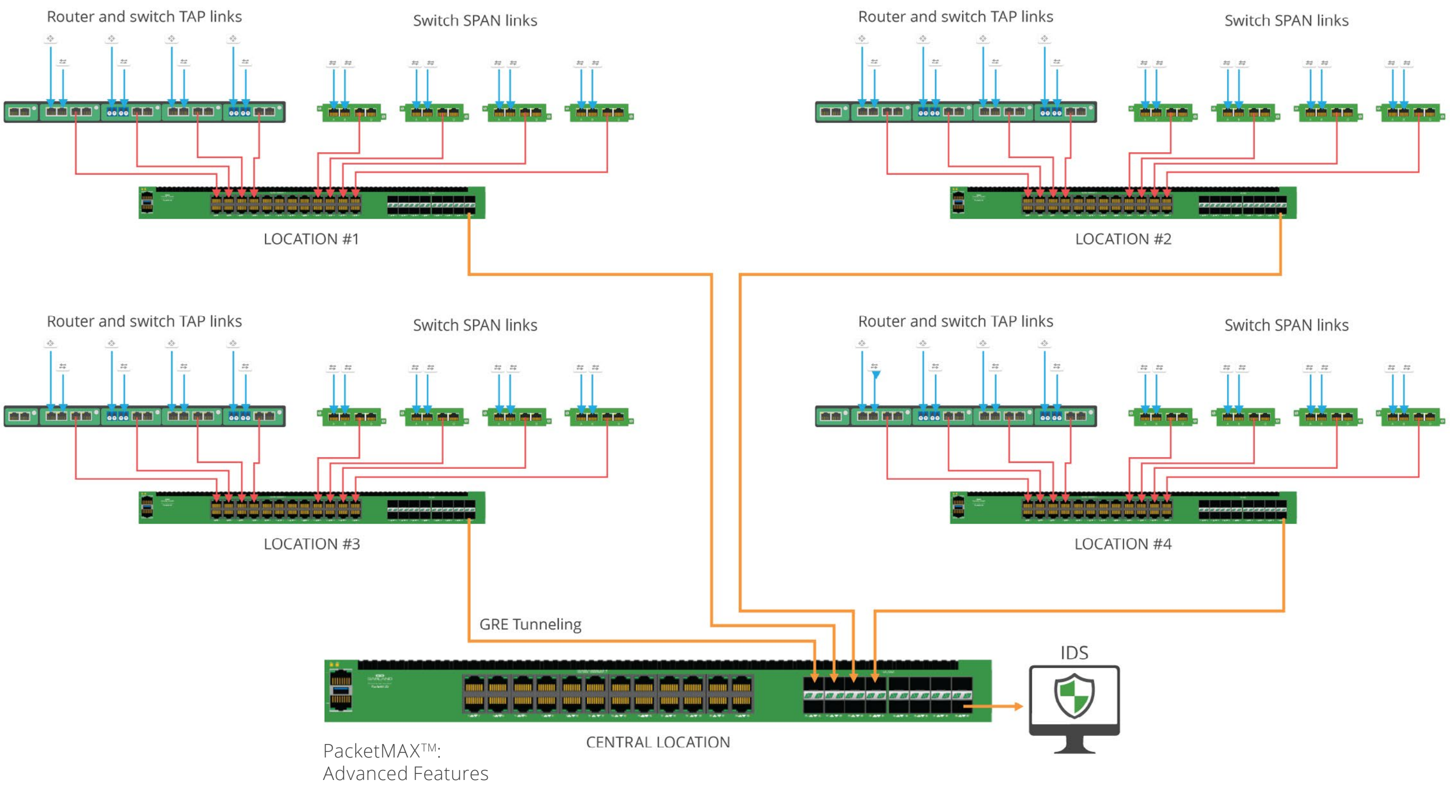
In this scenario, you are able to TAP 11 links and aggregate down to one monitoring port. Utilizing the XtraTAP's backplane, you are able to aggregate TAPs 1 through 4 on the top row, TAPs 5 through 8 on the second, and 9 through 11 on the bottom down to one monitoring port on TAP 12.


12 TAP links
Routers
Switches
GARLAND
TECHNOLOGY
See every bit, byte, and packet
PacketMAX™: Advanced Aggregator
IDS

In this scenario, you are able to TAP 12 'breakout' TAP links and aggregate down to one monitoring port. Utilizing the PacketMAX Advanced Aggregator allows you to aggregate 12 TAPs down to one. This high density unit has over 25 remaining ports, allowing for future growth.



In this scenario, utilizing the additional ports on the PacketMAX Advanced Aggregator you are able to TAP 24 'breakout' TAP links and aggregate down to one monitoring port.



In this scenario, utilizing the PacketMAX Advanced Features you are able to TAP and SPAN many links in various locations and GRE Tunnel back to a central location.

HOW TO PROVIDE UNIDIRECTIONAL TRAFFIC TO SECURITY AND MONITORING TOOLS

Some manufacturing environments may face regulation guidelines that require one-way data transfers, to enforce physical unidirectionality to protect network segments from incoming threats between segments or facilities.

In these network deployments, using SPAN simply is not acceptable. SPAN or port mirroring from a network switch are bi-directional, which creates an opportunity for hacking by deploying a device for monitoring or security.

SOLUTION

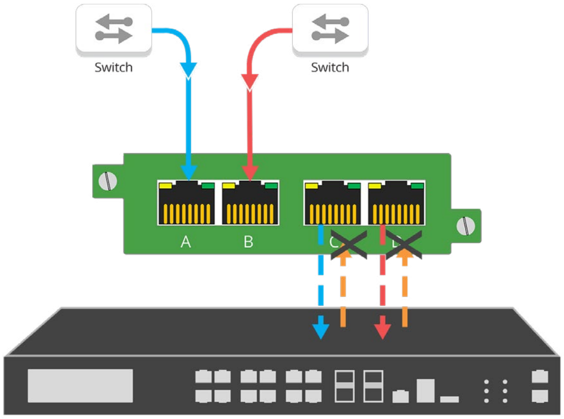
DATA DIODE TAPS OFFER UNIDIRECTIONAL SECURITY

Data diode TAPs are a purpose-built network hardware device that allows raw data to travel only in one direction, used as a traffic enforcer, guaranteeing information security or protection of critical digital systems, such as industrial control systems, from inbound cyber attacks.

Data Diodes are specifically designed not to send traffic back onto the network. Data diodes can be found most commonly in high security environments, such as federal defense and Industrial IoT, where they serve as connections between two or more networks of differing security classifications. This technology can now be found at the industrial control level for such manufacturing facilities as pharmaceutical, food and beverage, and chemical.

Garland Technology's Data Diode TAPs offer "no injection" tap aggregation for 10/100/1000M copper networks. This ensures no Ethernet packets can physically be sent to the Live Network TAP Ports or SPAN Ports.

Create unidirectional monitoring solutions that capture every bit, byte, and packet and ensure copied packets don't go back in and disrupt the industrial network — all in a package that's purpose-built and unhackable.



Recommended Products

Data Diode Network TAP
10M/100M/1000M (1G) | Unidirectional data diode circuitry design
Model # PT100
Model # P1GCCB
Model # P1GCCAS
Model # P1GMCA
Model # P1GSCA

Data Diode SPAN TAP
10M/100M/1000M (1G) | Unidirectional data diode circuitry design
Model # P1GCCAS-Custom
Model # CTAP-P1GCCREG
Model # INT10G10SP1

AggregatorTAP: Data Diode
10M/100M/1000M (1G)| 1U ½ rack | Aggregation & Regeneration
Unidirectional data diode circuitry design
Model # INT1G10CSA
Model # NT1G10CSA-DC
Model # INT1G10CSASP
Model # INT1G10CSASPDC

Provides a physically secure one-way communication path to the monitoring ports - securing SPAN.

HOW TO PROVIDING A SECURE AIR GAP VISIBILITY SOLUTION FOR VIRTUAL ENVIRONMENT MONITORING

Performance demands and the rise of innovative Industry 4.0 use cases for IoT devices, artificial intelligence, machine learning, and other advanced technologies have made completely air-gapped networks seem too limited.

Many say that air gapping is no longer a viable security tactic because of the widespread connectivity of industrial networking components. Increased connectivity combined with ever-growing usage of cloud-based solutions have pushed industrial network architects to look for more modern answers to cybersecurity issues.

This speaks to the larger challenge that industrial network architects face. When you start to deploy public and private cloud environments, how are you able to maintain visibility of all packets coming into and going out of the network in a way that keeps you in complete control of security? Designing industrial networks with passive network TAPs and data diodes have always been important. But new cloud environments and air-gapped networks require a more dedicated solution.

SOLUTION

VIRTUAL AIR GAP PACKET VISIBILITY FOR ADDED SOLUTION SECURITY

Garland Prisms allows you to mirror your out-of-band virtualized traffic to your monitoring tools, from an air gapped platform.

Garland Prisms Private Controller manages virtual Prisms sensor deployments from on-premise environments that are “air-gapped” or without Internet connections for security purposes.

Garland Prisms Private Controller is built from the same Garland Prisms Cloud based SaaS controller platform Garland customers use to monitor application workloads in a Public cloud. To extend virtualized visibility capabilities to air-gapped networks, Garland Prisms introduces on-premises management options that will help industrial environments remain secure without sacrificing cloud capabilities.

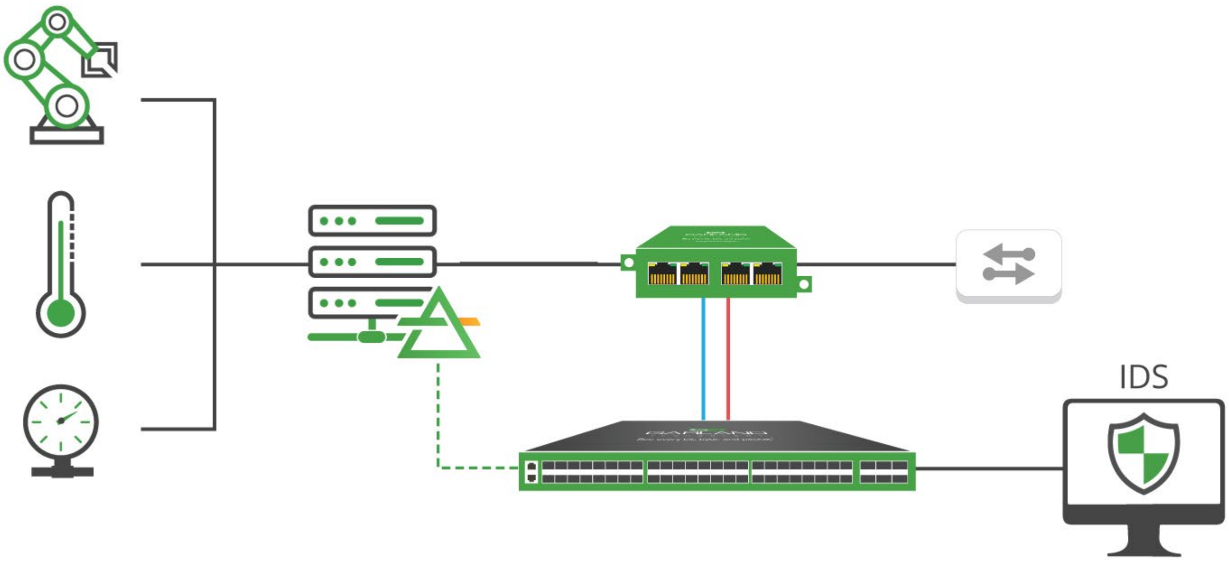
Recommended Products

GTVTAP1YRA
1 Year License Single Prisms Smart vTAP Agent for Public & Private Clouds ‘A’ Price Level applies to 10 licenses

GTVTAP1YRE
1 Year License single Prisms Smart vTAP Agent for Public & Private Clouds ‘E’ Price Level applies to 100-249 Licenses

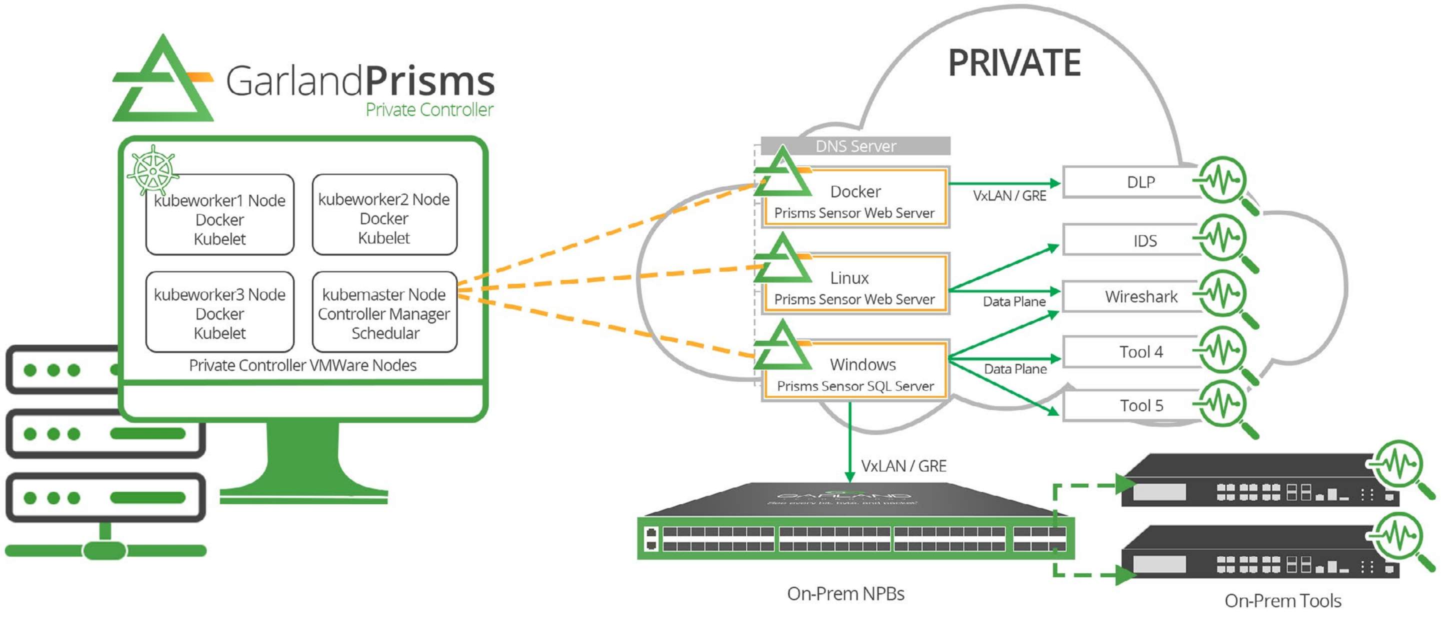
GTVTAP1YRH
1 Year License single Prisms Smart vTAP Agent for Public & Private Clouds ‘H’ Price Level applies to 1000+ Licenses

*Other licensing options are available



Migrating to a virtualized SCADA deployment offers many benefits including hardware server consolidation, high availability, migration capabilities, and easier backup and restore processes. However virtualizing a SCADA deployment leads to many challenges, including having to reconfigure resource allocation, conflicts with network OS activities and reduced visibility into the remote segment.

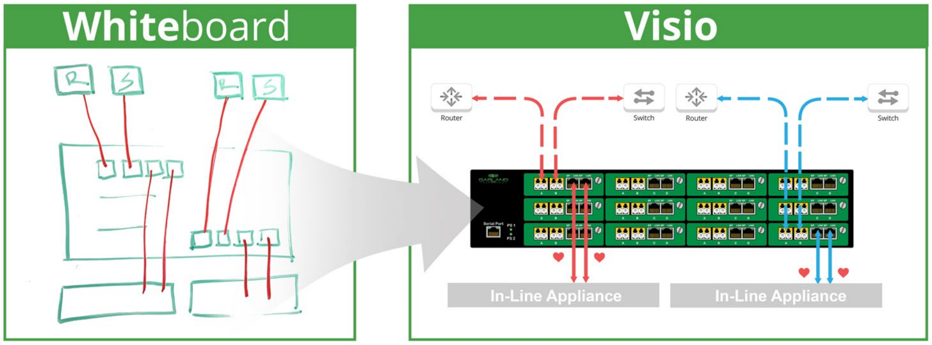
Deploying Garland Prisms traffic mirroring with the remote server hypervisors, eliminates these cloud data blind spots, providing the SCADA platform and any other connected system access and visibility. Integrating this virtual packet traffic with physical layer network TAPs and packet brokers provides a complete end-to-end visibility fabric for remote manufacturing segments.



- Private vTAP controller for air gap architectures
- Supports containers, Linux, and Windows Server
- Integrates with Garland physical TAPs and packet Brokers for complete end-to-end visibility

SETTING YOURSELF UP FOR ICS VISIBILITY SUCCESS

Looking to add ICS visibility to your manufacturing deployment, but not sure where to start? Join us for a brief network Design-IT consultation or demo. No obligation - it's what we love to do. For more info, please visit:
https://www.garlandtechnology.com/design-it



Garland Technology is a trusted leader in critical infrastructure visibility solutions for OT, enterprise, service providers, and government agencies worldwide. We believe secure network visibility should be an easy, seamless experience. Since 2011, Garland Technology has worked with OT customers to identify their unique challenges and requirements for critical infrastructure environments and deliver the industry's most reliable Network TAP, Data Diode, Network Packet Broker and cloud visibility solutions, that deliver packet visibility while ensuring the secure connectivity needed.

1 - NIST's Cybersecurity Framework Version 1.1 Manufacturing Profile
https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf

2 - https://www.techrepublic.com/article/industrial-iot-market-will-hit-922b-by-2025-driven-by-cost-savings-and-availability/

3 - https://www.forbes.com/sites/danielnewman/2020/11/11/the-industrial-iot-data-expansion-and-the-future-of-work/

4 - https://blog.infraspeak.com/iot-in-industry-and-the-future/

5 - https://www.scmagazine.com/home/security-news/apts-cyberespionage/verizon-picks-industries-that-are-prime-targets-for-cyber-espionage/

6 - https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf

7 - https://www.nist.gov/cyberframework/online-learning/five-functions

8 - https://collaborate.mitre.org/attackics/index.php/Main_Page