TECHNICAL PAPER

SD-WAN for Manufacturing

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As demand for goods peaks, supply chain instability and labor shortage are forcing manufacturers to become more efficient and find new ways to maximize productivity. Manufacturers are accelerating their path to digitalization or Industry 4.0, to improve automation and be more competitive. Additionally, with the digitalization of their operations, manufacturing companies are increasingly moving their applications to the cloud for more agility and to enable their employees to work-from-anywhere. The number of IIoT (Industrial Internet of Things) devices is skyrocketing, while IT and OT (operational technology) networks are converging, raising concerns about cybersecurity risks.

In this context, a traditional MPLS router-based network architecture is no longer sustainable. It is often rigid, complex, and provides a poor quality of experience.

This paper examines six use cases in the manufacturing industry that show how the implementation of an advanced SD-WAN solution helps manufacturers accelerate their transformation journey to Industry 4.0 and become a cloud-first organization. With SD-WAN, manufacturers can improve agility and security by seamlessly connecting remote sites, simplifying network infrastructure while reducing costs. The paper also describes how SD-WAN is the foundational component of a SASE framework (Secure Access Service Edge) and how it helps manufacturers adopt a zero-trust architecture to secure IoT devices and comply with cybersecurity frameworks.

CHALLENGES IN THE MANUFACTURING INDUSTRY

A recent Gartner survey[1] shows that 57% of manufacturing leaders believe their organization lacks skilled workers to support smart manufacturing digitization plans. One of the key challenges in manufacturing is indeed the transition to Industry 4.0 and the digitization of operations, to be more efficient, reduce time-to-market and improve product quality. On the other hand, the pandemic has created an unprecedented labor shortage. Manufacturers are also facing other key challenges such as supply chain instability, increased cybersecurity risks with the growing number of IoT devices, and compliance issues.

Industry 4.0 – The fourth industrial revolution

In the late 18th century, the first industrial revolution transformed hand production methods into steam machines. The second industrial revolution which occurred at the end of the 19th century revolutionized communication and transport methods with the telegraph and railway. The third revolution brought computing power to manufacturing processes in the second half of the 20th century.

Industry 4.0 now revolutionizes the automation and data exchange in manufacturing technologies and processes which include cyber-physical systems, IoT, industrial internet of things, cloud computing, cognitive computing, and artificial intelligence.

Labor shortage and supply chain disruption

With the pandemic, manufacturing organizations struggle to meet growing demand for their goods. One of the reasons is that manufacturing organizations lack skilled labor to operate production chains due to the successive lockdowns. Another reason is more structural as the baby boom generation is now retiring, and manufacturing organizations are struggling to hire new skilled people to replace them.

The labor shortage is also causing a supply chain disruption as primary components have become scarce due to the slowdown of the production, impacting the entire production chain. For example, the shortage of semiconductor chips has directly impacted the automotive industry, increasing the price tag – and the lead time – for new cars. The movement of containers around the world, slowed by the pandemic, has also impacted the supply chain with a record number of boats blocked in ports. Other factors such as the rising costs of raw materials explain the instability of the supply chain.

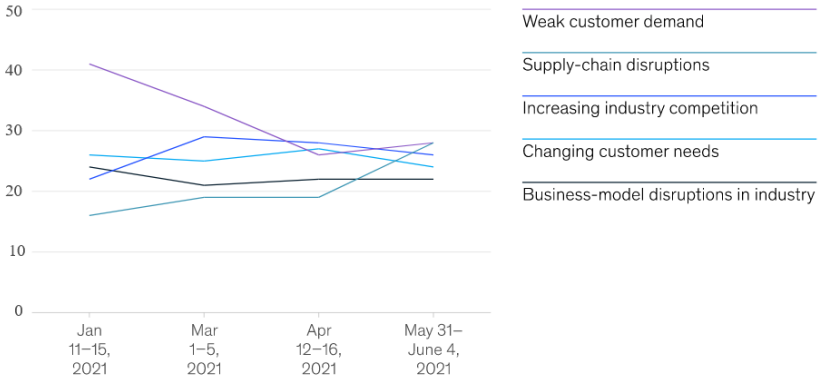
The disruption of the supply chain is not only impacting the auto industry and is now one of the main concerns of the manufacturing industry. In a McKinsey survey[2], respondents cite supply-chain disruptions as a top risk to their companies' growth and a more acute concern than ever before.

[1] Source: Smart Manufacturing Strategy and Implementation Trends Survey, Gartner, December 2020

[2] Source: Leaders brace for supply-chain setbacks, McKinsey, July 2021

Respondents cite supply-chain disruptions as a top risk to their companies' growth and a more acute concern than before.

Potential risks to companies' growth, next 12 months,[1] % of respondents



[1]Out of 15 risks that were presented as answer choices; question was asked only of respondents in private-sector companies. Jan 2021, n = 913; Mar 2021, n = 916; April 2021, n = 1,085; June 2021, n = 928.

Source: Leaders brace for supply-chain setbacks, McKinsey, July 2021

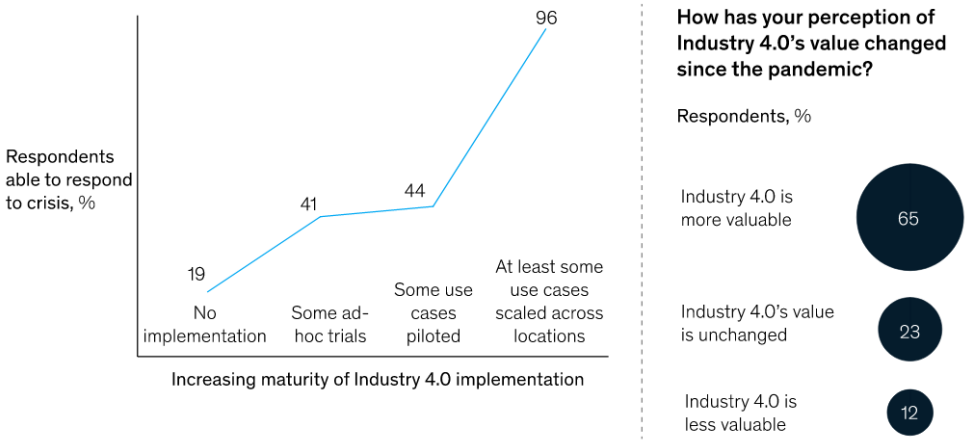
Accelerating the path to Industry 4.0

With the increase of interconnectivity and smart automation, the manufacturing industry is experiencing a fourth industrial revolution, or "Industry 4.0". The COVID crisis has put on hold this trend, but as more businesses emerge from the crisis, and with labor shortage, Industry 4.0 initiatives have moved from a "nice-to-have." to a "must-have"[3] as manufacturers need tools and technology to automate production and the supply chain.

Another McKinsey study[4] described how companies that have started an Industry 4.0 implementation before the crisis have been more able to respond to the COVID crisis.

Industry 4.0 is indeed transforming the manufacturing sector into smart factories using technologies such as artificial intelligence and advanced robotics to automate the production environment and the supply chain. It relies on industrial internet of things (IIoT), to connect machines, devices, sensors, and people with each other. The use of artificial intelligence and machine learning creates transparency, predictability and automation of operations and supply chain.

Companies whose Industry 4.0 implementation is more mature report stronger ability to respond to crisis.



Source: COVID-19: An inflection point for Industry 4.0, McKinsey, January 2021

[3] Source: How AI And Automation Can Address America's Broken Supply Chain

[4] Source: COVID-19: An inflection point for Industry 4.0, McKinsey, January 2021

Investment in smart manufacturing is predicted to grow, taking a greater percentage of company budgets. In a 2020 Deloitte and MAPI Study survey[5], 62% of leaders are continuing smart factory investments, allocating 20% more to those initiatives than 2019.

With Industry 4.0, connectivity is not only essential to connect machines and IIoT devices, but also to connect remote manufacturing production facilities, warehouses, suppliers and distributors to maximize operations.

Digitization and the need to connect distributed locations have accelerated the transition to the cloud, reducing the role of the data center. A traditional network infrastructure based on MPLS is no longer efficient because it backhauls the traffic to the data center, impacting application performance and scalability. Additionally, private lines are often complex and high priced compared to agile internet broadband and 5G connections. The large number of IIoT devices also creates complexity as they individually require access the cloud which in turn results in security challenges.

IT-OT convergence and cybersecurity risks

In a recent Deloitte report[6], most manufacturing organizations reported phishing and ransomware incidents in 2021. Growing cybersecurity attacks have added a business risk to manufacturing companies and 82% of manufacturing executives expect their organizations will invest more in cybersecurity in 2022, with nearly one quarter budgeting at least 10% more than in 2021.

The increase in cybersecurity attacks is largely due to smart factory initiatives, and the extensive use of IoT devices have dramatically increased the attack surface, especially because they are more numerous and difficult to protect. Manufacturing companies indeed use a myriad of operational technology (OT) devices, with very low security, and at the same time, they add new ones like cobots, that have helped provide physical distancing, allowing manufacturers to keep operating during the pandemic.

Cobot or collaborative robot, is a robot intended for direct human robot interaction within a shared space, or where humans and robots are in close proximity. The cobot and human worker share the same space but complete tasks independently or sequentially. Cobot applications contrast with traditional industrial robot applications in which robots are isolated from human contact. Industrial cobots help automate tasks such as helping people moving heavy parts, or machine feeding or assembly operations (Source: Wikipedia)

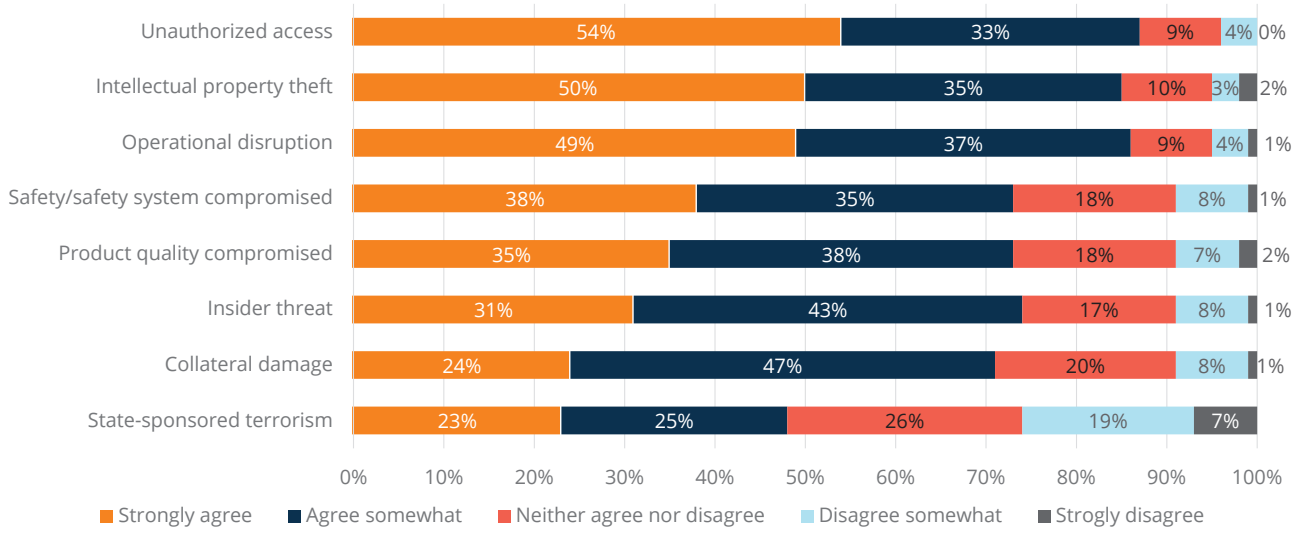
The convergence of IT and OT networks is another major concern. IT and OT networks used to be separated, but with the advent of Industry 4.0 and digitization, they are converging using the existing IT infrastructure. And they are becoming more and more complex. IT and OT security objectives are also different and pose security challenges. OT security is about protecting physical processes, safety, uptime, and efficiency while IT security is oriented on protecting all aspects of data and how information is stored, transmitted, and processed. Maintenance on OT systems can be challenging as the update for an antivirus, or any other routine tasks can require to momentarily shutdown production lines. OT are also typically not included in the SLAs of IT vendors.

In a Deloitte and MAPI smart factory study[7], manufacturing leaders are the most concerned with unauthorized access, intellectual property theft and operational disruption about their OT environment.

[5] Source: Deloitte and MAPI survey, October 2020

[6] Source: 2022 manufacturing industry outlook, Deloitte, October 2021

[7] Source: Deloitte and MAPI smart factory study, 2019



Top risks manufacturing leaders are concerned about in their OT environment (Source: Deloitte and MAPI smart factory study, 2019)

In this context, legacy networks are not suited for today's sophisticated network security challenges. Furthermore, remote working has created other vulnerabilities as employees can connect from anywhere outside of the corporate security perimeter.

Increased cybersecurity risks have made compliance to IT security frameworks critical. NIST CSF, ISO 27001 and ISA/IEC 62443 are three frameworks that can help manufacturing organizations mitigate IT security risks.

SD-WAN USE CASES SPECIFIC TO MANUFACTURING

Based on a few use cases, let's look at how adopting an advanced SD-WAN platform can help manufacturing companies accelerate digital transformation and move to a cloud-first organization.

Use Case #1: Improving network connectivity to remote manufacturing sites

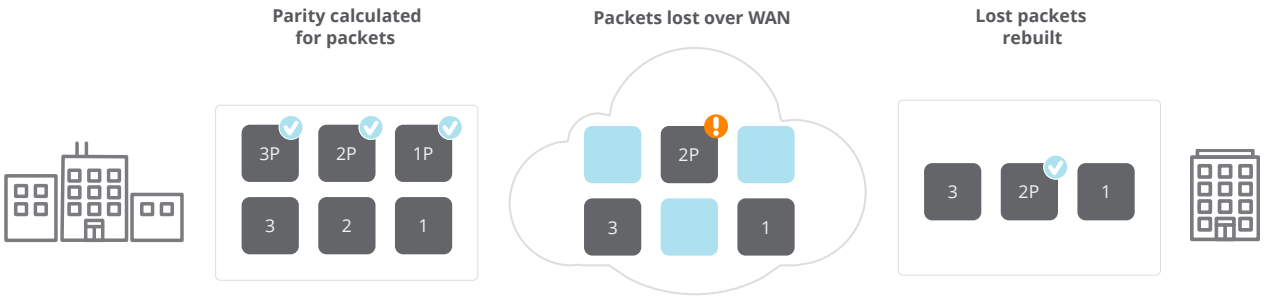
Manufacturing companies operate at global scale. Often because of their remote locations, network connectivity choices are limited and expensive, causing quality of service and network performance issues.

Poor connectivity can result in excess jitter and packet loss affecting real-time applications such as VoIP and video conferencing. Remote sites may also experience latency due to their distance from the corporate data center.

Through the virtualization of the WAN, Aruba EdgeConnect Enterprise SD-WAN is able to overcome internet and cell network limitations by leveraging various features such as **Path Conditioning and Dynamic Path Control to make efficient use of all the available bandwidth**.

Path Conditioning: With an Aruba EdgeConnect Enterprise SD-WAN, manufacturing companies can securely leverage internet broadband and 5G/LTE connections at a lower cost and get the same application performance - or even better - as when using dedicated private line services.

Path conditioning uses **Forward Error Correction (FEC)** feature to automatically reconstruct lost packets by sending additional parity packets. In addition, **Packet Order Correction (POC)** re-orders any packets that arrive out of sequence at their destination. Both of these ensure a better user experience at these remote manufacturing sites.



Forward Error Correction: packets lost in transmit across the WAN are automatically rebuilt

Dynamic Path Control dynamically selects the best WAN transport based on Link Bonding Policies. Aruba EdgeConnect Enterprise indeed combines multiple WAN transport services to create a single, higher bandwidth logical link. Link Bonding policies are configured in Business Intent Overlays and control how Aruba EdgeConnect Enterprise steers application traffic depending on business need and quality of service requirements.

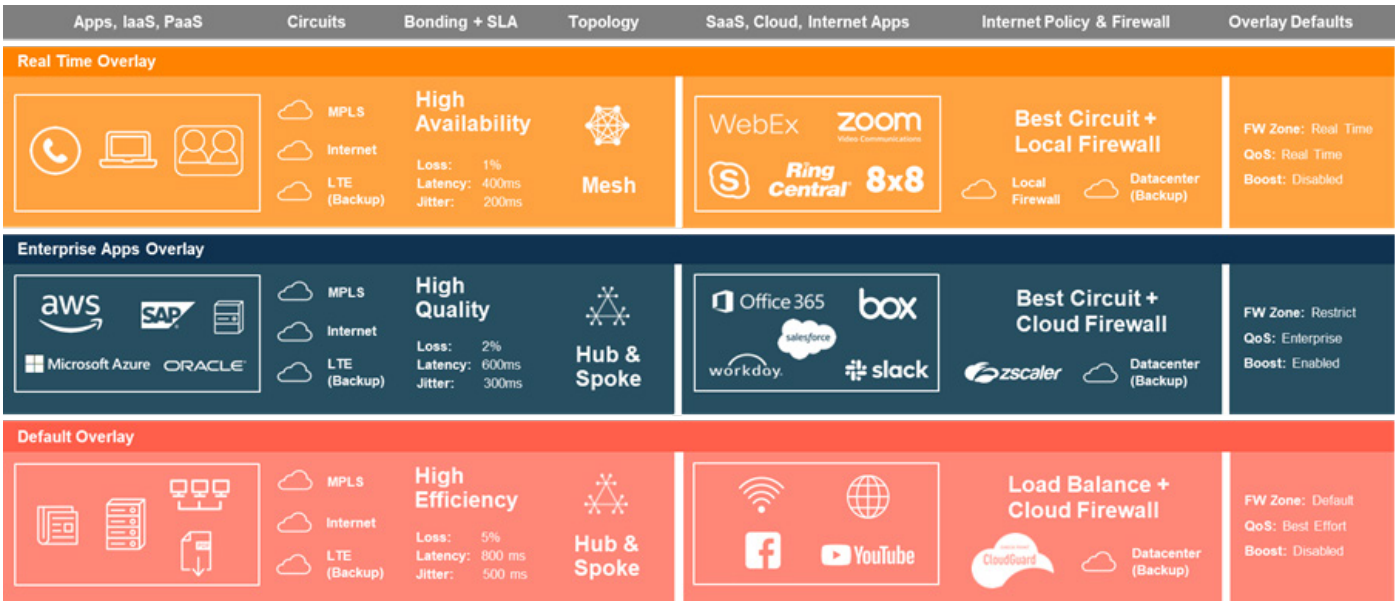
Link bonding policies include **"High Availability"** for high demanding applications such as video over IP. Data packets and error correction packets are sent over two different paths using a 1:1 FEC ratio. **"High Quality"** and **"High Throughput"** are for enterprise applications, and it applies a 1:5 variable auto FEC ratio. High Quality uses the best quality path for data, and error correction packets are sent on the second-best path. High Throughput load balances the traffic across multiple paths. **"High Efficiency"** is for recreational applications. It is similar to High Throughput, but it doesn't use Forward Error Correction.

By doing so, manufacturers can supplement an existing MPLS line, thus reducing the traffic over this line. **Additionally, expensive MPLS connections can be replaced by the reliable use of internet, satellite or 4G/5G links and deliver a private line-like experience to remote users.**

Use Case #2: Rapidly deploy new sites and simplify network infrastructure

Agility is a key characteristic of manufacturing companies as they must constantly adapt to changing business needs. Processes and business capabilities are regularly reviewed and assessed by leaders based on the evolving demand. This leads to opening new factories, closing inefficient ones, and reorganizing others. IT leaders of these organizations need to ensure that new sites are effectively connected to the network. Mergers and acquisitions, delocalization, new geographic territories and close cooperation with 3rd party suppliers are other factors that require organizations to quickly integrate new manufacturing units into their existing network.

The deployment of a new site or the connection to an external supplier can be accomplished using an MPLS connection. However, provisioning a new MPLS line can take several weeks or months, while broadband internet services are usually delivered within a few days. Additionally, organizations often don't have experienced IT staff in remote locations, so installing and configuring the WAN can be a daunting task. It is also common to find many discrete network and security appliances in manufacturing sites, including routers, firewalls, VPN concentrators and WAN optimization devices, adding complexity and difficulty in maintaining them.



Business intent overlays enable manufacturing companies to create virtual networks based on quality of service and business needs

As discussed in the previous use case, Aruba EdgeConnect Enterprise SD-WAN eliminates the need to provision an MPLS line as it can deliver private line-like performance over the internet using **path conditioning** and **dynamic path control**.

Additionally, Aruba EdgeConnect **Zero-touch provisioning** greatly simplifies connecting and deploying a new site. A local IT manager with limited IT experience can simply install the EdgeConnect SD-WAN appliance in the remote site. The solution will self-register if it has been authenticated prior to being admitted onto the SD-WAN fabric. Once authenticated, the solution automatically receives its configuration from Aruba Orchestrator with no human intervention required at the location.

Instead of taking months to deploy new sites, it just takes a couple of weeks with an EdgeConnect SD-WAN while reducing costs and improving network efficiency.

Centralized Orchestration also ensures that QoS and security policies are seamlessly enforced in the new branch. Security policies are automatically pushed to branches with zero-touch provisioning. New branches are set up quickly and easily, and security policy changes can be automatically distributed to hundreds or thousands of branches in minutes while minimizing errors.

Manufacturing companies can move from a heavy branch to a thin branch model and decrease the number of networking devices in remote locations such as routers, Firewalls and WAN optimization appliances.

Beside integrating a router and a WAN optimization solution, Aruba EdgeConnect Enterprise embeds an application-aware zone-based firewall, providing stateful capabilities. The built-in firewall also includes intrusion detection and prevention capabilities (IDS/IPS) to monitor, flag and drop traffic in case of a security threat.

Use Case #3: Accelerate file transmission and backups to disaster recovery sites

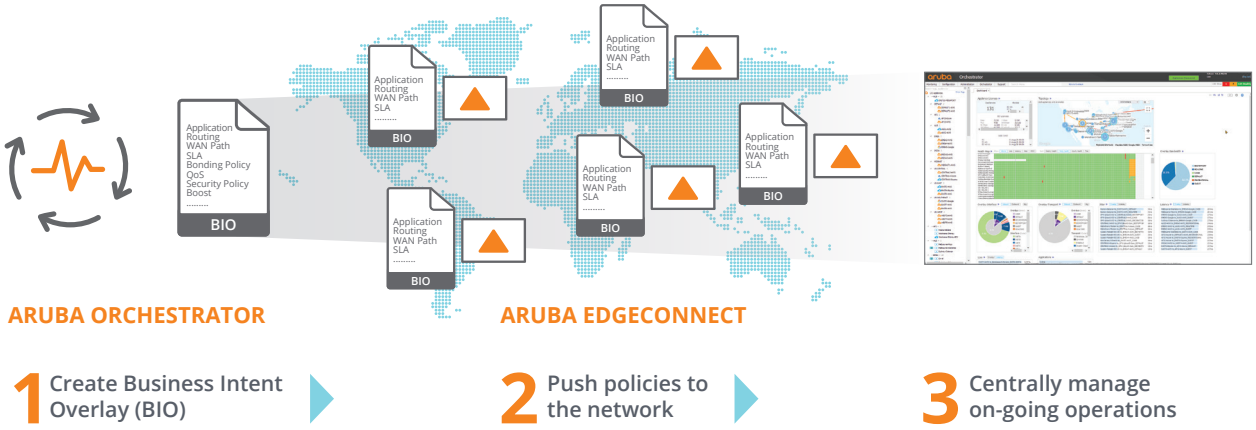
Manufacturing sites can be very far from each other causing network latency, for example a manufacturing plant can be located in China and an engineering facility in the US.

It is not uncommon for manufacturing companies to have large files that must be transmitted to remote sites, such as engineering CAD files. But large file transfers can take a long time due to the distance between the two sites. Additionally, manufacturing organizations need to perform backups to remote sites on a regular basis for disaster recovery purposes. Backups can also be long, and worst of all, they sometimes fail before they are completed.

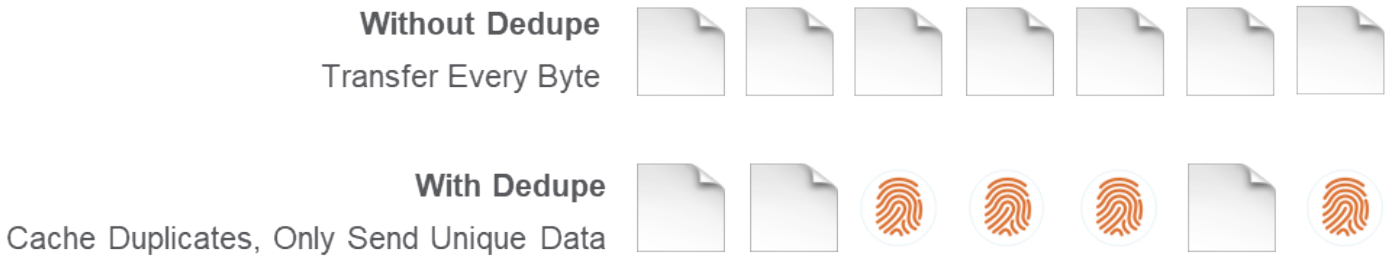
Latency, mainly caused by distance, affects network performance. Latency indeed represents the time for a packet of data to get to its destination. Latency impacts network speed and file transfers, application performance and productivity. It also affects IoT devices as it can influence the efficacy of the devices since they depend on the responsiveness of the network to work effectively.

Aruba Boost **WAN Optimization** significantly accelerates the transmission of data by applying TCP protocol acceleration as well as data deduplication and compression:

TCP Protocol acceleration: Aruba Boost TCP Acceleration overcomes delays caused by window scaling and acknowledgment procedures in latent environments.



Simplify and accelerate deployments with a top-down model and business-driven policies



Data reduction: Eliminate overhead of redundant packets traversing the WAN

Data deduplication and compression: Duplicate data is removed and replaced with a fingerprint and a pointer so that only the necessary data is transmitted across the WAN. Data compression leverages an LZ (Lempel-Ziv) compression algorithm to reduce the amount of data transmitted.

By applying Aruba Boost WAN optimization, manufacturing organizations increase the effective WAN throughput from their main locations to remote sites. They also significantly shrink backup time and accelerate file transmission. They increase replication capacity by sending more data to the recovery site while reducing bandwidth used.

Use case #4: Secure migration of applications to the cloud

To increase agility, flexibility and to facilitate work from anywhere, manufacturing companies continue to move business applications to the cloud. The migration to hybrid cloud (Public and private cloud) and multi cloud continue to accelerate, shrinking the data center. This means that there is an increasing need to simplify the process of orchestrating network traffic from on-premises to the cloud, but also from one cloud provider to another. It is also no longer viable to backhaul the traffic to the data center as it impacts application performance. The growing use of off-the-shelf cloud applications such as Microsoft 365 or Salesforce, require routing traffic closer to the user to reduce latency and the hop count.

Additionally, with employees and other stakeholders now connecting from anywhere, the security perimeter is dissolving creating increasing security gaps when accessing SaaS applications.

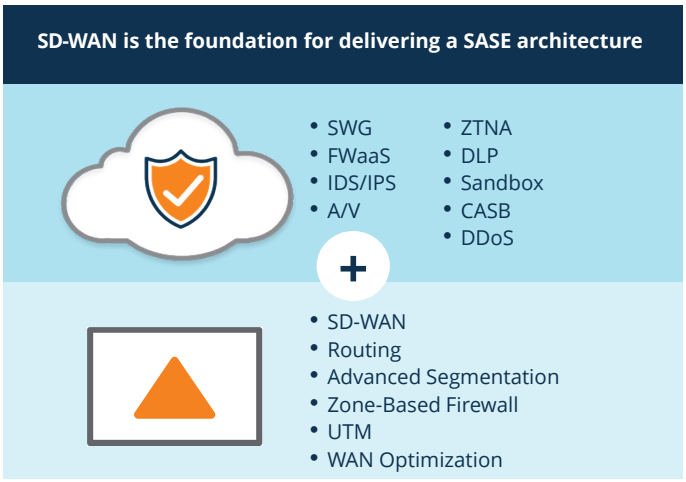
Aruba EdgeConnect Enterprise includes advanced features to support the transition to the cloud and improve security such as local internet breakout and SaaS optimization. It also supports a tight integration to a large number of cloud security vendors to implement best-of-breed security capabilities and create a solid SASE architecture.

Local internet breakout: The EdgeConnect First-packet iQ™ feature identifies and classifies applications based on the first packet, enabling intelligent traffic steering to the internet according to business and security requirements. With this feature, trusted cloud application traffic, such as Microsoft 365 or UCaaS traffic, is sent directly to the internet, while all other internet-bound traffic is sent to a cloud-delivered security solution for security inspection before it is handed off to the SaaS provider. In some cases, the traffic can be backhauled to the data center for advanced security inspection.

SaaS Express: With this feature, Aruba EdgeConnect Enterprise improves SaaS application performance. It uses statistical learning to select the best path and the closest point of presence based on advanced network health and performance measurements.

End-to-end connectivity to cloud providers: Aruba EdgeConnect Enterprise provides end-to-end connectivity to the cloud by deploying a virtual instance of EdgeConnect in any or all the four major public cloud providers. Manufacturers can also easily move workloads from one cloud provider to another, for example from AWS to Azure.

SASE-ready: With its advanced SD-WAN features, Aruba EdgeConnect Enterprise is the foundation of a robust SASE architecture. It natively integrates with leading third-party security capabilities such as CASB (Cloud Access Security Broker), SWG (Secure Web Gateway) and ZTNA (Zero Trust Network Access), enabling manufacturers to create advanced internet threat protection based on best-of-breed vendors.



An advanced SD-WAN combined with cloud-hosted security service delivers a SASE architecture that enables organizations to tackle cybersecurity threats

Thanks to the First-packet iQ application classification feature, Aruba EdgeConnect Enterprise automates the orchestration to these solutions while traffic from suspicious applications is sent to the data center for further inspection. The integration with cloud security vendors is fully automated enabling manufacturing companies to deploy security partner services in minutes.

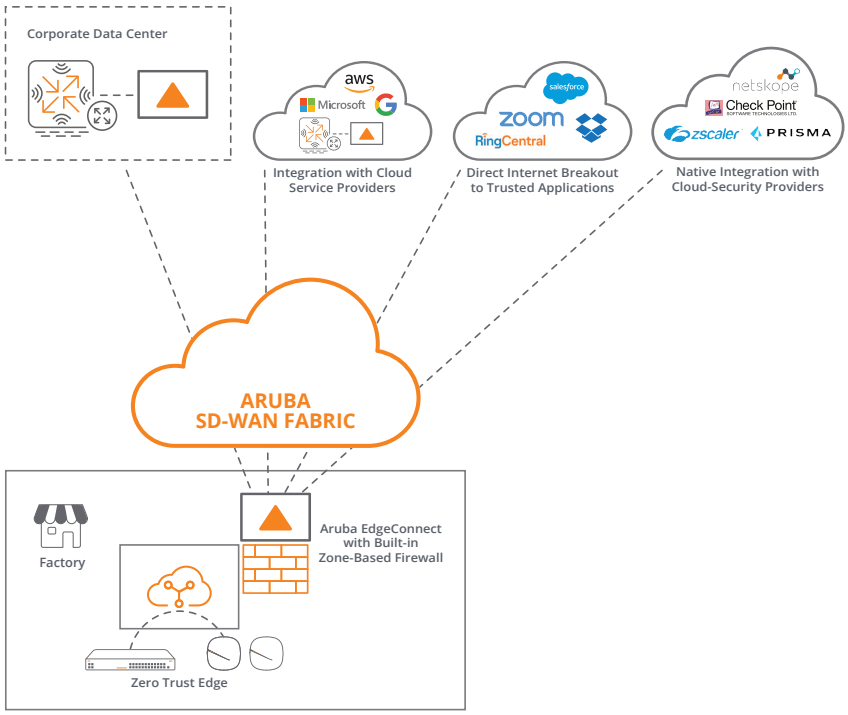
Use Case #5: Secure IoT devices with a zero-trust network

As manufacturers accelerate their path to Industry 4.0 and embrace digital transformation, IIoT (Industrial Internet of Things) has been instrumental to provide agility, visibility into operations and improving efficiency.

However, IIoT devices are difficult to secure as they cannot run a security agent and often lack authentication systems. They also become more vulnerable as they age. The security of these devices has become critical to ensure uptime and optimize business processes in manufacturing environments. Another concern is the convergence of IT and OT (operational technology). IT and OT networks used to be separate, but with the convergence of IT and OT, and the exponential growth of OT devices, the attack surface has increased dramatically, exposing manufacturers to more cybersecurity risks.

Zero trust segmentation

Zero-trust segmentation prevents an attack from spreading across the network and hitting critical applications. Aruba EdgeConnect Enterprise with Aruba ClearPass Policy Manager implements a zero-trust policy approach assuming that no user or device is trusted by default, using identity and role-based access control.



Aruba EdgeConnect Enterprise enables a SASE architecture by automating orchestration to cloud security vendors

Aruba ClearPass Policy Manager indeed adds identity knowledge of users, devices and roles with authentication capabilities such as RADIUS, TACACS+, and OAuth2 to manage network access and enable a dynamic segmentation, anywhere on the network – wired or wireless infrastructure. Through role-based access policies, IT, OT and IIoT devices are automatically assigned the proper access control policy and dynamically segmented from other users and devices.

An independent security policy may also be defined for each segment, defining the security policies to enforce for the device traffic.

Use case #6: Comply with NIST Cybersecurity Framework

Following an executive order in February 2013 by the US government due to repeated cyber intrusions, the NIST Cybersecurity framework was developed to improve cybersecurity in critical infrastructure. Critical infrastructure describes the assets that are essential for an economy to run well, and includes sectors such as transportation, public health, agriculture, and manufacturing. Version 1.0 of the framework was published in 2014, and a version 1.1 was updated in 2018 to add topics such as authentication and identity and managing cybersecurity within the Supply Chain.

The 2019 Gartner Security and Risk Management Survey confirms that 73% of organizations around the world espouse NIST CSF, while 30% of US organizations already used NIST in 2015.

	Robotics	Movement of goods monitoring	Machinery sensors	HVAC	Inventory tracking	Business apps	Data-sensitive apps
Robotics	✓	✓	✗	✗	✗	✗	✗
Movement of goods	✓	✓	✗	✗	✗	✗	✗
Machinery sensors	✗	✗	✓	✓	✗	✗	✗
HVAC	✗	✗	✓	✓	✗	✗	✗
Inventory tracking	✗	✗	✗	✗	✓	✓	✗
Business applications	✗	✗	✗	✗	✓	✓	✗
Data-sensitive applications	✗	✗	✗	✗	✗	✗	✓

Segment and isolate network traffic with zero-trust segmentation

The NIST framework is organized into five "functions", which are subdivided into a total of 23 "categories".

Functions of the NIST CSF frameworks include:

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

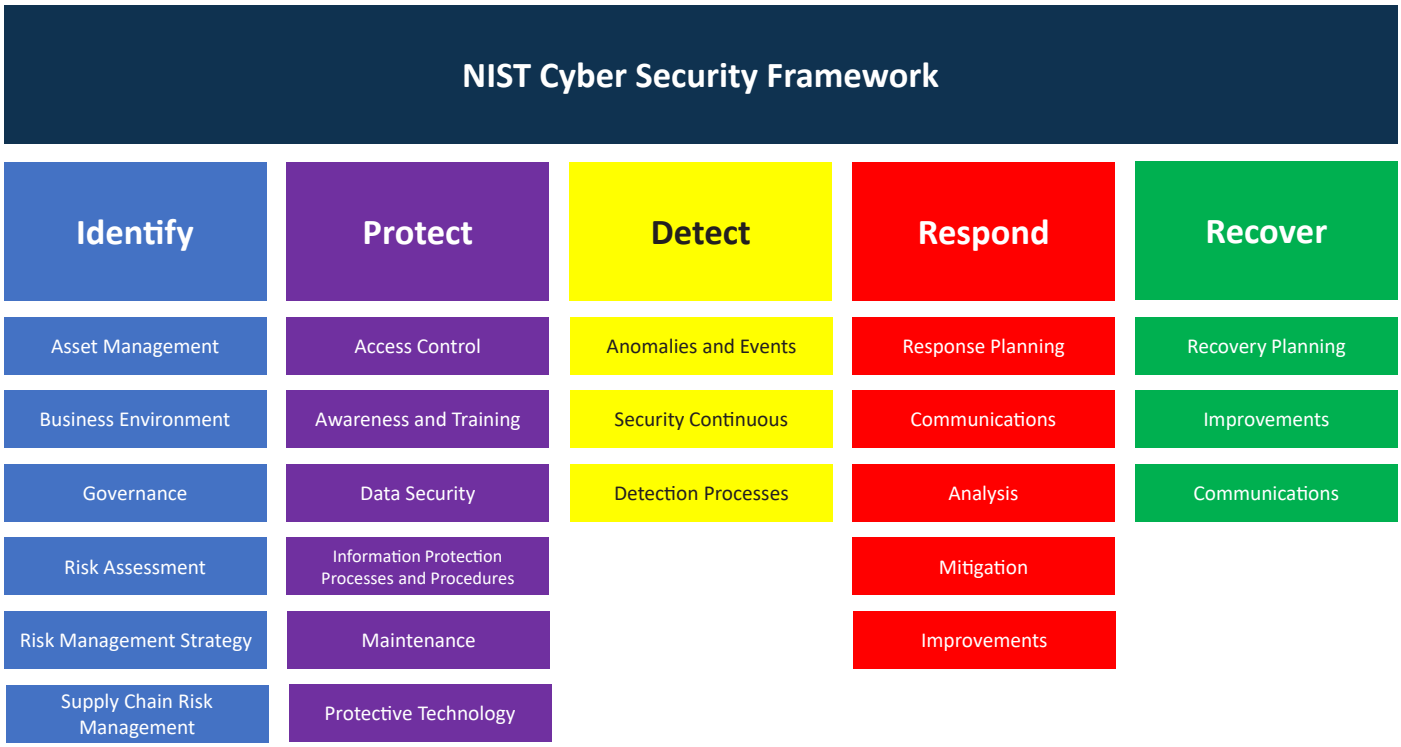
Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Aruba EdgeConnect Enterprise SD-WAN helps manufacturers achieve compliance to the NIST CSF framework with advanced network security capabilities such as zero-trust segmentation and IDS/IPS. In addition, Aruba offers other cybersecurity products to comply with this framework including:

- **Aruba ClearPass Policy Manager:** Aruba ClearPass provides complete visibility and role-based access control for IoT, corporate devices, as well as employees, contractors, and guests across any multivendor wired, wireless and VPN infrastructure.
- **Aruba PEF (Policy Enforcement Firewall):** Aruba ClearPass policies are enforced by the Aruba Policy Enforcement Firewall (PEF). PEF is also the underlying technology that enables Dynamic Segmentation. This capability extends to remote users giving administrators critical security visibility, control, and enforcement capabilities. Optionally, PEF includes a WebCC bundle for URL filtering, IP reputation, and geo-location filtering.
- **Aruba VIA:** VIA is a hybrid IPsec/SSL VPN client that automatically scans and selects the best, secure connection to terminate corporate-bound traffic. Unlike traditional VPNs which require dedicated hardware, Aruba integrates VPN services directly on existing Aruba secure infrastructure to simplify architecture and management.



NIST Cyber Security Framework with its 5 functions and 23 categories

The combination of these Aruba security products and EdgeConnect SD-WAN, provides manufacturers with the tools to accelerate compliance to NIST CSF. To achieve compliance with NIST CSF, the framework provides a reference to other standards and frameworks such as ISA 62443, ISO 27001, NIST SP 800-53.

Please refer to the table in the appendix for more details about how Aruba contributes to the compliance of the NIST CSF framework.

CONCLUSION

In a world disrupted by the COVID-19 pandemic, the manufacturing industry must now tackle major challenges. Manufacturing companies need to:

- Increase efficient network connectivity
- Support rapid migration of application connectivity to cloud services
- Secure IIoT devices in a hybrid network environment
- Ensure high application performance for critical applications from any remote site
- Reduce network infrastructure complexity

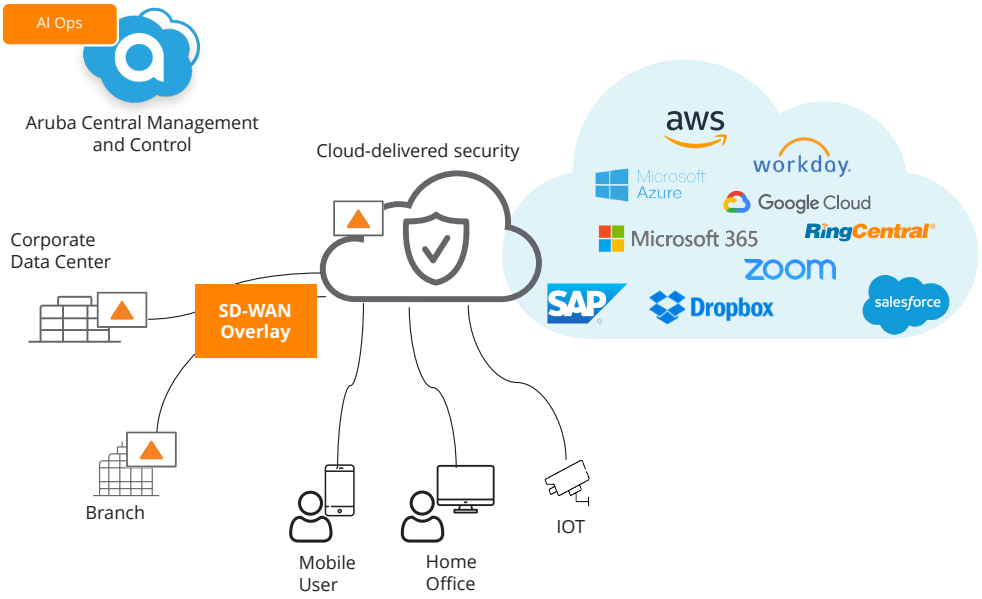
By virtualizing network connections and bonding logical links, SD-WAN allows manufacturers to leverage internet and 5G/LTE connections at a lower cost than MPLS lines while providing the same – if not better – performance, and greater flexibility and security.

Aruba EdgeConnect Enterprise SD-WAN delivers advanced SD-WAN capabilities in a single platform. It centrally manages network and security policies and can be deployed in minutes thanks to its zero-touch provisioning feature. The solution also greatly simplifies the network infrastructure in remote locations by incorporating many features such as a router, a firewall and a WAN optimization device. The solution is business-driven and intelligently routes the network traffic based on business needs and expected quality of service. It also constantly monitors network conditions and quickly adapt to deliver the best quality of experience.

Additionally, Aruba EdgeConnect Enterprise SD-WAN is cloud-ready and seamlessly integrates with all four major public cloud providers – AWS, Google Cloud, Oracle, Microsoft Azure as well as Microsoft 365 – increasing security and application performance.

With its built-in zone-based firewall and ClearPass Policy Manager, EdgeConnect can enforce a zero-trust policy approach through micro-segmentation. The firewall indeed creates a logical separation between IT and OT networks, protecting the IT network from IOT devices, and limiting the spread of cyberattacks and malware.

Aruba EdgeConnect Enterprise provides the foundation for a robust SASE architecture by natively integrating with industry-leading third-party cloud security vendors and automating the orchestration with security services. With this approach, manufacturers can select the best-of-breed security capabilities to ensure maximum protection.



Aruba EdgeConnect Enterprise is the foundation of a robust SASE architecture that enables manufacturers to choose from the best-of-breed security capabilities

Aruba EdgeConnect Enterprise is a key component of the Aruba Edge Services Platform (ESP) that enables a unified approach to centrally manage all security and network aspects including wireless, LAN and WAN connectivity with common zero trust and SASE security frameworks spanning the entire portfolio. Aruba advanced AIOPS capabilities automatically and continuously monitor network, and application performance as well as security policy enforcement, enabling automated remediation to impairments or potential threats. With this unique comprehensive security architecture, manufacturing enterprises can accelerate their compliance initiatives such as NIST CSF, ISO 27001 and ISA 62443.

The three layers of Aruba Edge Services Platform

APPENDIX

Contribution of Aruba to the NIST CSF framework

Function	Category[1]	Aruba Contribution
IDENTIFY	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	Aruba ClearPass Device Insight provides device discovery and automatic device classification based on machine learning. Aruba ClearPass Policy Manager supports role-based, unified network access enforcement across multi-vendor wireless, wired and VPN networks. Authorizations are established based on a wide variety of factors including org role, devices used, etc. It Supports a vast number of protocols such as TACAS+, RADIUS and OAuth2.
PROTECT (PR)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Aruba EdgeConnect and Aruba PEF embed advanced firewall capabilities that include IPS, malware protection, URL Filtering, IP reputation and Geolocation filtering to identify threats.
	Identity Management and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	Aruba ClearPass provides role-based access based on organization policies and authentication capabilities such as RADIUS, TACACS+, and OAuth2 as well as multi-factor authentication. Aruba VIA is a hybrid IPsec/SSL VPN that provides secure connectivity over public and private cloud. Aruba EdgeConnect Firewall offers network segmentation, combined with advanced intrusion prevention capabilities.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	With Aruba EdgeConnect Enterprise SD-WAN, data in transit are protected using 256 bit AES encrypted tunnels. Data at rest used by Aruba Boost WAN optimization network memory is encrypted using AES-128. Network segmentation enables the separation of production environments from development and testing environments. Aruba VIA provides VPN connectivity using a wide range of encryption protocols such as AES256 and IPSec IKEv1.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	A zone-based firewall and network segmentation capabilities provide isolation and protect critical parts of the network. Intrusion prevention capabilities monitors the network for malicious activities. Threat events are streamed to Security Information and Event Management (SIEM) systems for log review.
	solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	Aruba EdgeConnect Enterprise provides visibility and monitors the network. Event logs collected are sent to Security Information and Event Management (SIEM) external tools for further analysis.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	Aruba ClearPass detects and prevents unauthorized access. Subscription for URL filtering, IP reputation and Geolocation filtering is available in Aruba PEF to detect potential cybersecurity events and malicious files.

APPENDIX

Contribution of Aruba to the NIST CSF framework

Function	Category[1]	Aruba Contribution
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities.	Security dashboard includes threat metrics by type and geography. Threat intelligence services are available to classify and score incidents including URLs and IP reputation. Threat events are streamed to key security monitoring tools such as Security Information and Event Management (SIEM) systems
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	Once an attack or incident has been identified, the ClearPass position as "gatekeeper" of the network can be used to either manually or automatically take actions to contain it. Actions that ClearPass can take include: re-authentication, bandwidth control, quarantine and block. With Aruba EdgeConnect Enterprise, network administrators can define security policies to deny certain network zones and deny the traffic from one zone to another. Using WAN hardening, no traffic is allowed in and out of site that is not IPSEC tunneled. Aruba PEF can automatically change the permissions associated with the user or device by changing the role. Attack responses can include a range of actions from bandwidth reduction, quarantining and outright block.

Note 1: The categories below from the NIST framework are not in the table as they are considered business requirements, and not technical. For more information, refer to the NIST CSF framework.

The NIST framework lists the correspondence with the CIS CSC, COBIT 5, ISA 62443, ISO/IEC 27001 and NIST SP 800-53 frameworks by subcategories. There are 23 categories and 108 subcategories in total. For more information, please refer to the Framework for Improving critical Infrastructure Cybersecurity paper.

Function	Business requirements category not listed in the table above
Identify	Business Environment (ID.BE), Governance (ID.GV), Risk Management Strategy (ID.RM), Supply Chain Risk Management (ID.SC)
Protect	Awareness and Training PR.AT, Information Protection Processes and Procedures (PR.IP)
Detect	Detection Processes (DE.DP)
Respond	Response Planning (RS.RP), Communications (RS.CO), Improvements (RS.IM)
Recover	Recovery Planning (RC.RP), Improvements (RC.IM), Communications (RC.CO)

TP_SD-WANforManufacturing_SK_042522 a00122841enw

Contact us at www.arubanetworks.com/contact