WHITEPAPER

TRUEFORT®

Take the Purdue Model to the Next-level with Microsegmentation

Bring Zero-Trust Security to OT: Use Microsegmentation to Take the Purdue Model Next-level and Secure Operational Technology Infrastructures and Industrial Control Systems

TRUEFORT.COM

Introduction

The physical security and cybersecurity issues that have plagued IT environments in other industries are now becoming challenges for operational technology (OT) infrastructures.

The security postures on which OT and industrial control systems (ICS) professionals have relied do not provide sufficient asset visibility in relation to the application-mesh and cannot secure their environments as they integrate new edge computing platforms. As more enterprises demand that new technologies designed to drive efficiency become part of their infrastructures, OT owners and ICS professionals must address the security threats they pose. OT and IT must share the responsibility for securing OT infrastructures and ICS. To implement a zero-trust security model in OT and ICS environments, security teams must think differently about overcoming new challenges.

In this white paper, we present data showing that enterprises will integrate new technologies into OT environments at an accelerated pace. As OT and ICS owners bring on new technologies, the convergence of IT and OT/ICS will elevate threat concerns in their environments and expose the growing need to secure them effectively. We will review how a typical OT infrastructure/ICS security posture works today using the Purdue Model. You will learn how cyber risks are different in OT and IT environments, and see an overview of existing and emerging threats facing OT/ICS. We will demonstrate how OT and ICS professionals should approach the challenges of onboarding. This approach must focus on both providing security for current OT infrastructures from unauthorized traffic and exploits, and on enabling OT and ICS professionals to gain the visibility required in the larger environment to create a true zero-trust security posture.

We will further explain the importance of gaining asset visibility and understanding, and why it is essential to an OT security program. You will see how TrueFort's microsegmentation solution, real-time application behavioral mapping, and enforcement, works to secure industrial OT and IoT use cases. We will demonstrate how this ensures your existing OT infrastructure secures throughput on the factory floor, and maintains the safe operation of factory floor equipment. We will also explain the ongoing benefits of using the TrueFort Platform to help create a zero-trust security posture for your OT environment.

What the future holds for industry and what it means to OT and ICS

As the need grows to onboard new technology to make industries more efficient, OT devices that have historically worked in isolation must now connect to IT networks and solutions. This includes the cloud, servers, and baseline security measures like firewalls.

A 2021 report revealed that over 90 percent of OT organizations experienced cyber incidents in the prior 12 months. In a survey of 100 manufacturing, energy and utilities, healthcare, and transportation sector OT professionals working in organizations with more than 2,500 employees, more than half reported the cyber incidents they experienced resulted in an operational outage that affected productivity. Forty five percent also said that these incidents resulted in an operational outage that put physical safety at risk. From a cyber security perspective, only 4% of respondents said they were prepared to onboard these new technologies. While connectivity between IT and OT has been increasing over the recent past, over 70% of respondents assert that the pandemic accelerated OT-IT convergence. It seems that organizations have a great deal of work to do in order to shore up their OT strategies against cyber incidents. This is a worrying prospect; one analyst predicts that by 2025, cyber attackers and nation state bad actors will have successfully weaponized operational technology environments to successfully harm humans.

The number of OT connected systems and devices is surging. This encompasses everything from supervisory control and data acquisition (SCADA), manufacturing execution systems (MES), discrete process control (DPS), programmable logic controllers (PLCs), telematics, robotics, and even personal technologies such as the Internet of Medical Things (IoMT). As networking, remote management, and wireless connectivity have become principal drivers of performance efficiencies, production boosts, and better margins for industry, OT stopped being the safe place it has always been. In the future, many OT industry professionals believe that worrying about problems from the IT world will be the “new normal” for OT security specialists.

> More than half reported the cyber incidents they experienced resulted in an operational outage that affected productivity.

The Purdue Model: An overview

The Purdue Model is a widely used framework for designing and implementing industrial control systems (ICS) security. It was developed in the 1990s by the Center for Information Systems Security Studies and Research (CISR) at Purdue University.

The Purdue model provides a hierarchical structure for ICS architecture that helps to organize the various components of an ICS and enables security professionals to implement appropriate security measures at each level. It serves the segmentation requirements for both wireless and wired networks and protects the operational technology (OT) infrastructure from unwarranted traffic and exploits.

The Purdue Model for Industrial Control System (ICS) Security

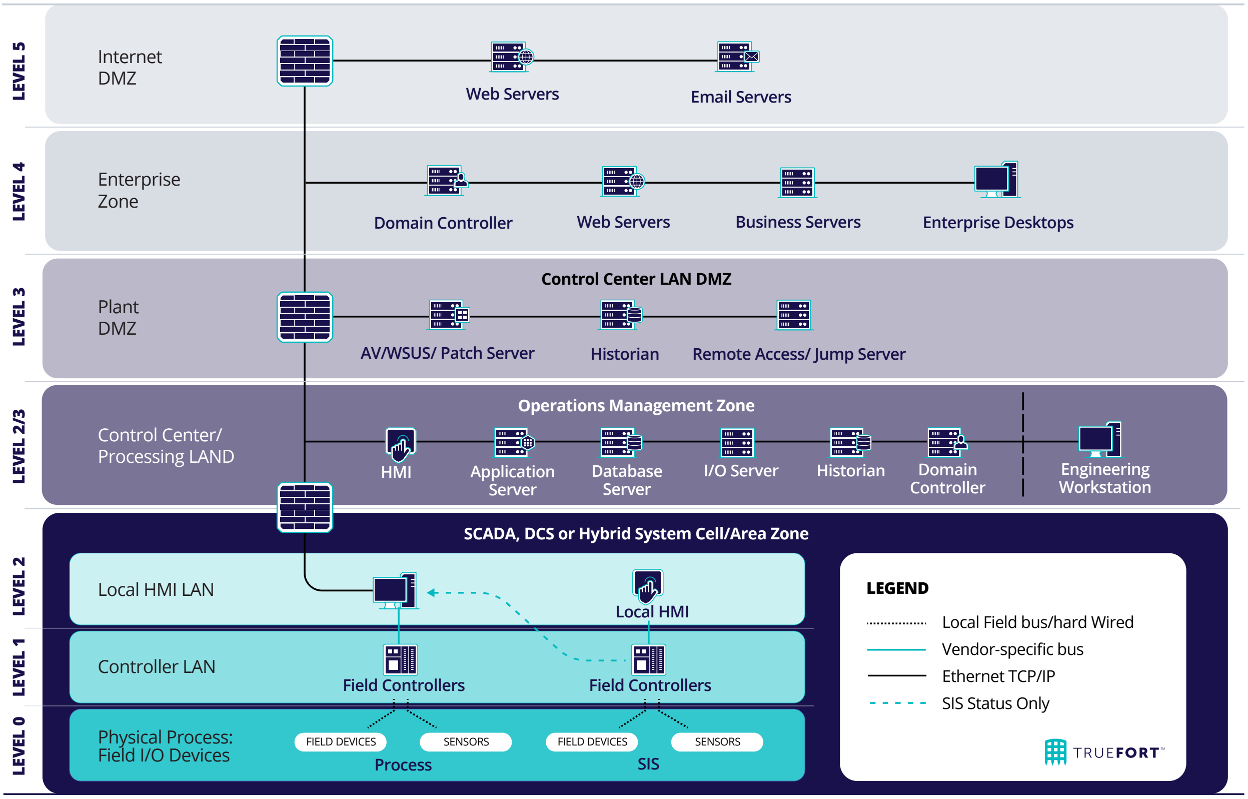

FIGURE 1: A layered illustration of the Purdue Model for Industrial Control System (ICS) Security

Purdue Model **Levels**

LEVEL 0

comprises the physical devices that form the foundation of the products, such as motors, pumps, sensors, and valves.

LEVEL 1

consists of systems that supervise and direct the devices at Level 0, including Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Intelligent Electronic devices (IEDs).

LEVEL 2

involves devices that manage the overall processes of the system, such as human-machine interfaces (HMIs) and SCADA software, which enable human operators to monitor and control the system.

LEVEL 3

facilitates the management of production workflows and includes batch management, manufacturing operations management (MOM), manufacturing execution systems (MES), and data historians. The Industrial Demilitarized Zone (IDMZ) serves as a buffer between the IT and OT networks. The iDMZ helps prevent infections within the IT environment from spreading to OT systems and vice versa.

LEVEL 4

encompasses systems such as Enterprise Resource Planning (ERP) software, databases, email servers, and other logistics-related systems that manage manufacturing operations and provide communication and data storage.

LEVEL 5

is the enterprise network, which is not an ICS environment but collects data from ICS systems for business decisions.

The Purdue Model provides a clear and logical structure for implementing security measures in ICS. For example, firewalls and intrusion detection systems can be implemented at the Supervisory Level to protect SCADA systems, while access controls and authentication mechanisms can be implemented at the Control Level to protect programmable logic controllers (PLCs) and distributed control systems (DCS).

How the evolution of OT environments and ICS is challenging the Purdue Model

As the previously cited research has suggested, a growing number of OT owners and ICS professionals are now compelled to adopt industrial edge computing and leverage its value.

They need to do this while still ensuring their industrial control systems (ICS) adhere to each level in the Purdue Model. They still need to segment off wireless and wired environments to protect the OT environment or infrastructure. The process of adopting industrial edge computing platforms creates discrete security concerns in both IT and OT environments. OT owners and ICS professionals must re-work their toolsets to achieve zero-trust security in this rapidly evolving space.

As cyber threats from the IT world present greater challenges to OT security specialists, they must identify new tools and processes necessary to achieve the goal of establishing and maintaining sufficient OT asset visibility. Cyber risks and operational approaches in OT are very different than those in IT, so understanding how asset visibility, threat visibility, and vulnerability management are realized in IT environments is key to creating a new way to achieve OT visibility.

> Understanding how asset visibility, threat visibility, and vulnerability management are realized in IT environments is key to creating a new way to achieve OT visibility.

Cyber Risks IT vs OT

Manage Information Servers,laptops, mobile devices, cameras, point-of-sale devices	**SYSTEM TYPES**	**Operate Physical Processes** PLCs, RTUs, HMIs that run actuators, sensors and valves
Patch/update software	**MANAGE VULNERABILITIES**	Patching production systems means plant or system shutdown; needalternatives
DNS, HTTPS, RTP, MP4 video	**NETWORK TRAFFIC**	Hundreds of industrial system communications protocols
Loss of data,intellectual property, network services	**MAJOR INCIDENT IMPACT**	Loss of electrical grid, pipeline or plant operations; loss of control safety system

Dragos - *Why OT Visibility Is Crucial for Industrial Cybersecurity*

Unfortunately for OT owners, managing these risks during the movement to adopt technologies like industrial edge computing is not as simple as deploying visibility tools from the IT world. Current IT asset visibility approaches are not compatible with the OT environment and IT vendors don't manage OT protocols well enough. Also, IT visibility tools perform platform scanning for asset discovery that can disrupt OT processes and it's hard for them to manually inventory geographically dispersed facilities.

Owners in OT environments often choose to risk threat exploitation because applying patches could create system stability disruption and result in critical downtime, or may even void the software warranty. This is especially true when there is not enough context about the risk. Even when the risk of patching is acceptable, organizations often must get approval from OT vendors before patching. OT systems often operate months or even years before a window presents itself for maintenance and patches; and in general, there is not much information about alternative threat mitigation approaches.

It is also very difficult for OT owners to assess vulnerability risk and detect threatening behavior based on how other organization's environments were exploited. In dynamic environments, maintaining a platform configuration that supports reliable anomaly detection is hard to do. When adopting industrial edge computing technology, limited asset visibility and coverage makes anomaly detection in OT environments insufficient using current tools.

Current threat groups targeting OT systems

Dragos reports that there are twenty threat groups that have been targeting organizations with ICS or other OT environments. Here are a few of the most high-profile:

Threat name	Targeted industries	Capabilities	Infrastructure	Main impact
CHERNOVITE'S PIPEDREAM	First known threat with cross-industry disruptive/destructive ICS/OT capability.	PLC credential capture. Brute force password cracking and DoS attacks. Malware can disrupt, degrade, and potentially destroy physical processes in industrial environments.	Unknown	Exposed information about victim's OT network architecture and assets; manipulation and disruption of processes.
BENTONITE	Maritime oil and gas, governments, and manufacturing.	Runs multiple, concurrent operations. Multi-stage downloaders, victim enumeration, reconnaissance and C2 capabilities and vulnerability exploitation.	Credential harvesting. Separate domains for phishing and C2. Utilizes Github for delivery, SSH and HTTP for C2.	Espionage, data exfiltration, and IT compromise.
KOSTOVITE	Global energy companies in North America and Australia.	Uses highly customized web shells and zero-day exploits to access target's OT networks and devices.	Compromises home and small business IoT devices exposed to Internet as well as enterprise perimeter devices.	Intrusion into victim's OT networks and devices.
KAMACITE	Electric, natural gas, and food and agriculture (manufacturing, processing, and storage)	Gains initial access through phishing and credential replay. Custom malware development and deployment; can modify third party criminal malware.	Spoofs legitimate technology and social media services.	Operational disruptions such as large-scale power outages.

Threat name	Targeted industries	Capabilities	Infrastructure	Main impact
XENOTIME	Liquefied natural gas and oils and gas operations.	Only threat group that has demonstrated it can compromise and disrupt industrial safety instrumented systems, which can lead to environmental damage, loss of containment and control, and loss of life.	Virtual Private Server and compromised, legitimate infrastructure.	Disruption and possible destruction of critical infrastructure, particularly in the oil and gas sector.
ELECTRUM	Electrical grid.	Unique RAT and malicious wiper modules.	Leverages servers hosting many additional services such as Tor.	INDUSTROYER2 malware deployed with wiper malware manipulates electric transmission equipment.
ERYTHRITE	Manufacturing, electrical utilities, food and beverage companies, automotive, IT service providers, and oil and natural gas.	Search engine optimization poisoning; bespoke, rapidly refashioned low detection credential stealing and remote access malware.	Reverse proxies in North America and Europe, hundreds of thousands of vulnerable but otherwise legitimate websites abused for SEO poisoning.	Credentials, sensitive information, and remote access to OT environments can be sold to illicit third parties.
WASSONITE	Nuclear energy, electric, oil and gas, advanced manufacturing, pharmaceutical, and aerospace.	Leverages spear phishing lures as the initial infection vector. Malware displays highly targeted modifications for individual environments, including hard-coded credentials, non-public IP addresses, and uncommon ports for specific applications.	Adversary-registered and controlled domains and infrastructure for C2. Use of compromised, legitimate services in some instances.	Focus on network actions consistent with information gathering, including from protected network segments.

SOURCE: *Dragos - ICS/OT CYBERSECURITY YEAR IN REVIEW 2022*

Is the Purdue Model still relevant in this new environment?

The Purdue Model offers a hierarchical structure for industrial communications, fostering predictability in OT environments. However, with the evolution of OT and ICS security landscapes, and the emergence of well-known threats, the model reveals certain limitations.

In the modern industrial edge computing landscape, data can come from various sources and serve multiple clients.

This diversification breaks away from the traditional hierarchical data flow. As we infuse more intelligence into sensors, actuators (Level 0), and controllers (Level 1) within the Purdue Model, risks of system exposure multiply and occur much earlier than the model anticipated. Edge computing platforms are gaining popularity, enabling vast amounts of data collection at Level 1. This data can be processed and transmitted to the cloud, bypassing the model's hierarchical data flow structure and segmentation aspects. Given these circumstances, it's worth pondering:
Why should OT owners and ICS professionals continue to rely on the Purdue Model?

The Purdue Model still serves the segmentation requirements for both wireless and wired networks and protects OT platforms from bad traffic and potential exploitation.

OT owners must continue to maintain segmentation for traditional instances of IT and OT data flow to ensure the continuous flow of production, and the safety of workers operating equipment on the factory floor.

OT and ICS professionals can use a hybrid solution that preserves the essential functionality the Purdue Model provides, and introduces an industrial edge computing platform software layer to gain sufficient flexibility as industrial OT use cases become more prevalent and data become less hierarchical. Using this layer, OT owners can make new industrial edge computing projects adhere to each level in the Purdue Model.

This platform layer can sit either at Level 2 or Level 3 and provide data collection capability from OT devices at Level 0, 1, 2, and 3, while also facilitating data collection from IT layers at Levels 4 and 5. The benefit is that the traditional hierarchies inherent in the Purdue Model can be bypassed where needed (such as sensors sending data from Level 0 to Level 5) by piping the data through the platform to ensure control and security.

The first and most critical step in establishing and enforcing a zero-trust security posture in OT environments is achieving total asset visibility. When OT owners maintain constant and comprehensive visibility of their OT assets, they can uncover a variety of issues. These include previously undetected connectivity and communication channels, active threats that have been silently operating within their environment, insecure configurations, latent vulnerabilities, and unauthorized assets, among others. Fully identifying and inventorying OT assets makes the cybersecurity process easier at all levels; from leveraging threat detection, initiating incident response, actively managing assets for vulnerabilities and weaknesses, or implementing overarching strategic OT security initiatives. The hybrid solution described above accomplishes this.

> The Purdue Model still serves the segmentation requirements for both wireless and wired networks and protects OT platforms from bad traffic and potential exploitation.

TrueFort's microsegmentation and application behavioral enforcement layer

Integrating TrueFort's microsegmentation and application behavioral enforcement layer into the Purdue Model allows a hybrid approach to OT cybersecurity.

This strategy empowers OT owners to utilize industrial edge computing platforms, reaping all the benefits they provide. It enables the maintenance of application segmentation for both IT and OT data flow, while providing the necessary flexibility as industrial OT and IoT use cases increase. This becomes particularly important as data flows become less compartmentalized and more horizontally integrated.

This approach enables any OT owner to make their industrial development adhere to each level in the Purdue Model. The TrueFort platform security layer can sit either at Level 2 or Level 3 and provide application and workload enforcement and analysis capability from OT devices at Levels 1, 2, and 3, while also facilitating application data traffic enforcement and analysis from IT layers at Levels 4 and 5.

The benefit is that the traditional hierarchies inherent in the Purdue Model can be bypassed where needed (e.g., sensors sending data from Level 1 to Level 5) by piping application-controlled and microsegmented traffic data to the industrial edge platform for production analysis and optimization. The traditional Purdue Model data flows will continue to ensure throughPut on the factory floor. The existing network model will still protect and maintain the safe operation of factory floor equipment.

> Traditional hierarchies inherent in the Purdue Model can be bypassed where needed.

How the TrueFort Platform and real time application behavioural enforcement works

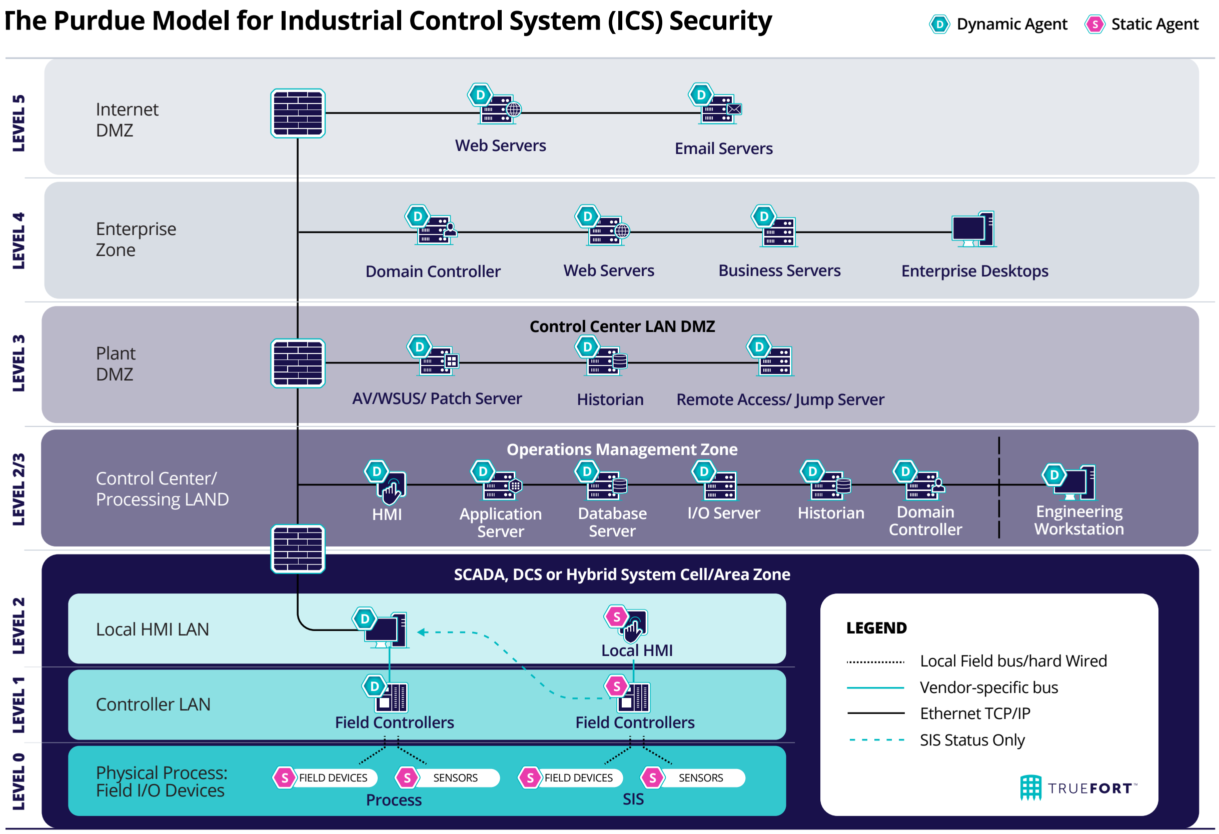
The Purdue Model for Industrial Control System (ICS) Security

FIGURE 2: The Purdue Model and the TrueFort Platform, for Industrial Control System (ICS) Security

Real-time application behavioural enforcement added on to the Purdue Model

- As shown in the image on the previous page, **TrueFort native agents (D – dynamic) and/or TrueFort passive agents (S – static, or agentless)** enforce intra and inter-application behavioral policies for hosts in OT and factory industrial environments and their applications to protect them.
- **Active agents (D)** control all bi-directional application traffic (to and from) all IP-based master controllers (HMI and SCADA) that support human interactions via VNC or MODBUS towards slave units such as PLC or PAC.
- **Passive agents (S)** control all application traffic sent from all IP-based slave units PLC, RTU, and Sensors that do not support native agent installation.
- **The OT control center and platform** is protected by TrueFort native agents (D) which enforce intra and inter-application behavioral policies for hosts and their applications.
- **The Corporate Edge (IDMZ)** - Factory Plant is protected by TrueFort native agents (D) which enforce inter and intra-application behavioral policies for hosts and their applications.
- **The Corporate HQ Core Network** is protected by TrueFort native agents (D) which enforce inter and intra-application behavioral policies for all hosts and their applications.
- **The Corporate HQ EDMZ Network** is protected by TrueFort native agents (D) which enforce inter and intra-application behavioral policies for all hosts and their applications.

What makes TrueFort Platform different?

TrueFort delivers discovery, understanding, and enforcement capabilities that enable complete asset visibility for data center and cloud applications and workloads.

This enables OT owners to:

1 **UNDERSTAND THE ATTACK SURFACE**

Traditional network security solutions cannot detect outside threats and compromised insiders or stop them from moving laterally through an OT environment. TrueFort's microsegmentation platform enables the visibility OT owners require to detect and remediate threats inside their environments.

2 **DISCOVER APPLICATIONS AND RESOURCES**

Most organizations don't know how servers and other workloads are used across their data center and cloud environments. TrueFort discovers and understands applications, users and their interactions with core systems and provides real-time behavioral insight into interactions; enabling users to determine the validity of the communication.

3 **IDENTIFY EXCESSIVE ENTITLEMENTS**

User and machine entitlements often contain unnecessary increased privileges that security teams rarely adjust or revoke. The TrueFort zero-trust approach to OT security prevents excessive access privilege and stops movement across the infrastructure when a privileged user is compromised.

4 **ENSURE OPTIMAL OPERATIONS**

Eliminating high-risk activity across workloads is a challenge without sacrificing application performance. The TrueFort microsegmentation platform applies zero-trust security rigor in a way that enables constant high-level operational performance.

Conclusion

One thing we know for certain: the drive to use industrial edge computing platforms and gain the benefits they offer in operational technology environments is not slowing down.

As a result, OT owners and ICS professionals have critical decisions to make. They need a cybersecurity approach that serves the segmentation requirements for both wireless and wired networks and protects their platforms from bad traffic and potential exploitation; and gain sufficient flexibility as industrial OT use cases become more prevalent and data becomes more segmented.

The Purdue Model is a tried and proven way to ensure throughput on the factory floor, and to protect and maintain the safe operation of factory floor equipment. Introducing a TrueFort microsegmentation and application behavioral enforcement layer, as an add-on, preserves the benefits the Purdue Model. It does so while also enabling the platform to bypass its hierarchy where needed (e.g., sensors sending data from Level 1 to Level 5), by piping application-controlled and micro-segmented traffic data to the industrial edge platform for production analysis and optimization.

The TrueFort microsegmentation platform enables OT owners to achieve complete visibility of the application-mesh and apply zero-trust policies, while preserving high-level operational performance and introducing the new and more efficient technologies into their environments.

> The Purdue Model is a tried and proven way to ensure throughput on the factory floor, and to protect and maintain the safe operation of factory floor equipment.

▶ CONTACT US TODAY

sales@truefort.com

ABOUT TRUEFORT

TrueFort puts you in control of lateral movement across the data center and cloud. The TrueFort Cloud extends protection beyond network activity by shutting down the abuse of service accounts. Founded by former IT executives from Bank of America and Goldman Sachs, leading global enterprises trust TrueFort to deliver unmatched application environment discovery and microsegmentation for accounts and activity.

For more information, visit truefort.com and follow us on Twitter and LinkedIn.

TRUEFORT™

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM