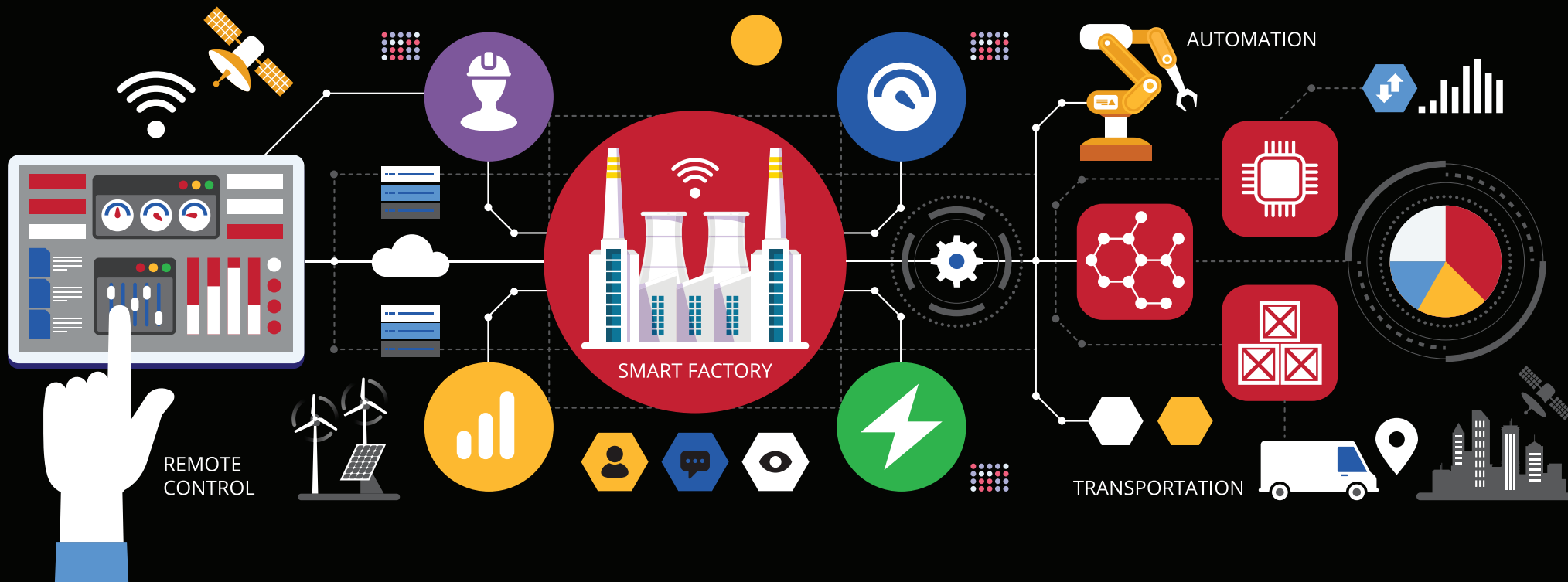


FALL 2018

# Remote Equipment Access Options Analysis




brought to you by:

PMMI | 11911 Freedom Drive, Suite 600 | Reston, VA 20190



**OpX**<sup>™</sup>  
Leadership Network  
Moving Operational Excellence Forward

HOW TO NAVIGATE THIS DOCUMENT

 Click on this icon in the top left corner to take you back to the table of contents.

Use the colored blocks to navigate throughout the sections of the table.

< Complete Chart 

CONTENTS

Purpose.....3

Contributors .....3

Best Value Options Analysis .....5

Direct VPN .....6

Converged Network .....9

Cell Modem Access.....12






Black Box .....15

External Managed Secure Network .....18

Technician Access .....21

Glossary of Terms .....23

KEY

-  IT (information technology) skills
-  OT (operational technology) skills
-  Acquisition and operating cost
-  Reliability
-  Operational and business protection

OVERVIEW

Consumer Packaged Goods (CPG) and their suppliers Original Equipment Manufacturer (OEM) and Service Providers can benefit from a common understanding of the relative pros and cons of industry methodologies regarding remote equipment access. The goal is to enable safe and secure remote equipment diagnostics and assistance by the suppliers of current and future operating equipment in CPG manufacturing plants.

While the technologies enabling remote equipment access have been present for quite some time, adoption has been slow. This is partially attributable to the disparate needs and goals of CPGs’ information technology(IT)andoperationstechnology(OT)functions.Moreprogresshasbeenmadeinremotemonitoring of equipment for predictive maintenance and improved OEE, but for security reasons, less has been made on in-bound troubleshooting, as fear of data breaches and cyber-security risks mount.

To help bridge this gap and provide guidance to choices about remote equipment access, the OpX Leadership Networks Remote Equipment Access Solutions Group created this Remote Equipment Access Options Analysis document. It provides descriptions of five of the most predominant industry methodologies enabling remote equipment access as alternatives to onsite technician access. Each of them is evaluated on seven key attributes regarding skills required, costs, reliability and security. Additionally, the relative pros and cons of each industry methodology are identified. Finally, leadership guidance for each industry methodology is offered by leveraging the Subject Matter Expertise (SME) of the OpX Remote Equipment Access Solutions Group (see sidebar).

This OpX work product is not designed and is not intended as a how to guide. It is designed as a discussion tool for each production team to consider the approaches they may choose to enable access to equipment for diagnosis, potential repair, and performance improvements from typically remote suppliers that are not part of the customer’s company. The five alternatives to onsite technician access were identified by the Solutions Group based on their collective experience. Each alternative is best described by the graphic and accompanying detail in the following pages.

The following is a purposely brief identification of the five alternatives and onsite technician access:

- **DIRECT VPN** – The customer’s firewall requires permission granted by the customer to the OEM for access to the network that has the production operations control devices on the line.
- **CONVERGED NETWORK** – The customer’s firewall plus a second secure switch require permission granted by the customer to the OEM for access to a segmented section of the network that has the production operations control devices on the line.
- **CELL MODEM ACCESS** – The OEM provides a device that has cellular wireless networking or the customer’s OT team turns on a mobile phone as a WIFI hotspot to enable an external network connection to the production operations control devices on the line.

MEMBERS OF THE OPX REMOTE EQUIPMENT ACCESS SOLUTIONS GROUP

Abbott . . . . .	James Li
Amway . . . . .	Rob Dargie
Arpac . . . . .	James Barry
Campbell’s. . . . .	Ted Franck Mark Potosky
Del Monte . . . . .	Bill Manhart
Frito Lay . . . . .	Richard Vandyke
HEB . . . . .	David Gard
Hormel Foods . . . . .	Adam Traeger
PepsiCo . . . . .	Tony Vandenoever Rolando Meireles
ProMach . . . . .	Chris Hough Mark Ruberg (formally Pro Mach)
Snyder’s Lance . . . . .	Mike Muscatell (Campbell’s Snacks)
Sugar Creek . . . . .	Ed Rodden Wes Dawes
Sunny D . . . . .	Shawn Roberts
OpX Leadership Network . . . .	Stephen Perry Stephen Schlegel
PMMI . . . . .	Tom Egan Bryan Griffen

Special thanks to ei³ for guidance on document graphics.

## Remote Equipment Access: Options Analysis

■ **BLACK BOX** – The OEM provides a device and, in some cases, a cloud service that establishes a temporary secure VPN tunnel through the customer's firewall to the network that has the production operations control devices on the line.

■ **EXTERNAL MANAGED SECURE NETWORK** – The OEM provides a third-party cloud service and device that establishes a permanent secure VPN tunnel through the customer's firewall with software features that enable customers to grant individual access to a segmented section of the production operations control devices on the line.

■ **ONSITE TECHNICIAN ACCESS** – The service visit that occurs when an OEM, integrator or third party technical expert comes to the customer's facility for direct access to a piece of equipment or full line.

### CYBERSECURITY

Please note that all of the options represent some degree of cybersecurity vulnerability. The group identified the "relative" security graphically with one (weak) to four (strong) lock icons on the Summary Attributes page. When, after considering all the attributes, some companies will select cell modem access as an approach, the group strongly recommends pursuing those options with at least two locks in the Operational Protection and in the Business Protection cells. In all cases, it is a best practice to discuss your approach with the appropriate security personnel in your company.

### IIOT DEVICES

Though not directly affected by the method of remote connectivity, the proliferation of IIoT connected devices brings new challenges to the manufacturing floor in terms of data management, security and network maintenance. These devices have the potential to become security holes within the network. Care must be taken to avoid potential breaches. This group strongly recommends solid collaboration between IT and OT personnel in the design and implementation of all networks, security protocols and connected devices.

### ALTERNATIVES NOT ON THE LIST

An independent Operations Technology (OT) network dedicated solely to the production operations was considered but ultimately not included as an alternative. While the Solutions Group members recognize that some independent OT networks already exist, these networks are very difficult to maintain and, for security purposes, purposely do not integrate with the customer's IT networks. As a result, the objective of having an integrated system with OT and IT linked to enhance and promote business processes is not achieved.

## SPONSORS

















































































Facilitated by PMMI, the OpX Leadership Network is a dynamic community of manufacturing, engineering and operations professionals dedicated to operational excellence. Through open dialogue between CPG manufacturers and OEMs, the OpX Leadership Network provides an exceptional forum where the best minds come together to identify and solve common operational challenges, and apply best practices and innovative solutions to the real-world context of manufacturing.



PMMI, The Association for Packaging and Processing Technologies, represents more than 800 North American manufacturers and suppliers of equipment, components and materials as well as providers of related equipment and services to the packaging and processing industry. We work to advance a variety of industries by connecting consumer goods companies with manufacturing solutions through the world-class PACK EXPO portfolio of trade shows, leading trade media and a wide range of resources to empower our members. The PACK EXPO trade shows unite the world of packaging and processing to advance the industries they serve: PACK EXPO International, PACK EXPO Las Vegas, Healthcare Packaging EXPO, PACK EXPO East, EXPO PACK México, EXPO PACK Guadalajara and ProFood Tech. PMMI Media Group connects manufacturers to the latest solutions, trends and innovations in packaging and processing year-round through brands including Packaging World, Automation World, Healthcare Packaging, Contract Packaging, ProFood World and OEM. PMMI Business Drivers assist members in pursuing operational excellence through workforce development initiatives, deliver actionable business intelligence on economic, market and industry trends to support members' growth strategies and actively connect the supply chain throughout the year. Learn more at [pmmi.org](http://pmmi.org) and [packexpo.com](http://packexpo.com) and [pmmimediagroup.com](http://pmmimediagroup.com).

This copyright © 2018. PMMI. is publication was developed through the OpX Leadership Network, convened by PMMI. It may be downloaded, reproduced, and distributed for business or academic use, but not for license or sale, provided there is clear attribution to the OpX Leadership Network as the developer of the publication and PMMI as the copyright owner.

## Best Value Options Analysis *Click each attribute to see its detail.*

ATTRIBUTES	DIRECT VPN	CONVERGED NETWORK	CELL MODEM ACCESS	BLACK BOX	EXTERNAL MANAGED SECURE NETWORK	TECHNICIAN ACCESS
IT Skills required to select, install and train	   	   			  	N/A
OT Skills required to maintain, update and support operations		  			SUBSCRIPTION	N/A
Acquisition Cost to acquire and install hardware and software (one time, existing IT network)		  			 	N/A
Operating Cost to maintain and update thru staffing (internal or outsourcing) licenses and hyper-care		 	N/A	N/A	 	   
Reliability of Method is the stability and robustness of means of access	  	  		  	  	
Operational Protection to technically secure the factory floor (Operational Technology)		   		   	   	NONE
Business Protection to segregate the OT network from the IT network	 	   		  	  	

NOTE: 4 icons is the max for any category.

## DIRECT VPN

[< complete chart](#)


### ATTRIBUTES

### DIRECT VPN

HIGH LEVEL VIEW

TECHNICAL VIEW

IT Skills required to select, install and train



OT Skills required to maintain, update and support operations



Acquisition Cost to acquire and install hardware and software (one time, existing IT network)



Operating Cost to maintain and update thru staffing (internal or outsourcing) licenses and hyper-care



Reliability of Method is the stability and robustness of means of access



Operational Protection to technically secure the factory floor (Operational Technology)



Business Protection to segregate the OT network from the IT network



## LEADERSHIP GUIDANCE:

- Treat this as you would any other project, e.g. CIP design, etc.
- Get engaged early and understand the requirements.  
Is continuous connectivity or transactional connectivity required?
- Follow design process (RACI Matrix) similar to other equipment reviews, e.g., any normal engineering project, and follow best project execution practices.
- Balance what's needed with risk associated with it – employ operational risk analysis.
- The plant does not have to follow a single methodology – methodologies can be mixed.

# DIRECT VPN

< complete chart



## BENEFITS:

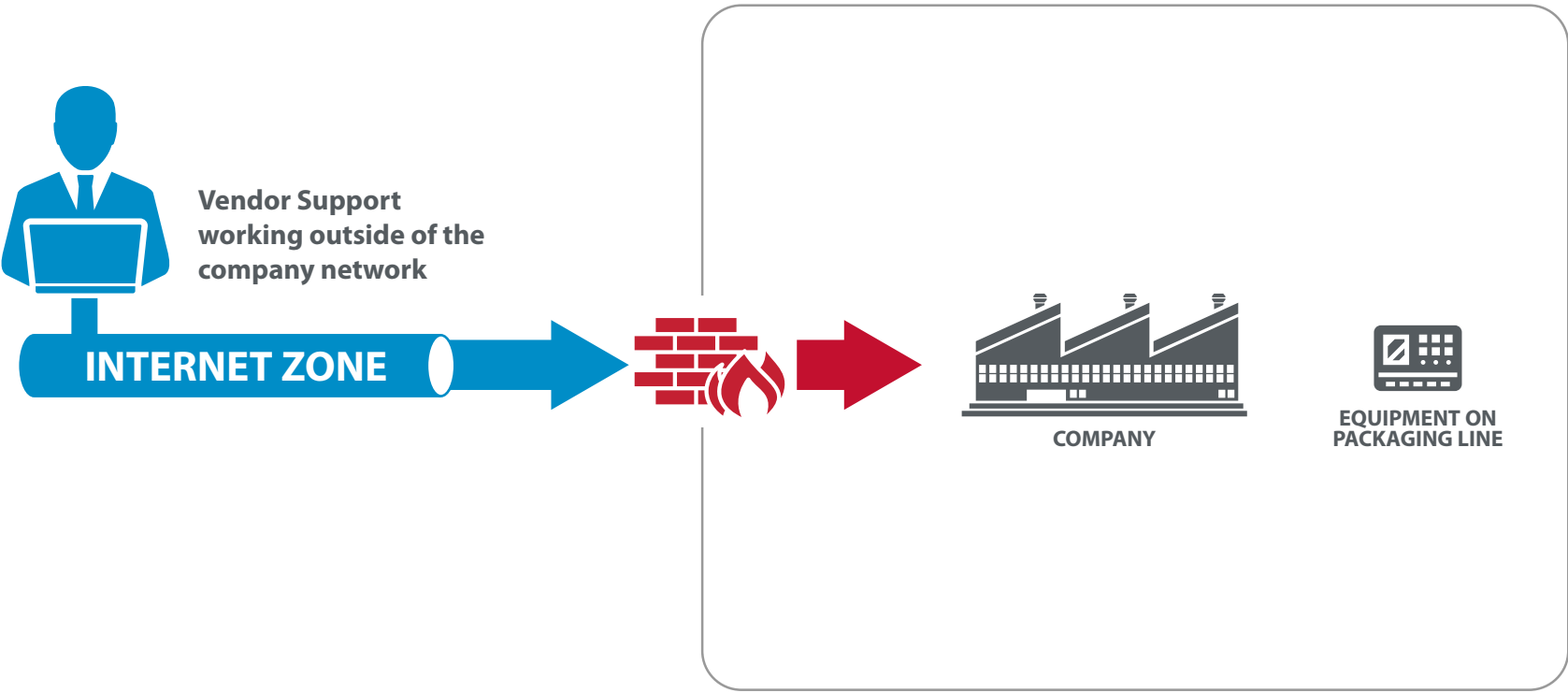
- Leverage External Partners
- Speed to Solution

## RISKS:

- Password Management
- Support Overhead
- Updating Users

HIGH LEVEL VIEW

TECHNICAL VIEW



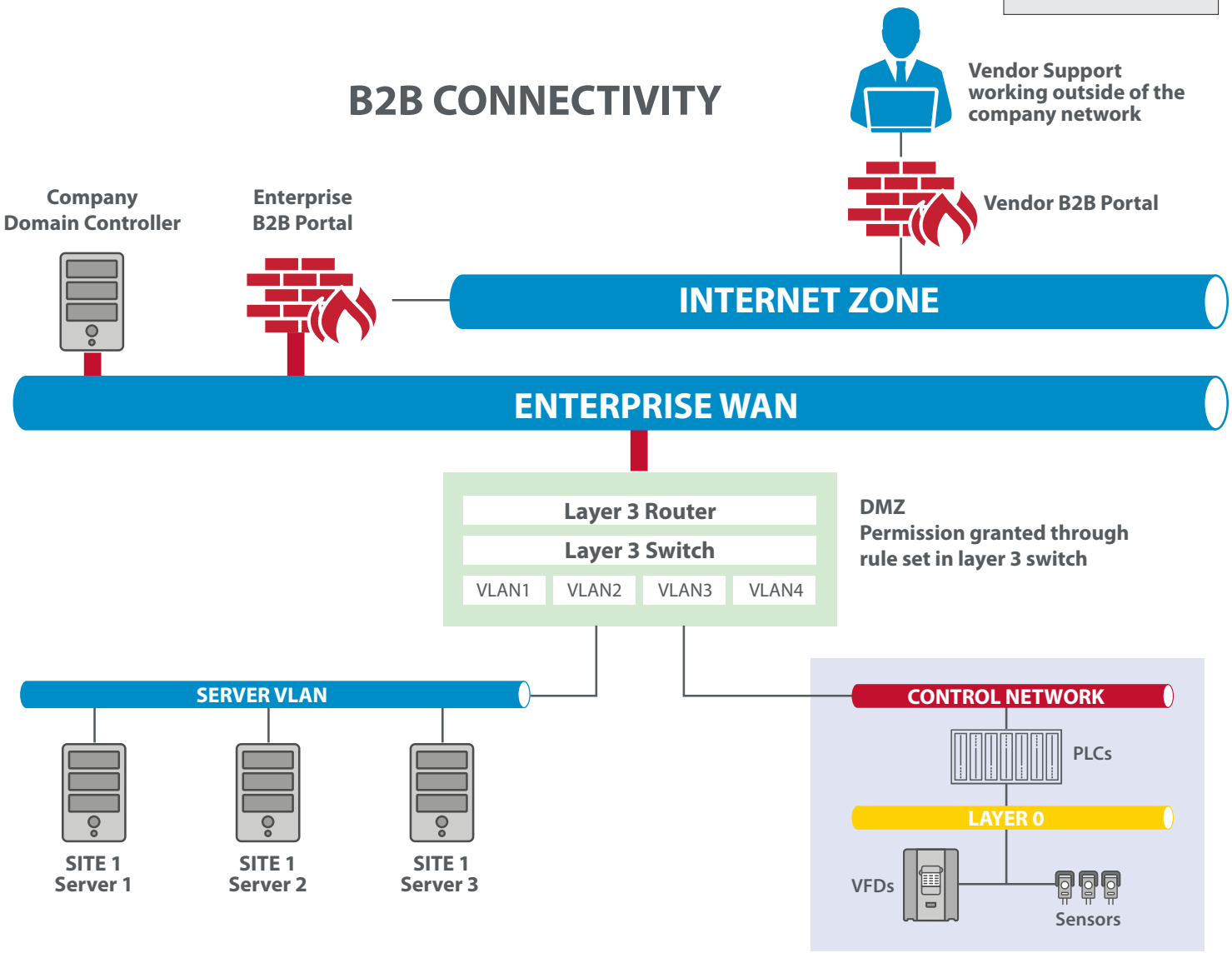
DIRECT VPN

< complete chart



HIGH LEVEL VIEW

TECHNICAL VIEW





# CONVERGED NETWORK

< complete chart



ATTRIBUTES	CONVERGED NETWORK
------------	-------------------

HIGH LEVEL VIEW

TECHNICAL VIEW

IT Skills required to select, install and train	
OT Skills required to maintain, update and support operations	
Acquisition Cost to acquire and install hardware and software (one time, existing IT network)	
Operating Cost to maintain and update thru staffing (internal or outsourcing) licenses and hyper-care	
Reliability of Method is the stability and robustness of means of access	
Operational Protection to technically secure the factory floor (Operational Technology)	
Business Protection to segregate the OT network from the IT network	

## LEADERSHIP GUIDANCE:

- TCO is higher for hardware and support required to implement.
- Security against intrusion is strong.
- DMZ: Vendors are challenged by version control, standardization, and license management.

## CONVERGED NETWORK

[< complete chart](#)

### BENEFITS:

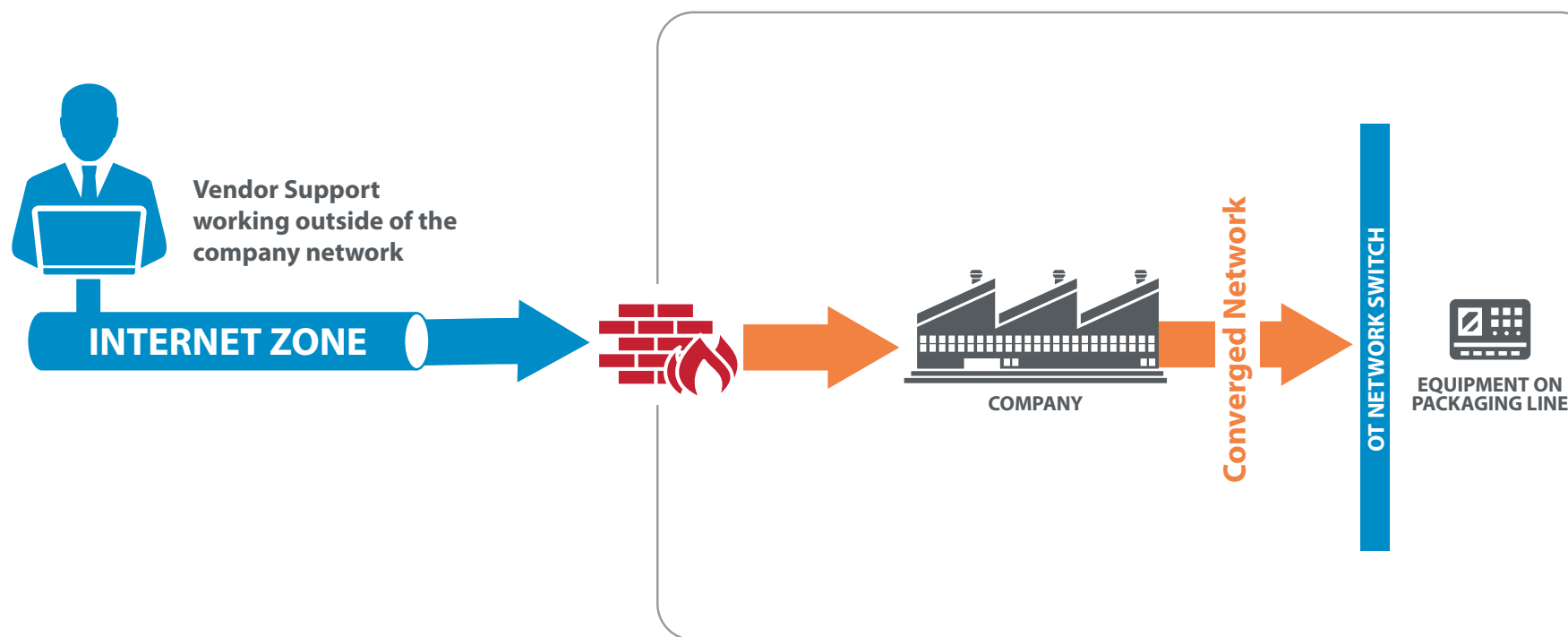
- More Secure

### RISKS:

- Expensive
- High level of skill required
- Maintenance and support
- Vendor adoption

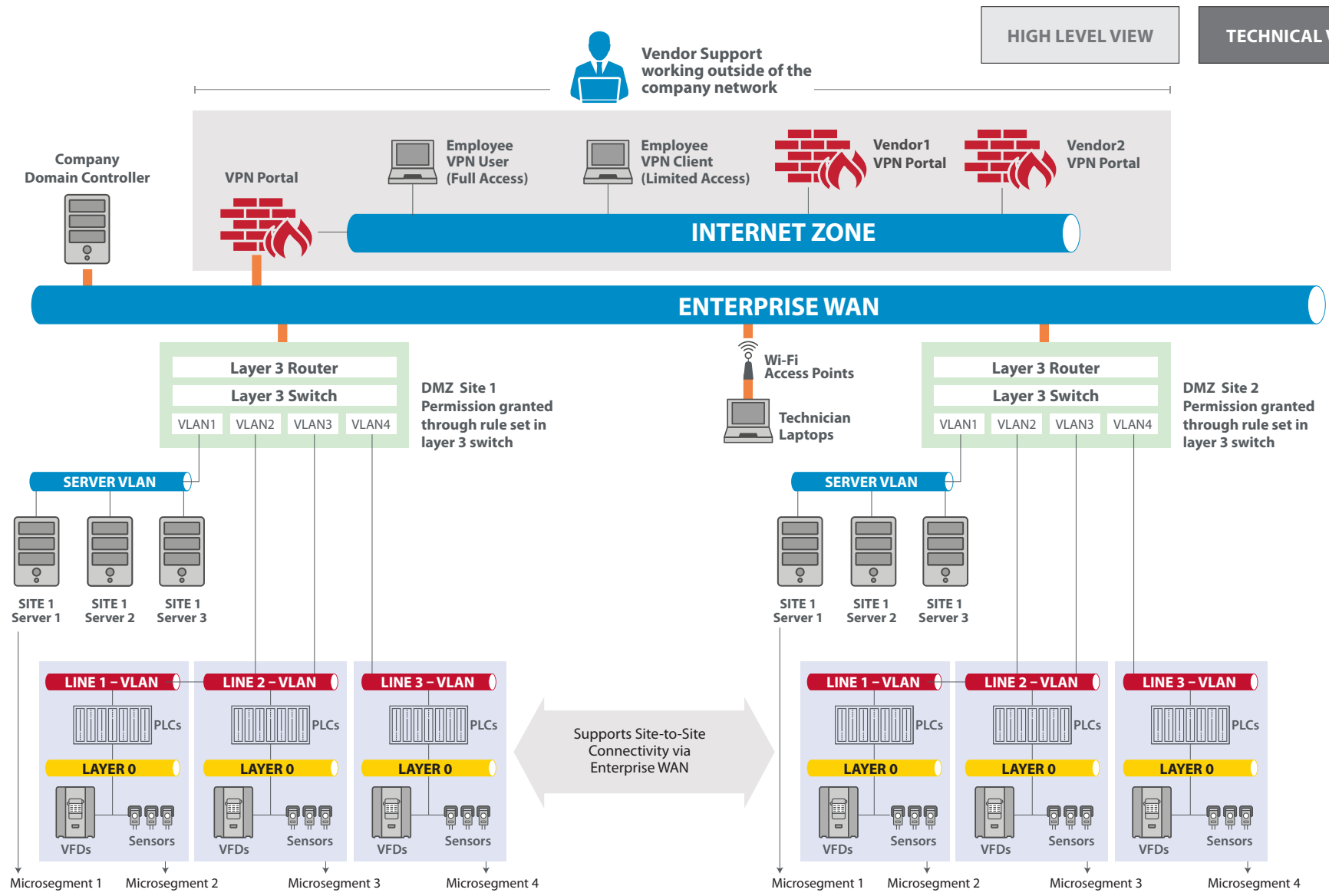
HIGH LEVEL VIEW

TECHNICAL VIEW



# CONVERGED NETWORK

< complete chart



# CELL MODEM ACCESS

< complete chart



ATTRIBUTES

CELL MODEM ACCESS

HIGH LEVEL VIEW

TECHNICAL VIEW

IT Skills required to select, install and train	
OT Skills required to maintain, update and support operations	
Acquisition Cost to acquire and install hardware and software (one time, existing IT network)	
Operating Cost to maintain and update thru staffing (internal or outsourcing) licenses and hyper-care	N/A
Reliability of Method is the stability and robustness of means of access	
Operational Protection to technically secure the factory floor (Operational Technology)	
Business Protection to segregate the OT network from the IT network	

## LEADERSHIP GUIDANCE:

- Be aware that this type of connectivity circumvents all security firewalls.
- Realize that connectivity goes undetected and unmonitored, which introduces additional vulnerability.
- Be cognizant that connectivity quality is highly variable.
- This methodology is very easy to connect to equipment without going through existing IT infrastructure.

## CELL MODEM ACCESS

[< complete chart](#)

### BENEFITS:

- Easy to do
- Works when no network is available

### RISKS:

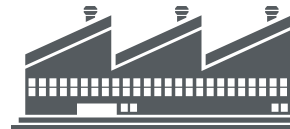
- Hard to monitor
- Connected machines can be vulnerable to network

HIGH LEVEL VIEW

TECHNICAL VIEW



Vendor Support  
working outside of the  
company network

**INTERNET ZONE**

COMPANY

OT NETWORK SWITCH

CELL MODEM  
ACCESSEQUIPMENT ON  
PACKAGING LINE

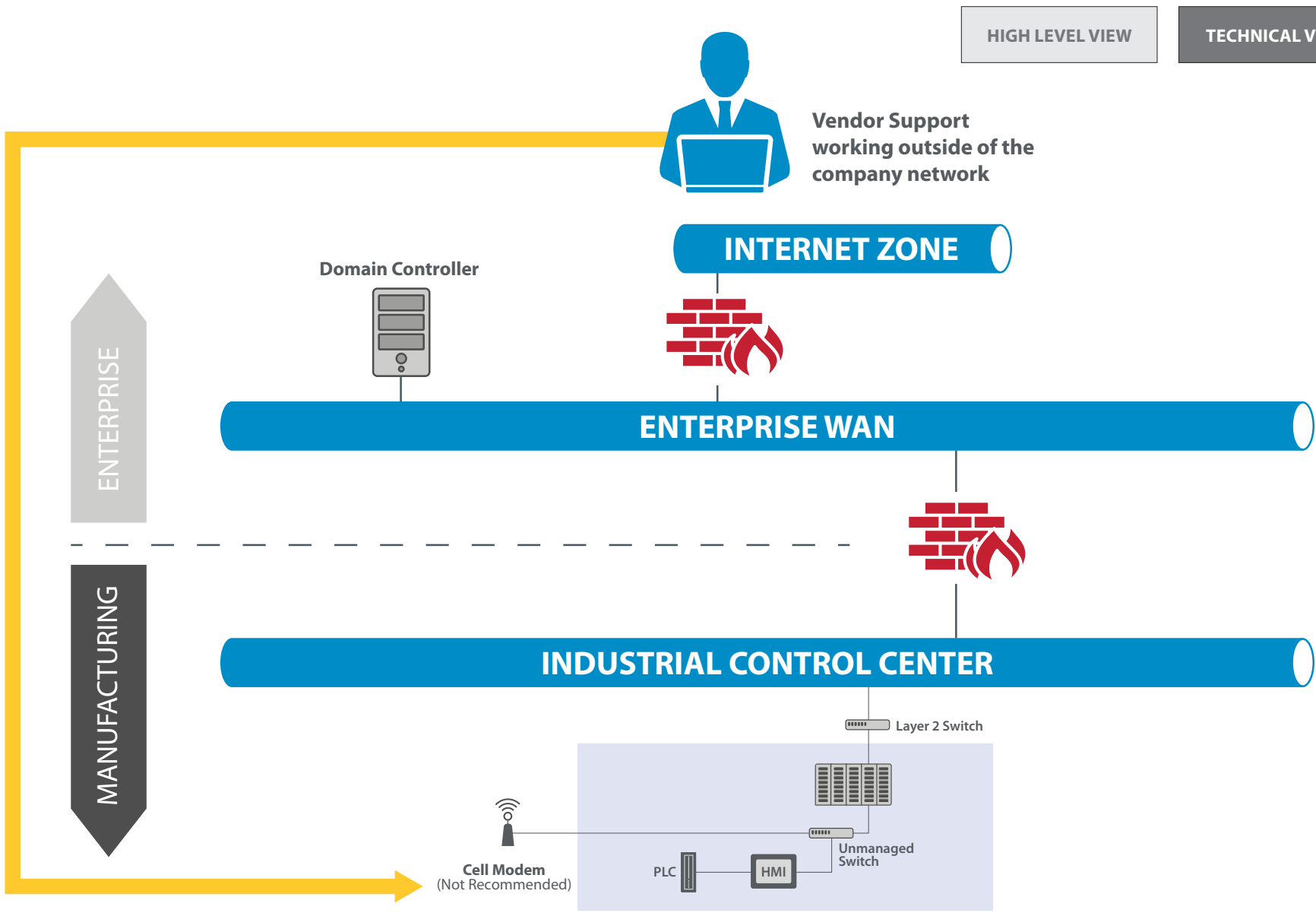
# CELL MODEM ACCESS

< complete chart



HIGH LEVEL VIEW

TECHNICAL VIEW



# BLACK BOX

< complete chart



ATTRIBUTES

BLACK BOX

HIGH LEVEL VIEW

TECHNICAL VIEW

IT Skills required to select, install and train	
OT Skills required to maintain, update and support operations	
Acquisition Cost to acquire and install hardware and software (one time, existing IT network)	
Operating Cost to maintain and update thru staffing (internal or outsourcing) licenses and hyper-care	N/A
Reliability of Method is the stability and robustness of means of access	
Operational Protection to technically secure the factory floor (Operational Technology)	
Business Protection to segregate the OT network from the IT network	

## LEADERSHIP GUIDANCE:

- Be aware that continuous connection creates access vulnerability.
- There is a strong need for security management, e.g. OEM users sharing credentials.
- Be cognizant that this methodology creates an outbound connection to a third party server, e.g. communication phone home server or to cloud server.
- Potential visibility and control limitations, e.g. change control, audit trail, security compliance.

# BLACK BOX

< complete chart



## BENEFITS:

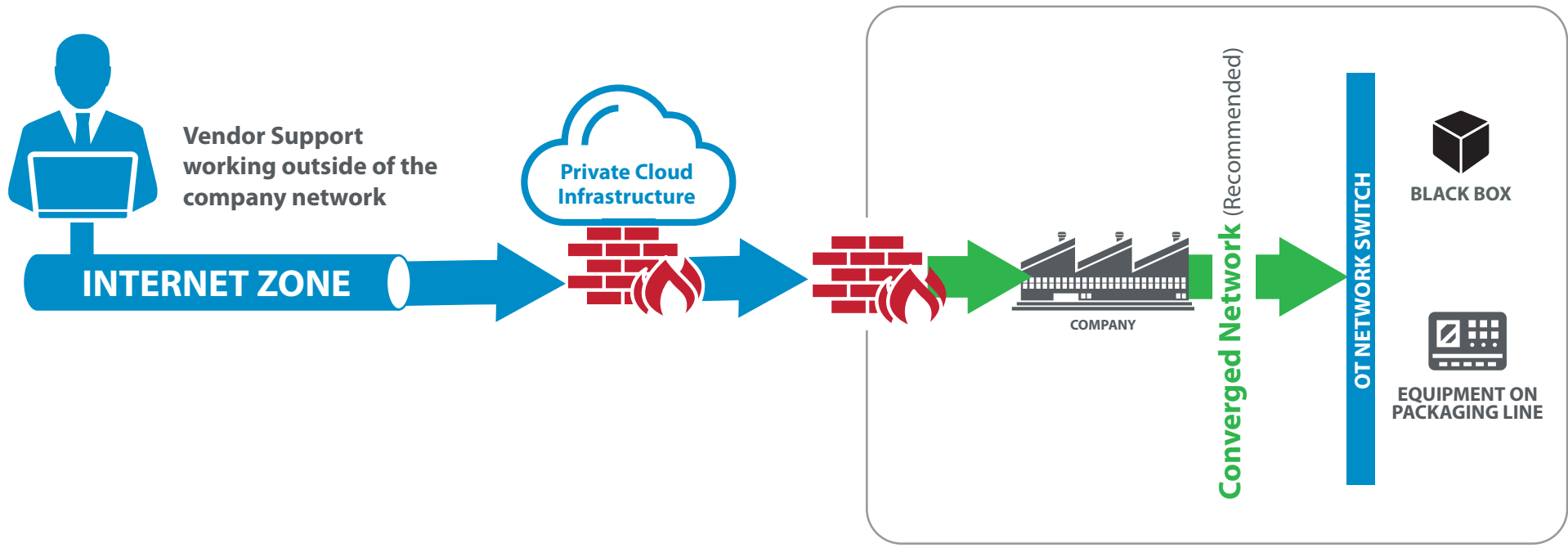
- Low reliance on IT resources
- Comm. Link made on demand

## RISKS:

- Password Management
- Support Overhead
- Updating Users

HIGH LEVEL VIEW

TECHNICAL VIEW





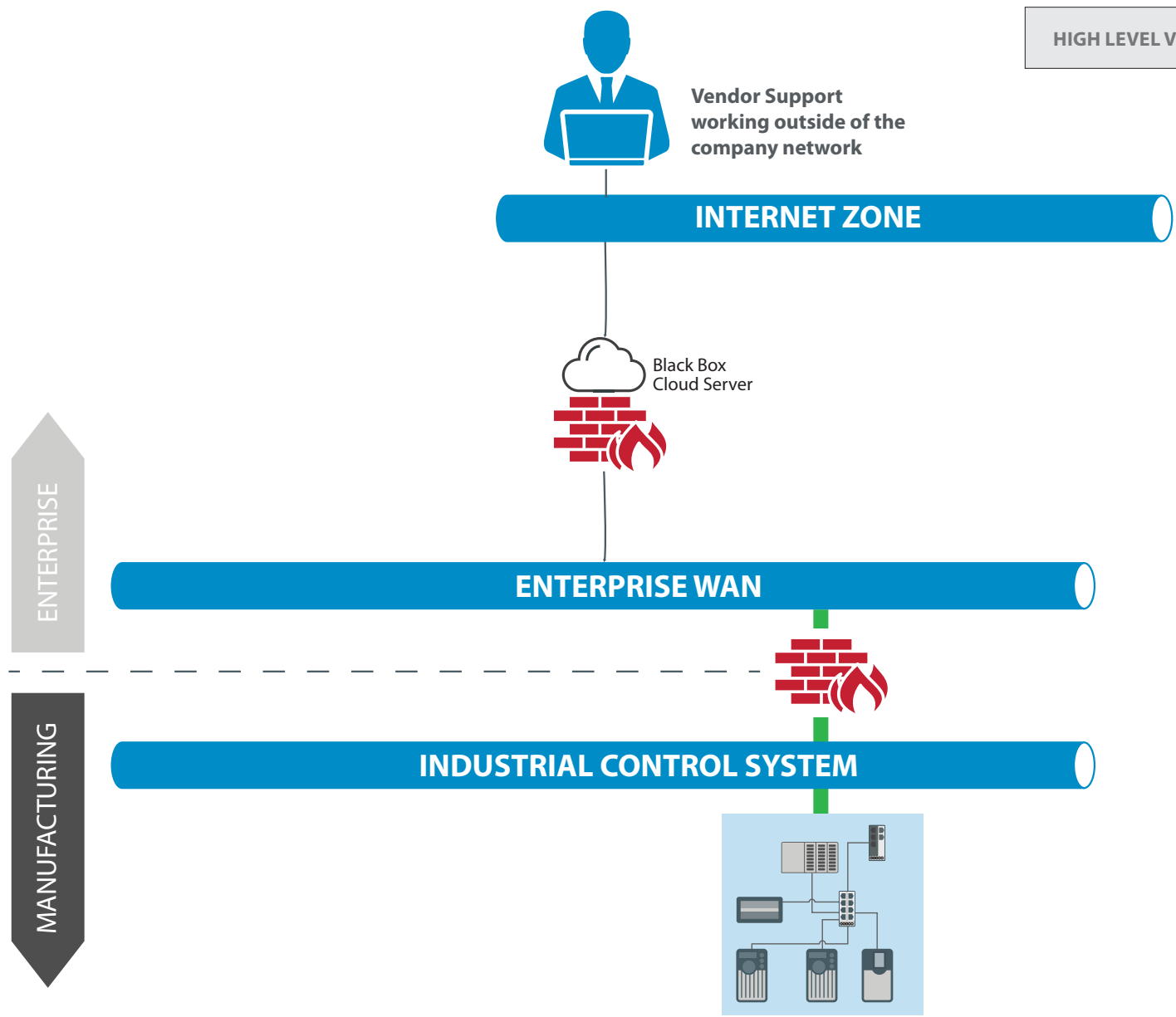
BLACK BOX

< complete chart



HIGH LEVEL VIEW

TECHNICAL VIEW



EXTERNAL MANAGED SECURED NETWORK

< complete chart



ATTRIBUTES	EXTERNAL MANAGED SECURE NETWORK
IT Skills required to select, install and train	
OT Skills required to maintain, update and support operations	N/A
Acquisition Cost to acquire and install hardware and software (one time, existing IT network)	
Operating Cost to maintain and update thru staffing (internal or outsourcing) licenses and hyper-care	
Reliability of Method is the stability and robustness of means of access	
Operational Protection to technically secure the factory floor (Operational Technology)	
Business Protection to segregate the OT network from the IT network	

HIGH LEVEL VIEW

TECHNICAL VIEW

LEADERSHIP GUIDANCE:

- Similar to Black Box but adds software defined converged network.
- IT user administration outsourced, so necessitates a more focused look at a master service agreement for proper implementation and support.
- Typically accompanied by a SaaS (software as a service) subscription fee.
- Recommend that reliability of user access and other services be audited and reported on by service provider.
- Recommend internal control evaluation of external access on a continuous basis.

# EXTERNAL MANAGED SECURED NETWORK

< complete chart



## BENEFITS:

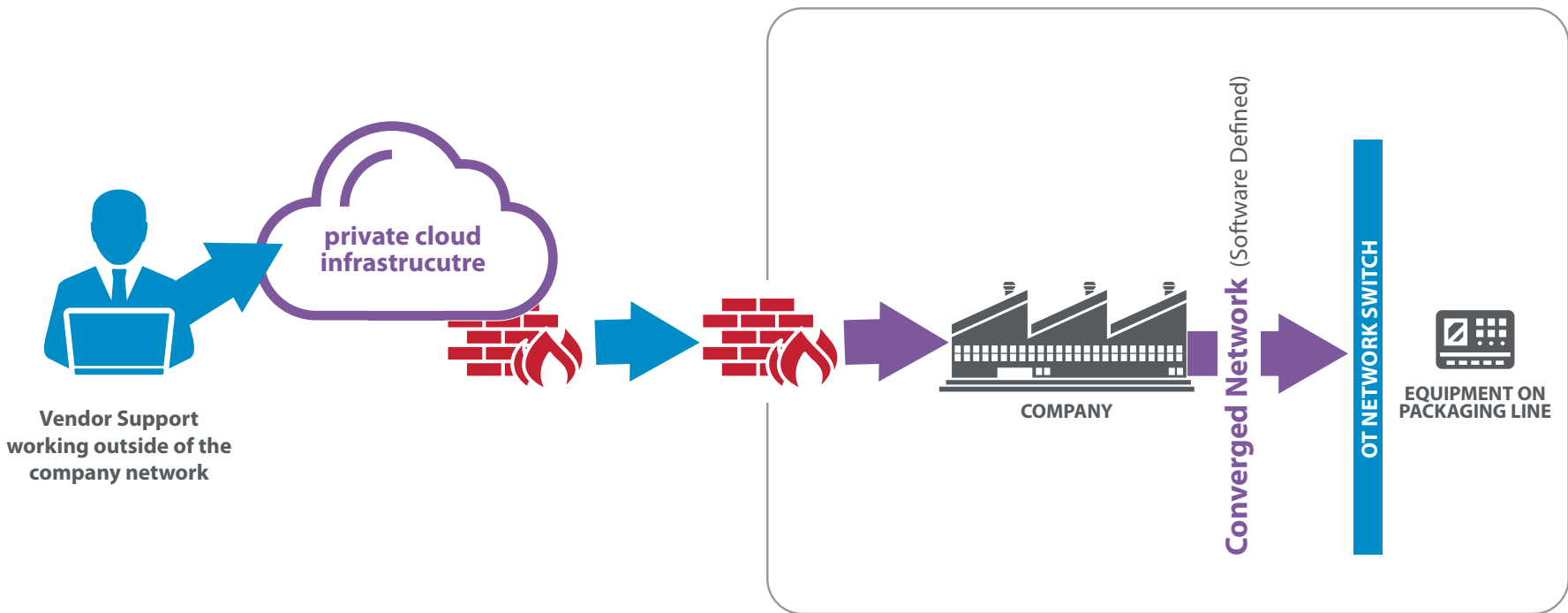
- High level of security
- Easy to manage

## RISKS:

- Requires working with a 3rd party specialist provider

HIGH LEVEL VIEW

TECHNICAL VIEW



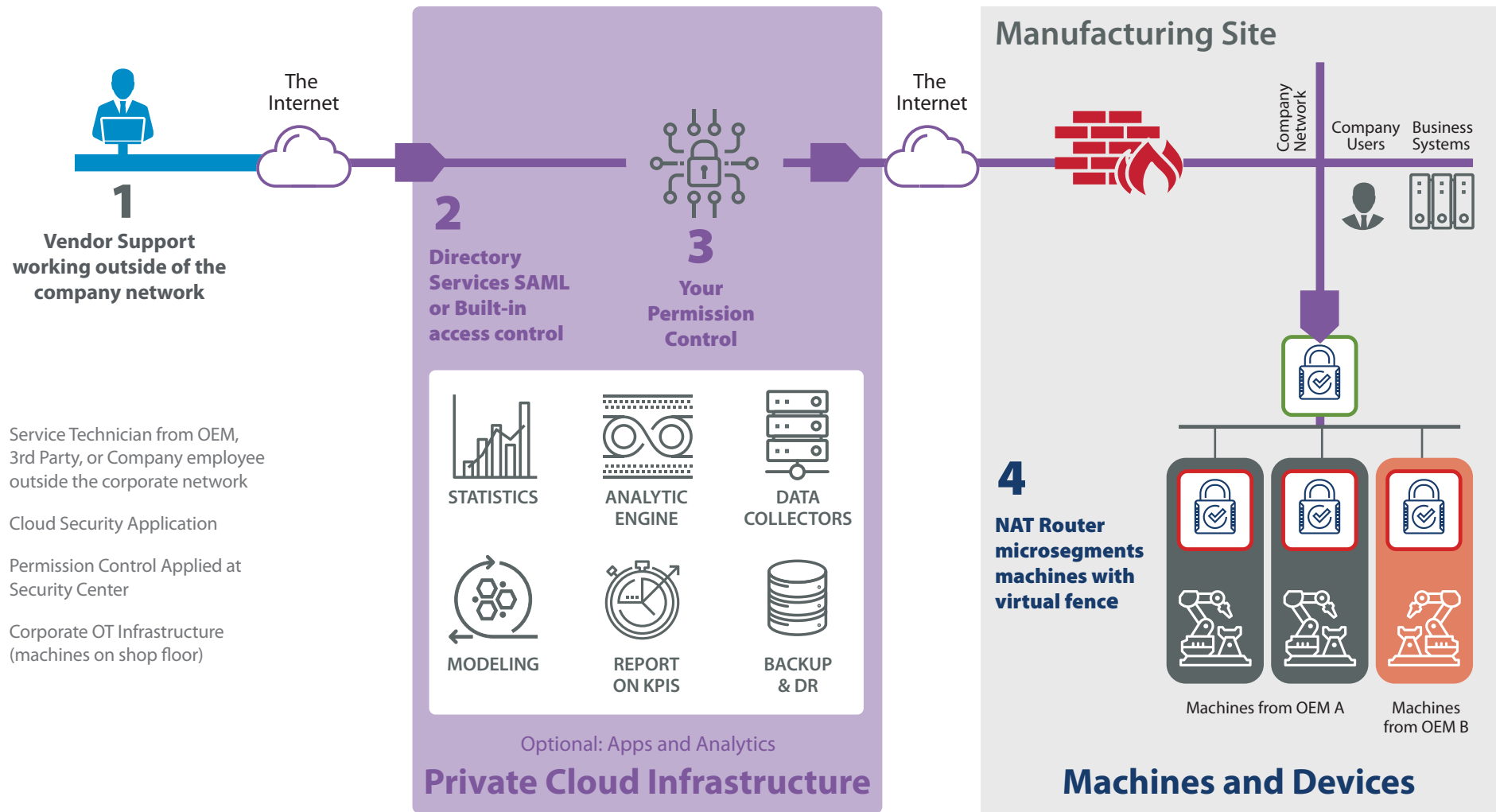
# EXTERNAL MANAGED SECURED NETWORK

< complete chart



HIGH LEVEL VIEW

TECHNICAL VIEW



Service Technician from OEM,  
3rd Party, or Company employee  
outside the corporate network

Cloud Security Application

Permission Control Applied at  
Security Center

Corporate OT Infrastructure  
(machines on shop floor)

# TECHNICIAN ONSITE ACCESS

< complete chart



ATTRIBUTES	TECHNICIAN ACCESS
IT Skills required to select, install and train	N/A
OT Skills required to maintain, update and support operations	N/A
Acquisition Cost to acquire and install hardware and software (one time, existing IT network)	N/A
Operating Cost to maintain and update thru staffing (internal or outsourcing) licenses and hyper-care	\$ \$ \$ \$
Reliability of Method is the stability and robustness of means of access	
Operational Protection to technically secure the factory floor (Operational Technology)	NONE
Business Protection to segregate the OT network from the IT network	

HIGH LEVEL VIEW

NO TECHNICAL VIEW

## LEADERSHIP GUIDANCE:

- Important for IT to understand that manufacturing equipment downtime is very costly; additionally, travel for technician access can increase costs dramatically, e.g. LOTO.
- Strict screening policies enforcement required, e.g. not allowing outside laptops access to avoid security breaches (e.g. virus infections).
- Most often used during installation, so use appropriate onboarding policies, which may differ from standard operating procedures.
- Be mindful to segregate projects that technician may have access to through use of NDA.

# Technician Onsite Access

< complete chart



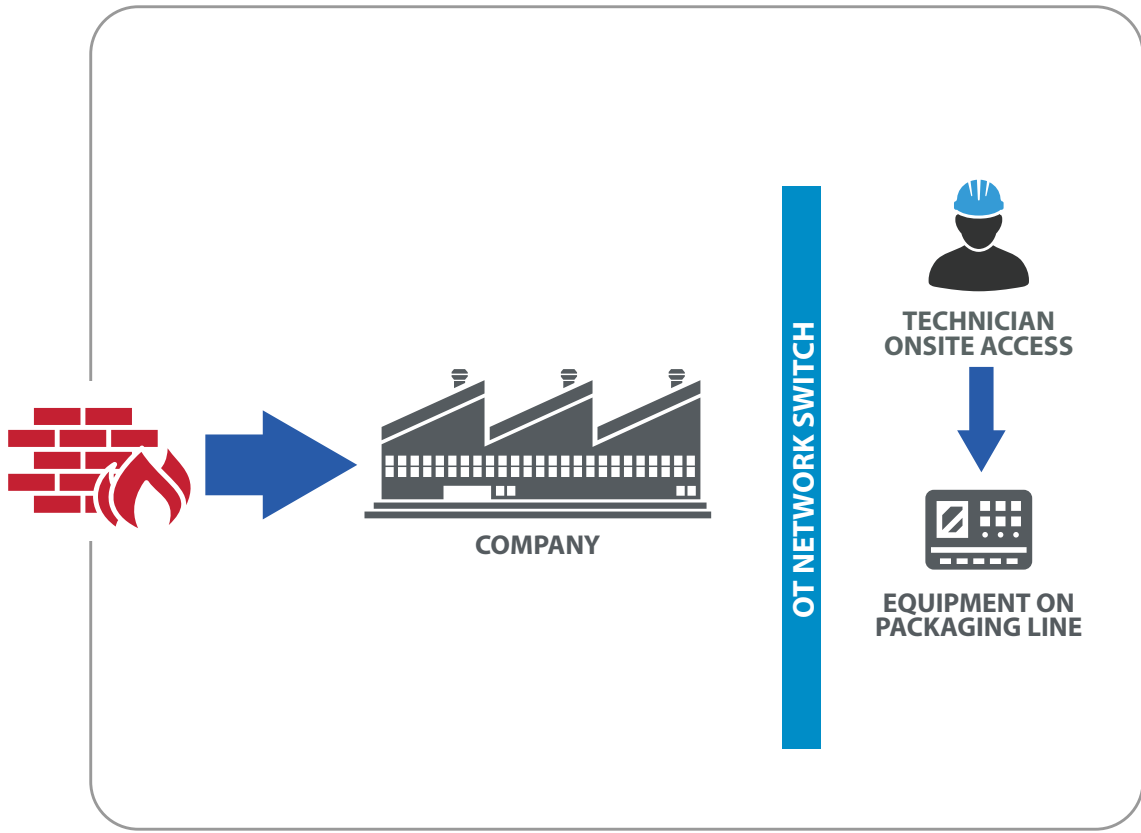
## BENEFITS:

- Leverage External Partners
- Speed to Solution

## RISKS:

- Password Management
- Support Overhead
- Updating Users

HIGH LEVEL VIEW



# TOOLS FOR DRIVING MANUFACTURING EXCELLENCE

Total Cost of Ownership (TCO): Processing and  
Packaging Machine Guidelines for CPGs and OEMs



# OpX

Leadership Network  
Moving Operational Excellence Forward



## THE CHALLENGE

A lack of clarity in TCO resulting in unmet expectations for stakeholders when engaging in the commercial transactions for capital equipment.



## THE SOLUTION

A comprehensive TCO Playbook that includes guidelines and checklists – developed by industry experts – for the broad adoption and use throughout the CPG industry.



The TCO Playbook and checklist cover what your company will need to effectively address:

### ACQUISITION COSTS

- Equipment Design and Application
- Project Requirements
- Installation
- Initial Training
- Validation
- Utility/Energy Costs



### OPERATION COSTS

- Quality
- Labor
- Maintenance, Set-Up and Changeover
- Cleaning & Sanitization
- Training
- Utilities and Environmental

"Introducing the Total Cost of Ownership to our team has resulted in significant benefits and savings. Using these guidelines has led to more efficient start-ups, lower cost of operation, and a product that satisfies the consumer and our customers."

– Roy Greengrass, Senior Engineering Manager, Del Monte Foods

## ADOPT THE TCO PLAYBOOK AND CHECKLIST AT YOUR COMPANY TODAY.

Download the full report and find out how to engage with the OpX Leadership Network at industry events by visiting [OpXLeadershipNetwork.org](http://OpXLeadershipNetwork.org).



# GLOSSARY OF TERMS

## Black Box

A black box is a device, system or object that can be viewed in terms of its inputs and outputs (or transfer characteristics) without any knowledge of its internal workings.

A black box refers to a piece of equipment provided by a vendor, for the purpose of using that vendor's product. It is often the case that the vendor maintains and supports this equipment, and the company receiving the black box typically is hands-off. [Wikipedia](#)

## Private Cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

[NIST-CSRC](#)

## VPN (Virtual Private Network)

A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks. [NIST SP 800-113](#)

## IT (Information Technology)

Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes computers, ancillary equipment, software, firmware, similar procedures, services, and related resources. [NIST SP 800-64 Rev. 2](#)

## OT (Operational Technology)

Operational technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

[Gartner IT Glossary](#)

## RACI Matrix

The RACI matrix is a responsibility assignment chart that maps out every task, milestone or key decision involved in completing a project and assigns which roles are Responsible for each action item, which personnel are Accountable, and, where appropriate, who needs to be Consulted or Informed. The acronym RACI stands for the four roles that stakeholders might play in any project. [CIO from IDG](#)

## DMZ (Demilitarized Zone)

Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

[NIST SP 800-82 Rev. 2 \(CNSSI 4009\)](#)

## VLAN (Virtual Local Area Network)

A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes.

[technopedia](#)

## WAN (Wide Area Network)

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN. [NIST SP 800-82 Rev. 2 \(API 1164\)](#)

## Microsegmentation

Microsegmentation is a method of creating secure zones in data centers and cloud deployments that allows companies to isolate workloads from one another and secure them individually. It's aimed at making network security more granular.

This method also applies to plantwide ethernet networks, including VLAN and DMZ usage, even down the production line and machine level segmentation.

[NetworkWorld from IDG](#)

## NDA (Non-Disclosure Agreement)

A non-disclosure agreement (NDA), also known as a confidentiality agreement (CA), confidential disclosure agreement (CDA), proprietary information agreement (PIA) or secrecy agreement (SA), is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties. [Wikipedia](#)

## SAML

Security Assertion Markup Language - An open standard for exchanging authentication and authorization between parties, in particular, between an identity provider and a service provider.

[Wikipedia](#)

## Secured Vendor Access

Secured vendor access is a method of industrial remote access that is designed to offer easy remote access across the Internet to machines and installations at customers' locations or remotely.





The Association for Packaging  
and Processing Technologies



Leadership Network  
Moving Operational Excellence Forward