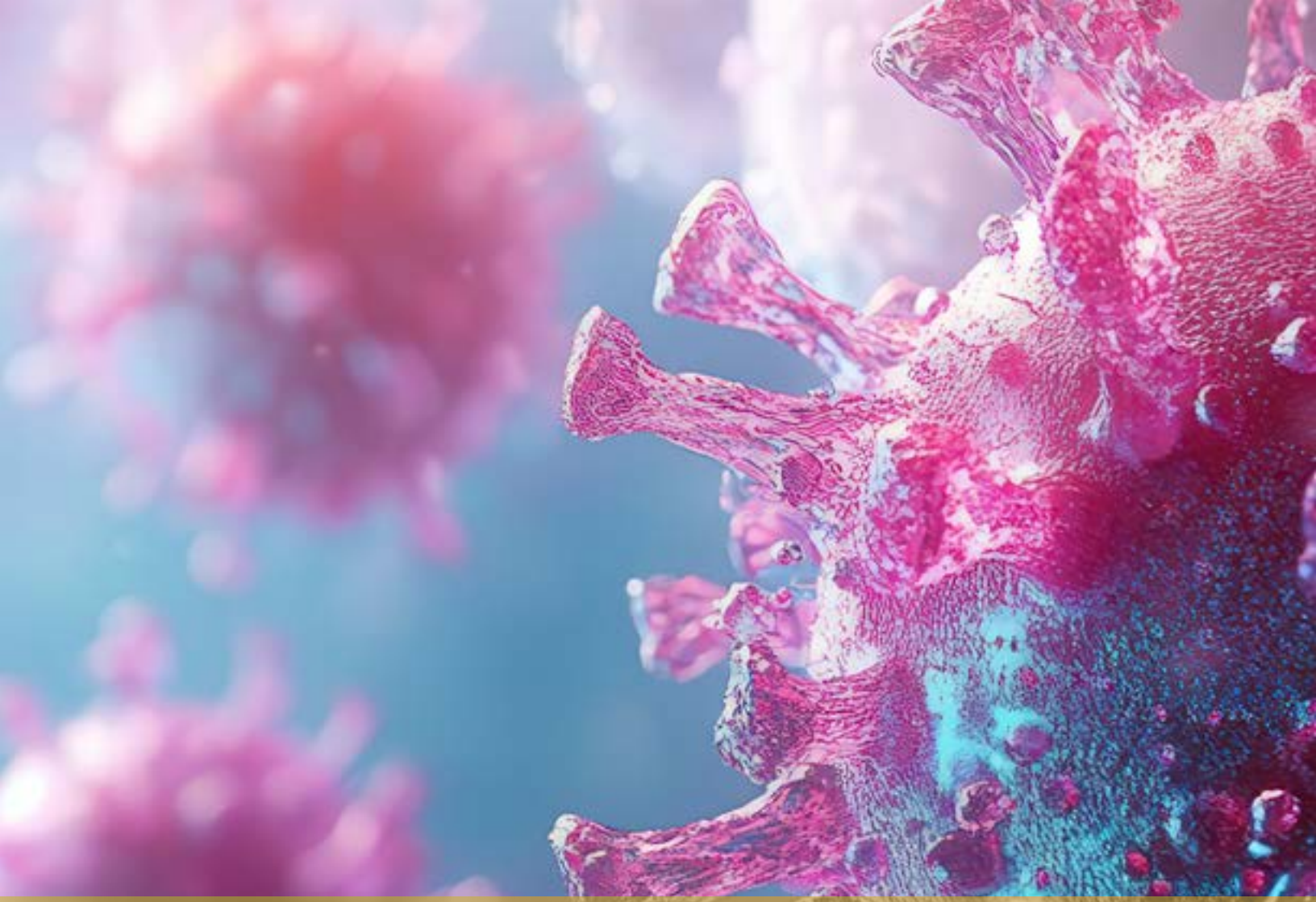


WHITE PAPER

Proactively Eliminate Entire Classes of Risk

Desired Outcomes from an OT Cybersecurity Protection Investment

BlastWave

TL:DR

This whitepaper examines the desired outcome of implementing Zero Trust Protection for Operational Technology networks.

The MITRE ICS AT&CK framework outlines several attack vectors (Discovery, Initial Access, Privilege Escalation, and Lateral Movement) that pose the biggest external and internal threats to OT networks.

The NIST Cybersecurity Framework (CSF) outlines the requirements for Zero Trust environments and what is required to minimize risk.

When the desired outcome of each CSF Protection requirement is determined, we evaluate what solution options exist today and determine the optimal solution: Comprehensive OT Zero Trust Protection.

A comprehensive solution will provide Network Cloaking, Passwordless Secure Remote Access, and Software-Defined Microsegmentation, eliminate multiple classes of risk, and provide a superior Return on Mitigation (ROM) for your OT Cybersecurity Protection investment.

BlastWave

CONTENTS

Understanding Classes of Risk

There is no such thing as an ultimately "secure network." In the early days of network security, one of the pioneers, Gene Spafford, put it best when he said:

> **"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts."**
>
> GENE SPAFFORD

However, cybersecurity is about removing risk from your network deployment, so naturally, we look for a structure to guide us in structuring our network. Humans love structure. It helps us categorize things so we can relate to and understand them. Many (although not all) humans also love checklists. The serotonin reward for crossing an item off your to-do list is a sublime pleasure for list lovers.

One mistake often made in cybersecurity is focusing on technology rather than outcomes. For example, mandating a firewall does not protect a network; it dictates the solution rather than the desired outcome. Indeed, firewalls protect a network, but what does the firewall need to do to minimize your risk? Some firewalls have targeted capabilities, and some have a wide range of technical abilities (often too much capability, if we are honest). Just because an IT manager deploys a firewall does not mean that their network is now fully protected.

The MITRE ATT&CK ICS Framework

The **MITRE ATT&CK ICS** framework establishes multiple tactics for penetrating ICS networks. We won't go into a detailed analysis of the tactics (many sites can do). However, we want to focus on the tactics with a remote networking component. Implementing a network protection framework prevents many of these tactics from succeeding, blocking off other tactics that depend on the success of another, earlier-stage tactic. Categories like Initial Access, Lateral Movement, and Discovery are all key tactics that any Protection solution should largely mitigate for a network administrator.

Figure: The MITRE ATT&CK for ICS matrix

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Communication Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameters	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Account	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Rootkit		
								Service Stop		
								System Firmware		
								Utilize/Change Operating Mode		

The desired outcome of any OT cybersecurity deployment should be to block all of the tactics that you can and monitor the rest. The more you can block, the less risk you are taking by operating your network.

Return on Mitigation with Cybersecurity Investments

Network administrators must balance the mission with risk management, which comes with a cost. That cost, in today's environment, is either: I spend to protect my network or spend to recover from a hack. The cost of dealing with an attack comes at companies from multiple angles, and the cost of security breaches and hacks is higher than ever before.

Some of the costs that result from a hack, ransomware, or data breach are:

Direct Costs

Ransom Payment: This is the most obvious cost, but it's important to note that paying the ransom doesn't guarantee data recovery and can encourage further attacks.

Data Recovery Costs: Even if a company pays the ransom, data recovery can be complex and expensive, involving specialized tools and experts. It is more than unencrypting and reusing – the data must often be rebuilt and relocated.

System Restoration and Business Disruption: Rebuilding systems, restoring data, and recovering from operational disruptions incur substantial costs.

Legal and Forensic Fees: Investigating the attack, complying with regulatory requirements, and potential legal actions can be costly. Notification Costs: Informing affected individuals about the data breach can involve significant expenses.

Indirect Costs

Lost Revenue: Business interruptions due to downtime, loss of productivity, and customer churn can lead to significant revenue loss.

Reputational Damage: A publicized cyberattack can damage an organization's reputation, leading to customer loss and difficulty attracting new business.

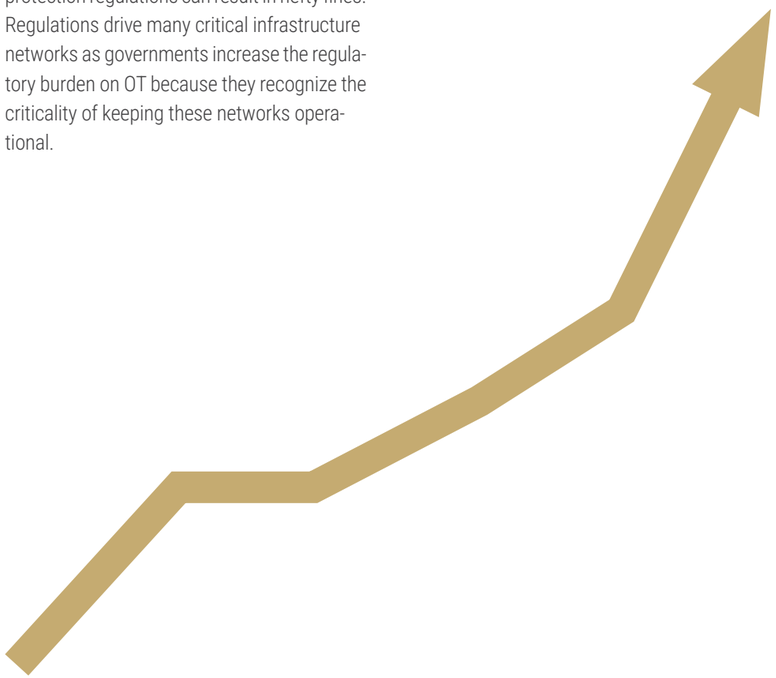
Increased Insurance Premiums: Insurance premiums often rise after a cyberattack, increasing operational costs.

Regulatory Fines: Non-compliance with data protection regulations can result in hefty fines. Regulations drive many critical infrastructure networks as governments increase the regulatory burden on OT because they recognize the criticality of keeping these networks operational.

Long-Term Costs

Cybersecurity Investments: Strengthening cybersecurity measures to prevent future attacks requires ongoing technology, personnel, and training investments.

Business Continuity Planning: Developing and maintaining a robust business continuity plan to minimize disruptions in case of future attacks incur costs.



Human Cost

Direct Impact on Human Safety

Physical Injury or Death: In industries like manufacturing, chemical processing, or power generation, a ransomware attack can lead to equipment failure or hazardous conditions, posing a direct threat to human life.

Health and Safety Risks: Disruption of critical infrastructure, such as water treatment or healthcare facilities, can compromise health and safety conditions.

Economic Hardship and Job Loss

Loss of Livelihood: Extended downtime can lead to layoffs or reduced work hours, causing financial hardship for employees.

Community Impact: Disruption of essential services can affect entire communities, leading to economic hardship and social unrest.

Psychological Impact

Stress and Anxiety: Concerns about service availability can stress the community, leading to overspending on alternatives, backups, or overreaching security methods.

Trust Erosion: A ransomware attack can damage public trust in organizations responsible for critical infrastructure.

Social and Environmental Consequences

Supply Chain Disruptions: Ransomware attacks can disrupt supply chains, leading to essential goods and services shortages.

Environmental Damage: Disruptions in oil and gas or power generation industries can lead to ecological accidents or pollution.

In Microsoft's Digital Defense Report, one metric mentioned is a return on mitigation (ROM) metric that determines the return on investment in cybersecurity deployments. Generally speaking, the lower the resources and effort involved, the higher the ROM (For more details on the methodology, go to Page 41 of the report). Applying the highest ROM items to your OT network improves your cybersecurity. This chart aligns with the critical component of any Cybersecurity Framework – protecting the network to remove or reduce risk. Removing as many significant or entire classes of risk as possible will drastically reduce the danger to your OT network. The highest ROM items are listed below, so we can consider these as we analyze protection needs as part of the Zero Trust Framework.

ROM Severity	Issues Found	% Customers w/Problem
15	No advanced MFA protection mechanisms enabled	37%
15	Poor user lifecycle management	21%
15	Lack of EDR coverage	13%
15	Lack of detection controls	10%
13	Resource exposed to public access	2%
12	Insufficient protections for local accounts	60%
12	Missing security barrier between cloud and on-premise	54%
12	Insecure Active Directory configuration	43%
12	Insufficient device security controls	8%
11	Legacy cloud authentication is used	47%
11	No advanced password protection is enabled	37%
11	Missing content-based MFA protection mechanisms	24%
11	Insecure operating system configuration	3%

The actual cost of not protecting your network is a combination of a breach, downtime, loss of reputation, and loss of customers. Later in this paper, we will return to the ROM framework to discuss OT's ideal cybersecurity protection solution.

Significant Threats to OT Networks

OT networks have never been a bigger target than they are today. CISA, FBI, DoE, Homeland Security, and NSA have all issued advisories on risks and threats to OT networks, reflecting the US government's concern. A hearing was held in Congress in January 2024 that outlined the CISA, FBI, NSA, and other government leaders' concerns with China's threat to the US. Multiple studies show the risk to OT networks and the targets of known bad actors, hostile nation-states, and hacktivists.

A new concern has come to the forefront recently with the addition of GenAI to the hacker's arsenal. The UK's NCSC and the US's InQTel are issuing reports on how GenAI turbo-charges specific attack vectors like Reconnaissance and Phishing. This change in tactics makes establishing a strong Protection barrier around your network more critical than ever since GenAI is a powerful force multiplier.

The NCSC report highlights that the impact of AI on cyber threats is uneven, both in terms of its use by cyber threat actors and in terms of uplift in capability. AI will primarily offer threat actors an uplift in social engineering capabilities. Generative AI (GenAI) creates convincing emails to improve interaction with victims, including creating lure documents without the translation, spelling, and grammatical mistakes that often indicate phishing. Threat actors, including ransomware groups, are already using AI to increase the efficiency and effectiveness of cyber operations, such as reconnaissance, phishing, and coding. Phishing, typically aimed at delivering malware or stealing password information, is vital in providing the initial network access that cyber criminals need to carry out ransomware attacks or other cyber crimes. AI will assist with malware and exploit development, vulnerability research, and lateral movement by making existing techniques more efficient.

ROM Severity	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	**Moderate uplift**	**Moderate uplift**	Uplift
Social engineering, phishing, passwords	**Uplift**	**Uplift**	**Significant uplift (from low base)**
Tools (malware, exploits)	**Realistic possibility of uplift**	**Minimal uplift**	**Moderate uplift (from low base)**
Lateral movement	**Minimal uplift**	**Minimal uplift**	No uplift
Exfiltration	**Uplift**	**Uplift**	**Uplift**
Implications	Best placed to harness AI's potential in advanced cyber operations against networks, for example use in advanced malware generation.	Most capability uplift in reconnaissance, social engineering and exfiltration. Will proliferate AI-enabled tools to novice cyber actors.	Lower barrier to entry to effective and scalable access operations - increasing volume of successful compromise of devices and accounts.

However, external threats are not the only concern for OT network administrators. The entire concept of Zero Trust is "never trust, always verify." Part of this is that an employee who may be allowed to access one segment of your IT or OT resources may not be permitted to access another segment, and your cybersecurity solution should both prevent that and warn you if someone is trying to breach that barrier.

Since threats can be internal or external, let's examine them closely. This section will explore some of the classes of threats in more detail.

External Threats

External threats are the most numerous threats to OT networks. In an OT network, a hacker's desired outcome often differs from an IT network's. For hostile nation-states, the desired outcome is to immediately disrupt the OT network to cause havoc or place control software into the network that can be activated when desired. Command and Control software activation can coincide with other activities to inflict maximum damage to the nation under attack.

For hacktivists, the desired outcome is often to shut down the OT systems and leave messages that promote their cause. Other bad actors or criminals will frequently go after high-profile OT networks (like manufacturing) and seek to hold them for ransom because downtime is often 10x or more than the cost of a data breach. Hence, the likelihood of getting paid is higher than in many IT networks.

In the era of GenAI, it is pretty simple to utilize automated tools to conduct the initial phases of an attack using two of the most successful vectors from the MITRE ATT&CK framework: Reconnaissance (Discovery) and Phishing (Initial Access).

Discovery

The most common precursor to a cyberattack is reconnaissance (referred to in the MITRE ATT&CK as Discovery). If I know what is in your network, I can optimize my attack vectors to exploit known weaknesses in your network. Many cyberattacks begin with exploiting known CVEs, whether in network systems or end devices (depending on how "holey" the network is), to gain access to the network. GenAI makes both sides of this task easier, using no-code tools to create scanning software and enumerating all known CVEs for the systems discovered in the initial scanning. The more thorough the reconnaissance, the faster and easier a cyberattack is. The desired outcome for an OT administrator is to make reconnaissance impossible with a minimal attack surface.

Effective reconnaissance, or Discovery, is often the first step in a cyberattack, exploiting known vulnerabilities to breach networks.

Initial Access

The most common Initial Access exploit is phishing, considered one of the most significant risks in cybersecurity. According to various sources (Deloitte, Cofense, CISA), over 90% of successful cyberattacks begin with a phishing email. Hackers and bad actors can use GenAI to craft better phishing emails and research targets. This results in more effective emails tricking the user because they use the right "voice" of the spoofed identity. They also use the research to reference things that the target of the phishing attack might not realize that an attacker could find out. For example, social media enables a hacker to show an intimate knowledge of the target (trips, events, etc.). These tactics might seem far-fetched for a consumer attack, but a nation-state-sponsored attack on critical infrastructure would attempt to leverage this ability.

Combine this with the use of GenAI by cybercriminals in attacks resulting in data leaks that include passwords (Even LastPass has suffered data breaches). We now have an untenable situation for passwords. The shift in the IT world may take a while to resolve, but there is less time and room for error in the OT world, where a steady stream of hacks has occurred over the last year. The impact of the attacks is growing, and countries worldwide are ramping up their efforts to improve security and attack detection. With GenAI emerging as a powerful tool for hackers, security solutions that still rely on or promote passwords will eventually fail. MFA that does not rely on passwords must become a best practice for OT environments, or the rise of incidents resulting from credentials leaks will explode in 2024/2025. The desired outcome is a passwordless MFA not susceptible to MFA bombing or browser session hijacking.

Other initial access risks involve exploiting open or vulnerable applications accessible from external sources. In IT, it is difficult to shield all systems from remote access. However, this is not typically a problem in OT. Hence, the desired outcome is that systems are virtually air-gapped from the Internet, as very few OT systems need direct access to the Internet. Still, they need access to control systems (which need to be accessed remotely).

Internal Threats

Insider risk is 100% of users – whether intentional or unintentional. Gartner said it best: "Not every insider risk becomes an insider threat; however, every insider threat started as an insider risk."
The 2023 Ponemen Cost of Insider Threats Global Report stated that 75% of incidents resulted from non-malicious insiders (55% negligent, 20% careless), and 25% were malicious insiders.

Negligent employees fail to protect their systems, click on invalid links (phishing), get infected with malware, or have their credentials stolen through external hacks. For this reason, all employees are an insider risk – any employee may fall for a phishing email, MFA bombing, or some other external factor and have their accounts turn into an insider threat (even if the employee is not malicious).

Disgruntled employees may do this intentionally, especially ex-employees or employees leaving the company on bad terms. When employee or contractor credentials are left active once an employee leaves, the risk of compromise escalates. Malicious insider incidents are far more expensive and take longer to recover from than external hacks because these employees know how to do the most damage to the OT network.

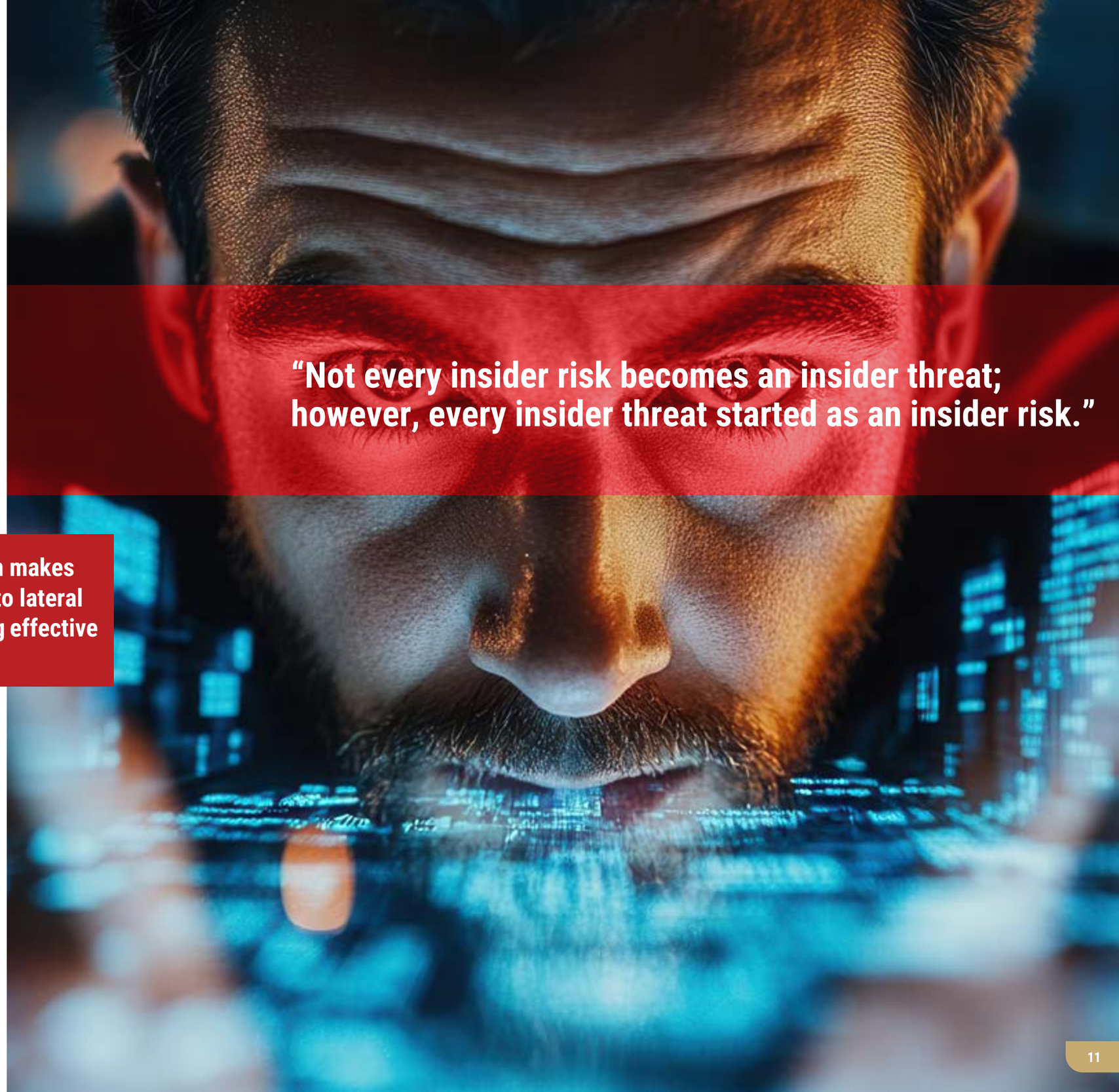
Privilege Escalation

Any hacker who obtains access to authorized credentials will seek to escalate their privileges to gain access to more accounts and systems. The ultimate goal is to increase their access to the most privileged accounts (aka root or administrator) to gain complete control over the network. Malicious insiders will attempt to escalate their privileges using insider knowledge of co-workers and systems. The desired outcome for the OT network administrator is not to allow privilege escalation for any accounts.

Lateral Movement

OT has a different problem than IT when it comes to lateral movement. Classic OT networks are utterly vulnerable to lateral movement when someone gains access to any system because they are flat Layer 2 environments. Even today, many OT networks are flat, often because they avoid segmentation to limit performance impact. With IT networks, it doesn't matter if your email arrives in 3 seconds, but in OT, milliseconds matter. The Purdue model promotes segmentation to fight this challenge. Still, many OT networks struggle because segmentation done with firewalls takes an excruciatingly long time and requires network downtime, which is unacceptable in many OT networks. The desired outcome is that lateral movement is complex (some OT devices need to talk to each other) or impossible between OT devices, even if they are on the same LAN segment.

OT networks' flat design makes them highly vulnerable to lateral movement, complicating effective segmentation



Attack Types

Today, the cyberattacks most often factored into IT risk calculations are data breaches, ransomware, and downtime. These events keep CISOs and CEOs up at night and continuing to invest in cybersecurity. Let's look at each of these and how they affect OT networks.

Data Breaches

Data breaches are primarily an IT cybersecurity problem. Still, there have been many instances where a vulnerability in IT was the opening act of an OT hack, primarily due to the sheer volume of vulnerabilities in the IT infrastructure. There have also been OT vulnerabilities that led to an IT breach (the Target data breach). Poor boundaries between IT and OT led directly to many of these hacks. In the Target case, a path into the OT and IT network existed because of a contractor's credentials, and hackers subsequently stole information from as many as 110M customers. If the IT and OT networks had been properly segmented and remote access had been adequately secured, no hacks would have occurred. IBM estimated the cost of a data breach to be $4.45M in their 2023 Cost of a Data Breach Report, but that cost varies by industry. OT network operators, especially in revenue-generating operations like manufacturing or oil & gas, are likely to see cases where a data breach may be accompanied by ransomware (see below) holding their OT assets hostage.

Ransomware attacks not only demand ransom payments but also cause costly downtime and long-term financial impacts, often starting with a phishing email

Ransomware

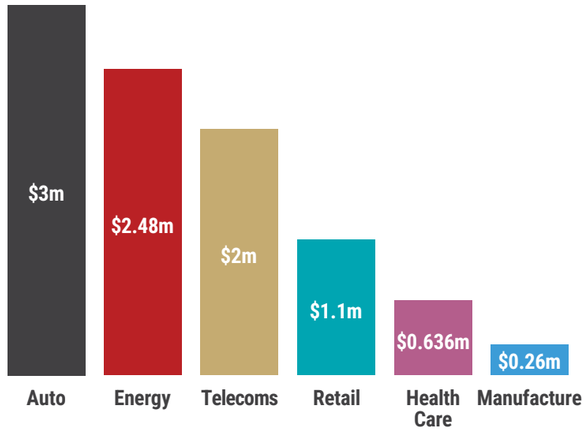
Ransomware attacks impose significant financial burdens on organizations. The costs extend far beyond the ransom payment itself. Several studies (IBM's Cyber Resilient Organization Study and CISA) indicate that most ransomware attacks begin with a phishing email, highlighting the danger of that specific attack vector.

It's crucial to remember that the total cost of a ransomware attack often far exceeds the ransom payment. The indirect and long-term consequences can be devastating for organizations of all sizes. Comparitech estimates the average downtime from ransomware in 2023 is 18.71 days, costing $15.5M (for healthcare). Fisher Phillips reports that the average cost of ransomware attacks was $5.13M. For OT networks that generate revenue, ransomware is responsible for downtime and the associated human cost.

Downtime

Downtime is the worst possible scenario for OT networks (It is called Operational Technology for a reason.) Ransomware gangs seek to disrupt the OT network and hold it hostage until the hackers. In many cases, the question is if the ransom is less than the cost of downtime to recover from the hack without payment, and if so, the "smart" economics are to pay the ransom (which does not always result in the restoration of the network). Pingdom did a study that reports the cost of downtime for several industry verticals:

Cost of downtime per hour



One easy return on investment calculation for OT cybersecurity is that if it can prevent even a single hour of downtime, the network deployment is likely to pay for itself

OT and IT Differentiating Factors

The fundamental differences in the risks and priorities of OT and IT should lead to different cybersecurity and protection activities, even though the desired outcomes are similar. Understanding these differences is important because they significantly impact the desired outcomes and tactics to secure OT networks. The critical difference between the two is the difference in the name: Information Technology versus Operational Technology.

One of the most important things is that an Operational Technology network MUST continue to be operational, which changes some of the desired outcomes. The **Operation** of the network is the distinguishing component for OT, whereas in IT, it is the **Information**. This fundamental difference manifests itself across the entire OT deployment process.

We call these the 8 P's of OT Security: Priorities, Personnel, Privileges, Programs, Protocols, Parameters, Processing, and Placement. Because of the focus of OT networks and the difference in the desired outcome, these "P" factors dictate a different focus for the OT cybersecurity framework.

Priorities: IT and OT differ in their organizational priorities

The average commercial IT group's priority is protecting proprietary and Personal Identifiable Information (PII). In OT, availability and reliability trump all other concerns except human safety. Most entities and organizations view IT as a cost center, whereas the OT group works at a profit or at least supports the processes that create the profit. If the OT network goes down, the company does not make money or produce products, which is catastrophic for companies. Downtime is even more devastating for public services and utilities like water, power, and fuel.

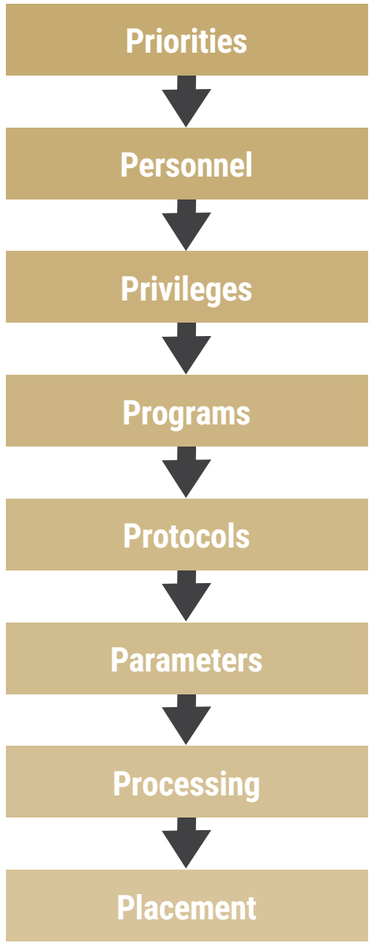
Personnel: IT and OT differ in personnel

Most IT personnel have a dedicated role with an IT title, such as Network Administrator, Help Desk Administrator, Database Administrator, etc. Conversely, OT personnel also charged with cybersecurity generally continue in their primary roles, with titles of SCADA Engineer, Process Control Engineer, and so on. These cybersecurity functions have been "bolted on" to their existing workloads as additional responsibilities, usually without any other streamlining or reduced duties. OT security solutions must be more straightforward to deploy, operate, and maintain than IT solutions.

Privileges: IT and OT differ in authentication and access.

Most IT systems require access to the internet and remote access, and security policies are broad and permissive. OT devices often do not but are configured to mimic IT policies. Under the guise of "easy access," OT devices may even provide automatic access to other devices from the same manufacturer without requiring re-authentication. However, the OT network is often flat, enabling risky lateral movement by internal and external threats. Different device groups must be segmented from each other to reduce the risk of lateral movement and privilege escalation by external and internal threats.

Contemporary IT systems regularly use Multi-Factor Authentication (MFA). IT resources estimate MFA adoption at greater than seventy percent. OT systems should seldom access the internet, and remote access must be severely restricted. OT uses MFA to a much lesser extent, where adoption may be less than twenty percent overall. Some OT facilities may forbid, interfere with, or simply lack sufficient data service to support standard IT MFA systems that require Short Message Service (SMS).



Programs: IT and OT differ in applications
COTS software, such as email clients, database applications, and Software as a Service (SaaS), fills IT catalogs. These user-centric applications and operating systems extensively use web-based interfaces and browser applications. OT applications focus on the OT asset, usually without regard for state-of-the-art user interface (UI) and user experience (UX) trends, and often utilize unencrypted protocols. There have been multiple exploits of HMI-based controls for OT systems over the past few years that highlight the need to shield these systems from remote access.

Protocols: IT and OT differ in protocols
The IT world has standardized on the Transmission Control Protocol / Internet Protocol (TCP/IP) suite of protocols version 4. Some IT cyber assets even use IPv6, but it still needs to be considered the Standard. On the other hand, OT devices may use any standard IPv4 protocols in conjunction with a long list[1] of custom or proprietary protocols (Modbus, DNP3, and DALI, for example). In these protocols, many operate in the clear for performance purposes. Additionally, many of these OT assets continue operating from their decades-old design without concern for cybersecurity, mandating protection from external access.

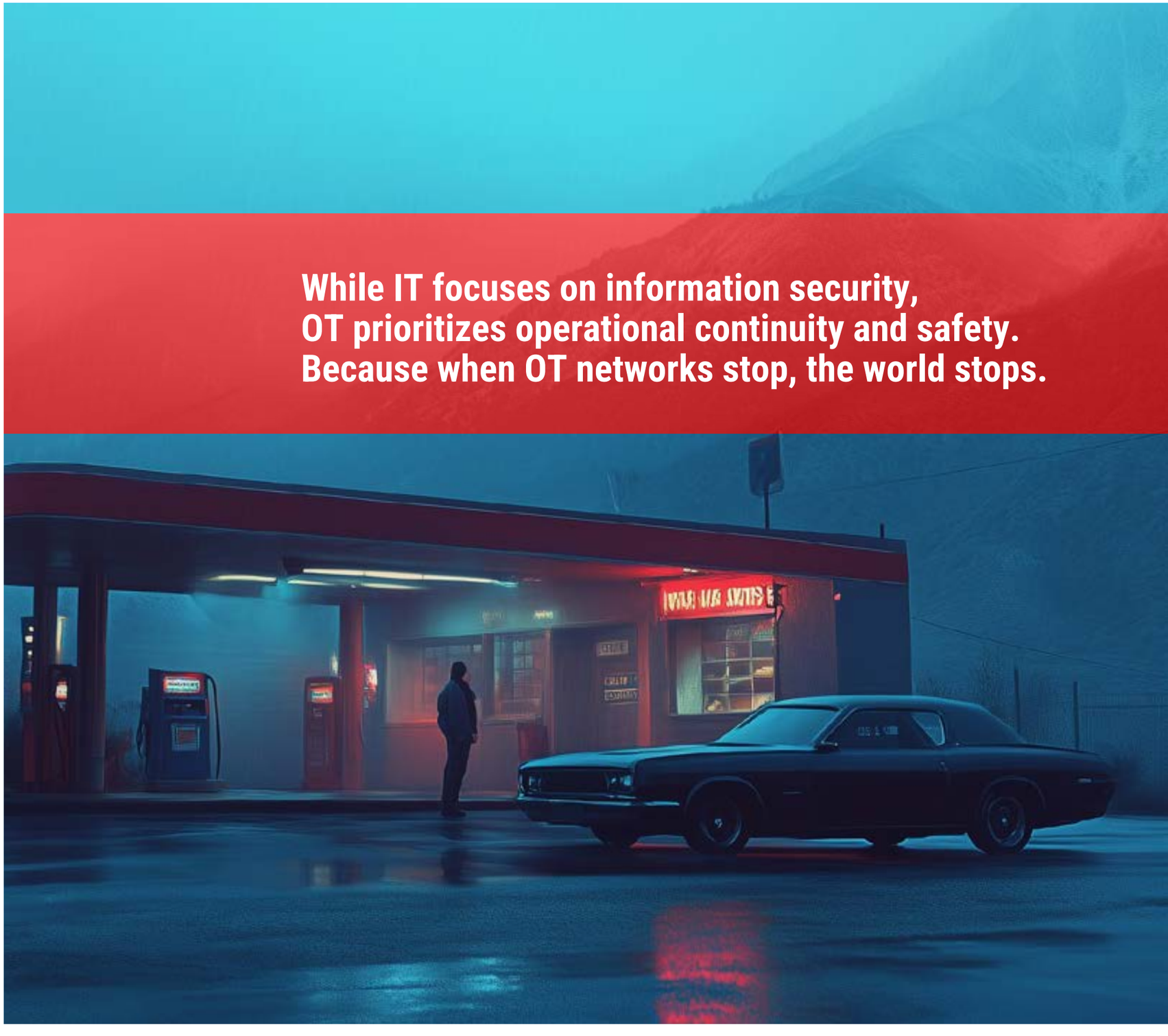
Parameters: IT and OT differ in data management
IT software has simplified the ability to encrypt, control, store, and consume data. In addition to this utilization, IT organizations regularly send metadata and statistics to cloud applications for Artificial Intelligence (AI) training and processing, especially for cybersecurity risk analysis. OT keeps access logs, naturally, for compliance purposes but primarily logs Sequence of Events (SOE) for forensics review after a reportable disturbance or unplanned outage. These data points rarely undergo AI analysis today, although OT AI systems increasingly analyze access and network logs in the CSF's Detection and Recovery phases.

Processing: IT and OT differ in hardware lifecycle.
IT assets range from desktops and laptops to servers and every network or WiFi component. Most organizations rotate these devices on a three-to-five-year cycle. OT cyber assets usually span the asset's lifetime, which is tens of years. Many OT systems operate flawlessly on small DIN rail-mounted systems running Windows NT 4.0 or Embedded. When hardware fails in these systems, the entity obtains new-old-stock hardware and restores the running software. It also means there will likely be unpatched vulnerabilities, meaning that unfettered access to OT devices would dramatically increase the cybersecurity risk.

Placement: IT and OT differ in environmental conditions.
The IT data center is the ultimate bastion of physical and electronic cybersecurity. Much time, money, and effort go into designing data centers, Security Operations Centers (SOC), and Network Operations Centers (NOC). Generally, the IT data center provides comfortable office conditions, sometimes called a "shirt-sleeves" environment, for personnel. The nature and purpose of OT equipment contrast sharply with those of the IT data center. OT equipment rarely comes from data or cybersecurity design but from production needs. Often, OT equipment may spread across many square acres or miles, like electrical substations, oil fields, or wind farms. This geographic separation means that almost all access to these systems will be remote.

OT and IT Differences Summary
These fundamental differences mean that the desired outcomes for OT may differ from the IT world. While a DDOS attack in the IT world may inconvenience a company, in the OT world, it could take down the electricity grid for a large city, causing extensive damage and even loss of lives. For this reason, this paper will focus on the Protection function within the Cybersecurity Framework. The critical question in any cybersecurity deployment is: "What outcome do I want from deploying this solution?"

1 List of Automation Protocols, Wikipedia
https://en.wikipedia.org/wiki/List_of_automation_protocols



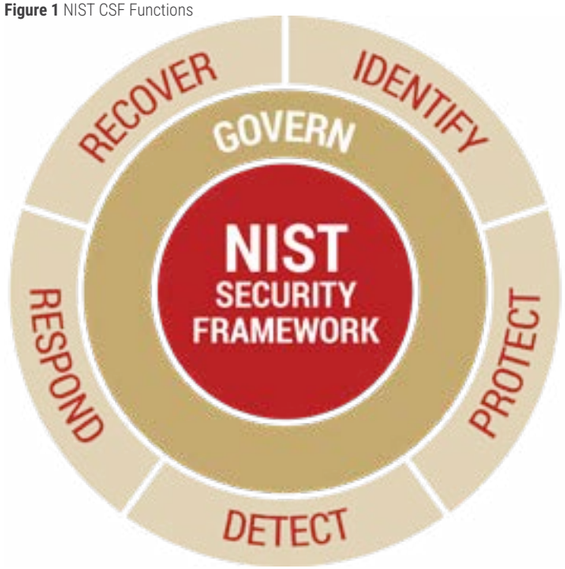
Core Functions of the Cybersecurity Framework

The NIST Cybersecurity Framework gives network administrators guidelines and a checklist for securing their network to the best of their abilities against external threats. NIST has been at the forefront of guiding risk reduction and introduced an initial Cybersecurity Framework in 2017. In 2023, NIST updated its Cybersecurity Framework in response to years of lessons learned from the initial version.

The cybersecurity market has come a long way since 2017, and the threat environment has changed significantly. The updated NIST CSF gives organizations a model for managing risk, and this paper will apply the principles of the CSF to Operational Technology (OT) rather than Information Technology (IT) network deployments, with a specific focus on the Protection Function.

The NIST Cybersecurity Framework does an excellent job of outlining the desired outcome for each function. Governance communicates and monitors the strategies and tactics for the remaining five functions, each a crucial component of a comprehensive cybersecurity strategy.

Figure 1 NIST CSF Functions



The following desired outcomes of each function are taken directly from the NIST document.

GOVERN (GV):
The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

IDENTIFY (ID):
The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

PROTECT (PR):
Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

DETECT (DE):
Possible cybersecurity attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.

RESPOND (RS):
Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

RECOVER (RC):
Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

NIST illustrates the CSF Functions as a wheel because all of the Functions are required and work together to build a comprehensive cybersecurity strategy. For example, an organization will categorize assets under **IDENTIFY** and take steps to secure those assets under **PROTECT**. Investments in planning and testing in the **GOVERN** and **IDENTIFY** Functions will support the timely detection of unexpected events in the **DETECT** Function and enable incident response and recovery actions for cybersecurity incidents in the **RESPOND** and **RECOVER** Functions. **GOVERN** is at the center of the wheel because it informs how an organization will implement the other five functions.

Organizations must implement a framework that covers all functions in the CSF. As stated in the CSF, the functions apply to IT and OT. Still, it is vital to acknowledge the difference between IT and OT because they have some crucial differences, especially regarding protection and the desired outcomes.

The NIST Cybersecurity Framework outlines crucial functions that work together to secure both IT and OT systems, emphasizing that governance and strategy are central to effective risk management

Protection for OT Networks Using the CSF as a Guide

With the above exploration of risk as a background, what are the desired outcomes for OT Cybersecurity Protection?

1. The OT cybersecurity protection solution network must prevent external intrusion or internal attacks from affecting OT network operations.

2. Remote Access must be tightly controlled to the OT network because almost all access is remote access for OT.

3. The OT domain must be separated from the IT domain to prevent spillover attacks and drastically reduce risk from highly vulnerable IT systems and remote access.

4. The OT network must be microsegmented to reduce the risk of lateral movement by insider or physical access threats.

5. Deploying protection must be minimally disruptive or intrusive into data flows and operational processes to reduce operational impact and lost productivity.

With these keys in mind, let's analyze the CSF's Protection Requirements and how they apply to achieve these desired outcomes for OT networks. The NIST PROTECT function requirements were safeguards to manage the organization's cybersecurity risks. We will take them individually and determine the best options to ensure the desired outcome.

OT ZERO TRUST ALLIANCE

The Operational Technology (OT) Zero Trust Alliance:

The OTZTA is a group of cybersecurity solution providers seeking to accelerate the deployment of comprehensive Zero Trust solutions. They built a coalition of Zero Trust focused on solving the biggest challenges for OT networks worldwide. Our solutions deliver real-world zero trust cybersecurity deployments, and we are actively working to scale and standardize ZTNA interfaces to enable flexible service adaptation for the many industries that rely on OT networks.

For more information, see www.otzta.org

Identity Management, Authentication, and Access Control (PR.AA)

The desired outcome for PR.AA is that access to physical and logical assets is limited to authorized users, services, and hardware, managed commensurate with the assessed risk of unauthorized access. More simply, anyone not supposed to access an OT resource doesn't get access.

There are six subcategories in the PR.AA section:

PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization

PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions

PR.AA-03: Users, services, and hardware are authenticated

PR.AA-04: Identity assertions are protected, conveyed, and verified

PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties

PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk

The PR.AA requirement, often called Secure Remote Access (SRA) to the OT network, is frequently the most significant driver for investment in the CSF's Protection function. However, it is also the biggest weakness in many organizations' OT cybersecurity framework, primarily due to the use of passwords. Let's look at each requirement individually since secure remote access is essential to achieving a desirable protection outcome.

PR.AA-01:
This is simple – only the organization can determine who should access which resources. That doesn't mean you cannot leverage external services; only the organization can approve the identities and credentials for access. The desired outcome is that the organization knows who and what is to be permitted access to their OT network.

PR.AA-02:
This requirement has been the biggest failure within the Protect function of the CSF. The binding between an identity and credentials has meant for a very long time in the cybersecurity space as a username and password. However, with some reports claiming that 90% of all successful attacks begin with a phishing email and 59% of users reuse passwords on multiple sites, it is logical to conclude that passwords are unsuitable for modern cybersecurity. Even the attachment of Multi-Factor Authentication (MFA) to password authentication is insufficient, as significant weaknesses with MFA bombing, session hijacking, and SIM swapping attacks are well known. The desired outcome is to tie an identity (who you are) with credentials (what you have and know) in the context of what resources you are trying to gain access to in the OT network. We will discuss this requirement in detail later, as it is a linchpin of a successful protection outcome.

PR.AA-03:
This is also a simple requirement – all users, services, and hardware must be authenticated on the OT network. There are nuances to this requirement, but the desired outcome is that neither users nor devices achieve unauthorized access.

PR.AA-04:
This requirement refers back to the comment in PR.AA-01 about the use of external services. Suppose you are going to rely on an external service. In that case, an organization needs to ensure that the response from an identity provider is protected (properly authenticated and not tampered with), conveyed (encrypted with non-repudiation), and verified (the user should be allowed access) before any access to the network. Discipline leads to the desired outcome: an unauthenticated user obtains visibility into the network only after authentication.

PR.AA-05:
This requirement seems straightforward until the last clause. Defining, documenting, managing, enforcing, and reviewing a policy is easy. The twist that defines the desired outcome is the incorporation of least privilege and separation of duties because it introduces specific requirements for access and network segmentation to restrict access for authorized users to specific resources.

PR.AA-06:
In the cybersecurity context, any requirement for physical security is often overlooked. From a cybersecurity risk management perspective, the desired outcome for this requirement is that even if a device is compromised, its ability to enable lateral movement and access to other resources should be minimal.

Awareness and Training (PR.AT):

The desired outcome for PR.AA is that access to physical and logical assets is limited to authorized users, services, and hardware, managed commensurate with the assessed risk of unauthorized access. More simply, anyone not supposed to access an OT resource doesn't get access.

There are two subcategories in the PR.AT section:

PR.AT-01: The requirement that personnel be provided with awareness and training to ensure they possess the knowledge and skills to perform general tasks while considering cybersecurity risks is straightforward. The desired outcome is minimal risk even if the personnel fail to perform their functions securely.

PR.AA-02: Individuals in specialized roles are provided with awareness and training to possess the knowledge and skills to perform relevant tasks while considering cybersecurity risks. The desired outcome is a properly managed OT network with minimal to no misconfigurations.

Data Security (PR.DS):

Data integrity is critical in OT networks. Many monitoring and safety systems need to respond to changes in behavior in less than one second to ensure public and personnel safety, so data protection in all of its stages (at rest, in transit, in use, and backup) is essential – data kept locally and data accessed remotely.

Unlike IT, the criticality of this data is paramount because the values often represent mission-critical information, not just someone's email, as in an IT scenario. In the OT world, the remote aspect of monitoring is becoming more crucial, especially in verticals like oil and gas, energy, and manufacturing. If hackers block data streams or modify values coming from sensors to the monitoring systems, the entire operational chain can be disrupted, damaged, or destroyed. Changing sensor values in a water treatment plant may cause wastewater to leak into the water supply. Changing sensor values in a chemical manufacturing plant could cause an explosion. Changing sensor values in a manufacturing plant could cause employees to be injured or killed.

The requirements for data security are simple. Data is managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

The four requirements given are::

PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected. Any system that stores data requires protection from unauthorized access or modification. The desired outcome should be that no unauthorized personnel can access these systems, and no authorized personnel can modify the data without logging their changes.

PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected. Any system transmitting data should ensure that its streams cannot be modified in flight. Ideally, this means data encryption from end-to-end, but this is only sometimes possible in legacy systems that do not support encryption. In these scenarios, the minimum requirement is that any data that leaves a protected enclave should be encrypted to its destination, meeting the desired outcome that these critical values are not modified in flight by a bad actor. It is also vital to note that not all data in the OT network can be encrypted. In many cases, the delay in encrypting the data would introduce more risk to the system (think real-time monitoring), so selecting technology to protect enclave-to-enclave traffic should introduce minimal latency. The desired outcome is that if data is not encrypted, the path between the systems should not be easily "snoopable" and not susceptible to man-in-the-middle attacks.

PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected. An example of this might be malware like Stuxnet, whose entire purpose was to modify the values of active software to cause damage. The desired outcome for this requirement would be to prevent any critical system compromise to the point where a hacker could change data values stored in memory or the CPU of an active system.

PR.DS-11: Regular data backups must be created, protected, maintained, and tested. Similar to the DS-10, the desired outcome is to ensure that a backup system does not fall under the control of a bad actor. In the backup scenario, a bad actor could not only manipulate the data in the system but could cover their tracks by modifying the backup, making it nearly impossible to conduct forensic analysis on a hack.

Platform Security (PR.PS):

Platform security is an interesting challenge for OT networks. The requirement is that the hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed in a manner consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability. Unlike IT, where the upgrade cycles are 3-5 years, and the update cycle is almost weekly, OT systems can last decades and never get software updates. Unpatchble OT systems require shielding to prevent risk and compromise.

Rather than address these requirements individually, we will list them and use a blanket protection strategy to cover the entire section.

There are six subcategories in the PR.PS section:

PR.PS-01: Configuration management practices are established and applied

PR.PS-02: Software is maintained, replaced, and removed commensurate with risk

PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk

PR.PS-04: Log records are generated and made available for continuous monitoring

PR.PS-05: Installation and execution of unauthorized software are prevented

PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle

To achieve the desired outcomes for the above requirements, the easiest method is to prevent anyone other than the operator and the system controllers from accessing these devices. Protection is accomplished through secure remote access and tight network segmentation controls to avoid lateral movement from within the OT network by unauthorized local users. In today's remote OT environment, creating a completely air-gapped network is nearly impossible, so instead, create a virtual air gap for all but authorized users.

Technology Infrastructure Resilience (PR.IR):

Like platform security, infrastructure resilience can be considered an overarching requirement. The organization must manage the security architectures with a risk management strategy to protect asset confidentiality, integrity, availability, and organizational resilience. The desired outcome is that the OT network remains available and operational.

There are four subcategories in the PR.IR section:

PR.IR-01: Networks and environments must be protected from unauthorized logical access and usage. Although this sounds straightforward, some nuances can be inferred (and should be) from this simple requirement. None of the requirements explicitly address firewalls, network segmentation, or air-gapping networks. This requirement is the place where general network protection comes into play. The desired outcome is that the OT assets are protected from network access by exploiting logical (Layer 2 or Layer 3) access or privilege escalation within accounts.

PR.IR-02: This requirement mandates that an organization's technology assets be protected from environmental threats. However, secondary and unspoken is to infer that the systems controlling the environment where the OT assets operate should also be protected. For example, ensure that the cooling system of a data center that houses servers is appropriately protected to the same level that the servers themselves are protected. There is also an unspoken requirement that deployed hardware can handle the environmental conditions. The desired outcome is that the systems continue to operate because they are protected environmentally from heat, cold, dust, etc.

PR.IR-03: In all networks, bad things happen sometimes. This requirement dictates that the OT network has implemented mechanisms to achieve resilience requirements in every day and adverse situations. This could be as simple as deploying redundancy (N+1 usually), multiple links between systems, and backup connectivity for critical systems. The desired outcome is that if systems fail or something happens to the network, operations can continue at an acceptable level, even if degraded.

PR.IR-04: One of the most common hacker techniques is to launch DDOS attacks at sites that overwhelm the security systems or the links connecting the location to the Internet. This requirement ensures adequate resource capacity is deployed to maintain availability even when the network is under severe stress. Again, the desired outcome is keeping the network operating for critical resources, even when under attack.

Operational Considerations: Simplicity

Although not a formal requirement, it is critical to note that one of the key differences between IT and OT is that security is often a "side job" for OT personnel. Any solution deployed must be simple and not require extensive maintenance and tweaking.

Changes in the network security configuration should be easy to describe and implement. Network segmentation (and microsegmentation) should be software-controlled and easy to configure. Since misconfigurations often cause successful cyberattacks and breaches (Upguard reported 80% in 2023, and Zscaler reported 68% in 2022), keep configuration management simple and intuitive for OT environments. It is not enough to point at the Training requirements and claim compliance – hold the systems used to protect OT networks to a higher standard – industrial-grade security with consumer-level ease of use. PR.AT-02 references training for specialized employees, but it is worth restating that the more complicated a cybersecurity solution is and the more it bundles into a single solution, the higher the likelihood of misconfiguration and errors and the higher the risk for the organization.

PR Summary Desired Outcomes Table

Category Identifier	Category	Desired Outcome
"Identity Management, Authentication, and Access Control"	**PR.AA-01**	The organization knows who and what is permitted access to their OT network.
	PR.AA-02	Tie an identity (who you are) with credentials (what you have and know) in the context of what resources you may access.
	PR.AA-03	Neither users nor devices achieve unauthorized access to any OT resources.
	PR.AA-04	Grant visibility to a user only after authentication.
	PR.AA-05	Incorporate least privilege and separation of duties through network segmentation to restrict access for authorized users to specific resources.
	PR.AA-06	Prevent the ability to move laterally even if a device is compromised.
Awareness and Training	**PR.AT-01**	Minimize risk even if personnel fail to perform their tasks securely.
	PR.AT-02	Minimize misconfigurations.
Data Security	**PR.DS-01**	"No unauthorized personnel can access these systems, and no authorized personnel can modify the data without logging their changes."
	PR.DS-02	Protect critical OT datastreams to prevent the modification of values in flight.
	PR.DS-10	The path between the systems should not be easily "snoopable" and not susceptible to man-in-the-middle attacks. It should be encrypted where possible (which is not always possible in OT).
	PR.DS-11	Ensure that a bad actor cannot access and control a backup system.
Platform Security	**PR.PS-01**	Prevent anyone other than the operator and the system controllers from accessing or modifying these devices.
	PR.PS-02	Prevent anyone other than the operator and the system controllers from accessing or modifying these devices.
	PR.PS-03	Prevent anyone other than the operator and the system controllers from accessing or modifying these devices.
	PR.PS-04	Prevent anyone other than the operator and the system controllers from accessing or modifying these devices.
	PR.PS-05	Prevent anyone other than the operator and the system controllers from accessing or modifying these devices.
	PR.PS-06	Prevent anyone other than the operator and the system controllers from accessing or modifying these devices.
Technology Infrastructure Resilience	**PR.IR-01**	OT assets are protected from network access by exploiting logical (Layer 2 or Layer 3) access or privilege escalation within accounts.
	PR.IR-02	OT assets are protected from network access by exploiting logical (Layer 2 or Layer 3) access or privilege escalation within accounts.
	PR.IR-03	OT assets are protected from network access by exploiting logical (Layer 2 or Layer 3) access or privilege escalation within accounts.
	PR.IR-04	OT assets are protected from network access by exploiting logical (Layer 2 or Layer 3) access or privilege escalation within accounts.

Any solution deployed must be simple and not require extensive maintenance and tweaking.

Protection Solutions

To determine what we need to do to protect against OT cyber threats, let's go back to our desired outcomes:

1. The OT cybersecurity protection solution network must prevent external intrusion or internal attacks from affecting OT network operations.

2. Remote Access must be tightly controlled to the OT network because almost all access is remote access for OT.

3. The OT domain must be separated from the IT domain to prevent spillover attacks and drastically reduce risk from highly vulnerable IT systems and remote access.

4. The OT network must be microsegmented to reduce the risk of lateral movement by insider or physical access threats.

5. Deploying protection must be minimally disruptive or intrusive into data flows and operational processes to reduce operational impact and lost productivity.

What approaches to meeting these desired outcomes are being offered to OT network administrators to meet their needs?

Summary of Protection Capabilities

On the market today, OT administrators are faced with four main options when choosing an OT Zero Trust Protection solution. The table introduces the solutions, and we explore each solution in more detail in this section..

Table:
OT Zero Trust Protection Solution Options

Solution Type	Description	Meets Desired Outcome	Fails Desired Outcome
Next Generation IT Firewall/VPN	Multiple boxes used to protect IT network repurposed for OT	"1,2,3 (However, costly, complicated, and prone to vulnerabilities)"	4 (Requires network re-architecture and downtime)
Virtual Air Gap	Protected enclaves with site-to-site VPNs	"1,3,4 "	"2 (Typically no secure remote access included in VA solutions) 1,3 (Typically does not segment OT network east-west)"
Privileged Access Management (PAM)	Proxy remote access solution	"1,2,3"	"1,3 (Typically does not segment OT network east-west or protect from internal attacks) 4 (proxy is intrusive, adds latency, and protocol dependent)"
Comprehensive Protection	"Network protection, secure remote access, and microsegmentation"	"1,2,3,4,5"	

Technology Infrastructure Resilience (PR.IR):

The first and largest competitors are the legacy IT vendors (Cisco, Palo Alto, Fortinet, and Juniper) selling firewalls and IT VPN solutions. OT administrators repurposed them to protect OT networks since they were already in their network, but these solutions have failed to protect OT networks. Since they are also used to protect the IT network, any vulnerabilities give hackers a free pass to move into the OT network laterally. The failure of existing IT solutions to protect OT networks has led to the creation of new OT Zero Trust Protection solutions.

Privileged Access Management (PAM) Solutions

The next class of competitors are Privileged Access Management (PAM) solutions that deliver cloud-based proxy SSL VPNs to access OT networks. They also often depend on cloud architectures, which increase costs for these competitors, add significant latency, and open up new attacks and denial of service vulnerabilities. They also are intrusive to the customer, as they either proxy the protocols used in OT or simply offer remote desktop solutions, introducing latency and adding performance challenges for remote sites. They also do not typically protect within secure OT enclaves for east-west traffic (i.e., between devices), so no insider threat protection is provided.

Air Gap and Virtual Air Gap Solutions

The next class of competitive threats is from Virtual Air Gap solutions that are scaled-up versions of data diodes, one of the first attempts to allow OT devices to connect to the internet safely. These solutions are site-to-site VPN solutions that encrypt traffic between enclaves and do not allow users to access a segment unless they come from another secure segment. The biggest weakness of this solution is that it requires a separate Secure Remote Access solution, so they are not a complete solution for a customer. They also do not typically protect within secure OT enclaves for east-west traffic (i.e., between devices), so no insider threat protection is provided.

Comprehensive Protection Solutions

The final category is Comprehensive Protection. This category combines network protection (Network Cloaking), Secure Remote Access (SRA), and software-defined Microsegmentation. These solutions are the natural replacement for the legacy firewall and VPN solutions designed for OT networks. Comprehensive solutions meet all of the Cybersecurity Framework requirements and the desired outcomes for OT. These solutions also block the remote classes of risk identified by the MITRE ATT&CK framework, drastically altering the Return on Mitigation equation for OT networks and delivering the highest ROI by stopping most attacks before they can begin.

The Optimal OT Zero Trust Solution

What components must a comprehensive Zero Trust Protection solution have to mitigate risks and meet the NIST CSF requirements?

CSF Function	Network Cloaking	Secure Remote Access	Microsegmentation	Operational Simplicity
PR.AA	Prevent access by hackers	Control Access to only authorized personnel	Enforce Least Privilege and prevent lateral movement	"Complexity breeds shortcuts, leading to undocumented vulnerabilities"
PR.AT	To hide vulnerabilities in case of training or policy failures	To limit access to authorized personnel and limit access in case of credentials theft	To limit exposure when users fail to protect themselves	"Complexity breeds shortcuts, leading to undocumented vulnerabilities"
PR.DS	"Limit external risks for monitoring or snooping for data-at-rest, data-in-transit, and data-in-use"	"Limit data-at-rest, data-in-transit, data-in-use by limiting access"	Limit data-in-transit and data-at-rest risks by enforcing least privilege	"Complexity breeds shortcuts, leading to undocumented vulnerabilities"
PR.PS	Prevent external visibility or access to critical systems	Allow only authorized access to OT systems	Prevent lateral movement by authorized personnel to unauthorized systems	"Complexity breeds shortcuts, leading to undocumented vulnerabilities"
PR.IR	"Prevent external attacks from penetrating OT network (DDOS, scans, etc.)"	Allow only authorized access to OT systems	Prevent lateral movement by authorized personnel to unauthorized systems	"Complexity breeds shortcuts, leading to undocumented vulnerabilities"

Returning to the MITRE ATT&CK ICS matrix, we can now evaluate risk mitigation with a comprehensive OT Protection Solution.

If you analyze the overall ATT&CK ICS Framework, comprehensive protection can block 84 out of 90 tactics – a massive win for any OT Cybersecurity Deployment.

	Complete Protection	Persistence	Privilege Escalation	Evasion
Initial Access	8	3	1	12
Execution	0	9	0	9
Persistence	2	4	0	6
Privilege Escalation	0	2	0	2
Evasion	4	1	1	6
Discovery	5	0	0	5
Lateral Movement	7	0	0	7
Collection	9	0	1	10
Command and Control	3	0	1	3
Inhibit Response Function	0	12	1	13
Impair Process Control	0	4	1	5
Impact	0	12	0	12
TOTAL	**38**	**47**	**6**	**90**

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	**9 techniques**	**6 techniques**	**2 techniques**	**6 techniques**	**5 techniques**	**7 techniques**	**10 techniques**	**3 techniques**	**13 techniques**	**5 techniques**	**12 techniques**
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	"Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Comprehensive Zero Trust Protection Key Technologies

Earlier, we focused on several key MITRE ICS ATT&CK vectors: Discovery, Initial Access, Privilege Escalation, and Lateral Movement. Since our desired outcome is to block these attack vectors from remote attacks, let's investigate the technology needed to prevent them from succeeding in your network.

Network Cloaking

At the foundational level, Network Cloaking starts with a firewall's capability to block access to protocols and ports. However, the central tenet of Network Cloaking is more like the policies you would see on a VPN box; only a single port is open (for remote access requests). All other ports are not just blocked; traffic to those ports is silently dropped on the floor as if it did not exist. Like wearing a black cloak hides anything you have on underneath, a network cloak prevents a hacker from seeing what is on your network. A better analogy for network cloaking is more like an invisibility cloak that can only be seen from a particular vantage point (in this case, with a valid PKI authentication request). A hacker doesn't even know that you are there, so they can't attack or formulate a method to attack you if she doesn't know there is a target there. This capability stops Discovery, preventing hackers from successfully mapping your network or discovering your vulnerabilities.

Also, like a firewall, Network Cloaking can hide private IP addresses behind a single public IP address and perform Private-to-Public Network Address Translation. However, in the OT market, Network Cloaking acts like a Virtual Air Gap system or Data Diode, preventing internal devices from talking to the internet directly (You can allow it, but it is not desirable). Unlike most firewalls, however, you can use that NAT functionality to further protect a system from other internal systems by performing Private-to-Private NAT – forcing even internal traffic to pass through the cloak to reach the protected system (even if connected to the same Layer 2 network and switch). NAT provides another cloaking layer by hiding private addresses from internal systems. It makes lateral movement much harder by forcing it through the cloaking gateway or reducing access to physical access alone.

Network Cloaking is a perfect first line of defense for OT networks. You can attack it all you want; it won't do any damage, and you can't determine the vulnerabilities. It also performs a targeted version of NAT by "moving" IP addresses around to protect systems with enhanced NAT capabilities, delivering Layer 2 lateral movement protection.

Secure Remote Access

Secure Remote Access for OT is more like a medieval castle and moat problem than how IT handles Remote Access. Since OT has a more limited "need-to-access" than IT and very little "need-to-exit," administrators can build a fortress around the OT network and let in only the good guys. The foundation of Zero Trust is "Trust no one." Secure Remote access starts with the premise that unauthenticated users should not obtain network visibility (See network cloaking above). Unlike firewalls that let in entire protocols (like SSL), no traffic can enter or exit an OT network unless encrypted and authenticated. However, IT remote access isn't always very secure. Today, it is easy to pretend to be someone online, steal that password, or social engineer your way into many networks. Passwords should no longer be a method accepted in OT Secure Remote Access. Even simply turning on MFA is often not good enough because of MFA hijacking and bombing.

True Zero Trust Secure Remote Access can be built today for critical infrastructure networks. For the crucial part of your network, create a moat and only leave a single entrance that isn't vulnerable to impersonation or stealing credentials. Rely on verified identities and devices for access, not traffic identification. Minimize your CISO's worries by forcing attacks down a single path and reducing the attack and reconnaissance noise. Rely on biometrics and device IDs, not usernames and passwords. Avoid browser-based authentication that is vulnerable to session hijacking.

Following this strategy ensures that Initial Access is secured and cannot be exploited by hackers to gain access. Even if they do, protecting against privilege escalation and lateral movement blocks their access.

Software-Defined Microsegmentation

One point that NIST makes in its strategy documents is that segmentation protects against external and insider threats. Many people focus on external threats and often forget internal threats when designing OT security solutions. Internal threats can be internal employees and temporary contractors who can access the network for maintenance or ongoing management tasks. Microsegmentation moves access to the "least privilege" minimum by limiting what a user can access on the network, even if access is allowed.

Here are the key questions to explore to determine how microsegmentation needs to work in your network:

1. **What devices need to be able to communicate? Are any of these devices vulnerable to known exploits, or have they previously had issues?**
   If they are, you should segment this class of devices from others. Since they are vulnerable, they could laterally move on your OT network and increase the scale of havoc that could be wreaked during an attack.

2. **Do you have any contractors accessing the network?**
   If you do, then you should microsegment the sections of the network that they can access to protect the network from being exploited by these contractors. Remember the Target hack that started with HVAC contractors?

3. **How secure is your Remote Access? Does it use MFA that you trust?**
   If your remote access uses passwords (even if they are SSO and MFA supported), you should microsegment your network as much as possible. Many hacks and attacks begin with credentials theft (including MFA bombing, MFA hijacking, etc.), and you should probably microsegment if there is a single password in your chain.

4. **Can unauthorized devices get on your network?**
   Suppose it is trivial for a bad actor to gain access to your layer two networks through WiFi or even a physical plug. In that case, you should microsegment since a hacker could use this to move throughout the network laterally. Although this seems like a strange question that no one would ever answer yes to….you might be surprised at the answers you get when administrators are honest.

At the end of the day, unless there is a technical reason (like latency, no managed switching infrastructure, or zero tolerance for even milliseconds of downtime), OT networks should have some microsegmentation, and usually, the more the merrier. It isn't unreasonable in some networks to segment every device for protection.

Solutions are available that can create software-defined microsegmentation, even on existing Flast Layer 2 networks. This solution is ideal for OT networks to minimize downtime and remove any requirement to re-architecture the network. By microsegmenting down to the device level, privilege escalation and lateral movement are largely blocked, and insider threats can be limited.

Let's evaluate the most severe ROM vulnerabilities and what Zero Trust solution is required.

ROM Severity	Issues Found	% Customers w/ Problem	Zero Trust Solution
15	No advanced MFA protection mechanisms enabled		Protect: Secure Remote Access
15	Poor user lifecycle management	21%	Governance
15	Lack of EDR coverage	13%	Detection
15	Lack of detection controls	10%	Detection
13	Resource exposed to public access	2%	Protection: Network Cloaking
12	Insufficient protections for local accounts	60%	Protection: Secure Remote Access
12	Missing security barrier between cloud and on-premise	54%	Protection: Network Cloaking
12	Insecure Active Directory configuration	43%	Protection: Secure Remote Access, Network Cloaking
12	Insufficient device security controls	8%	Protection: Network Cloaking, Microsegmentation
11	Legacy cloud authentication is still used	47%	Protection: Secure Remote Access
11	No advanced password protection is enabled	37%	Protection: Secure Remote Access
11	Missing content-based MFA protection mechanisms	24%	Protection: Secure Remote Access
11	Insecure operating system configuration	3%	Protection: Network Cloaking

BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to www.blastwave.com

v20250624

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499