White paper
Cisco public

The bridge to possible

Hybrid Cloud Industrial DMZ

Driving industry digitization at scale

The Industrial Demilitarized Zone (iDMZ) is a critical layer in a comprehensive end to end security strategy for an industrial operations environment. One of the challenges with an exclusively on-site iDMZ is the limited ability to meet future demand in a world where the growth of Industrial IoT (IIoT) and IT/OT/cloud convergence requires new capabilities. It can also become challenging for operations staff to maintain iDMZ consistency across multiple sites and deliver consistent security policies.

A hybrid cloud iDMZ model can be an alternative. Like an iDMZ deployed on premises, it provides a holistic security strategy, with the benefit of shared resources and assets, allowing for a more repeatable and consistent architecture, as well as easing the operational overhead and complexity. Finally, a hybrid cloud iDMZ aligns with the concept of the ROC (Regional Operations Center), which is top of mind for some industrial organizations, especially those with a global footprint.

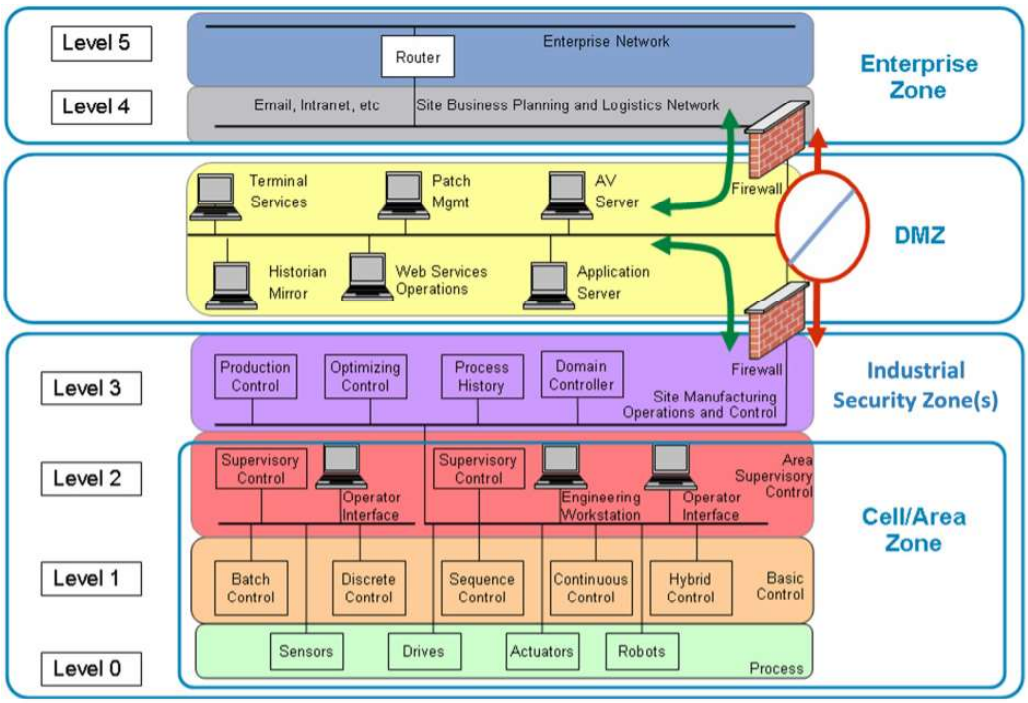
Evolving requirements and the industrial DMZ

Industrial operators and companies face multiple challenges related to productivity, skill retention, cost cutting, and competitive pressure, to name a few. Related to all these are the technical challenges of deploying advanced technologies to help address those issues. For example, collaboration technologies solve concerns related to skill shortages through remote-expert functionality, or what's commonly named "expert on demand" (XoD). Industry 4.0 is highly dependent on having access to operational data, ingesting it from multiple domains (even geographies), and analyzing it for the purpose of insight and predictive maintenance. In this context, security (with all its derivatives) becomes the most important puzzle to solve. In essence, proper deployment and configuration of security enables productivity, collaboration, and cost reduction.

As with any discussion about the industrial environment, the Purdue Reference Model as specified by the ISA95 and ISA99 standards helps put things in perspective. DHS, NIST and NERC provide guidance around similar architectures and reference models, especially as they pertain to the role of the Industrial Demilitarized Zone (IDMZ). Although the model describes six functional layers or levels, it separates the industrial support operations into three main areas:

1. **The enterprise zone** describes the plant or IT-controlled environments, including corporate data centers, LAN, WAN, and business application hosting.
2. **The Industrial Demilitarized Zone (IDMZ)** is the buffer between the critical environments or production floor systems and the enterprise network. All shared services between the industrial zone and the enterprise zone will be located at the IDMZ.
3. **The industrial security zone** is home to critical operations systems including the cell/area zone, where communication is frequent and on a low-latency or real-time basis. Since this document is mainly concerned with the IDMZ, we will skip detailed coverage of the cell/area zone.

Figure 1. Layers of the Purdue Reference Model



Given the strict security requirements of the various zones, security technology limitations, the different data access requirements, vendor access requirements, and the criticality of the environments, the IDMZ has become the most important area of focus for IT/OT convergence.

With the Internet of Things (IoT) came lightweight sensors and lightweight communication protocols, combined with the need to acquire and transmit high volumes of data to the data center or the cloud for further analysis. In addition, the sophisticated nature of next-generation industrial equipment and assets, and the wider adoption of process optimization, brought about the need to provide the OEM access to the environment for maintenance and performance services. The combined effect of the above created new pressures and requirements that demanded higher levels of flexibility, simplicity, and deterministically consistent security at the IDMZ to provide much-needed control while supporting data movement between the industrial and enterprise zones, as well as third-party vendors and ecosystem partners.

Also noteworthy are the pressures on the data center to handle Manufacturing and Execution Services (MES), Enterprise Resource Planning (ERP) applications and collecting massive amounts of data (from operations), improve flexibility, extend reach, and reduce costs, leading IT organizations to move their critical data management efforts to the cloud. Based on some of the latest statistics, the cloud continues to gain momentum and unlock value for enterprises, both in savings and in advanced computational capabilities. In addition, we see cloud operators extending their reach to the edge and improving access, allowing for both low latency and optimized performance. In some cases, performance exceeds that offered by hosting critical business applications privately or within enterprise data centers.

IDMZ can gain tremendous benefit from operating in hybrid infrastructures

Based on the aforementioned logic, we anticipate that the IDMZ (and eventually industrial operations) can see tremendous benefits from a hybrid cloud solution.

Misconceptions of the cloud

While many enterprise customers are well on their way to leveraging cloud services and capabilities, industrial operators have been slower to adopt cloud technology. Much of the reluctance may be attributed to the exposure of the industrial operation to a WAN, potentially increasing the attack surface. In some circumstances, having outside connectivity has led to operations being compromised, as has been highlighted in the media over the past decade. Whether it is perceived as not possible to sufficiently secure the industrial zone, or some other point of concern, here are a few common misconceptions related to cloud:

Cloud is an all-or-nothing concept, requiring all services and applications to be fully cut over to the cloud provider. In today's world, there is no single cloud. It's a multicloud world, where organizations use multiple cloud services from multiple providers. Hybrid clouds are infrastructure combinations of two or more clouds, such as on-premises private and public clouds, that can be centrally managed to enable interoperability for various use cases. A cloud migration strategy can be tailored to slowly migrate data and applications from an on-premises architecture to the cloud. Not all workloads benefit from running on cloud-based infrastructure; however, the IDMZ is one that gains tremendous benefit.

It is not possible to fully secure or protect data and applications hosted in a hybrid cloud environment. With the global availability of multiple public cloud providers, we have the freedom to choose what stays on-premises and what lives in the cloud. While connecting to all those clouds is easy, managing the different environments can get complicated. Cisco uses a defense-in-depth approach in which protection is added to all layers of the business. Whether it be industrial visibility with Cisco® Cyber Vision, segmentation with Cisco Secure Firewall, or application protection with Cisco Secure Workload, Cisco security delivers a broad, effective security solution for a multicloud world.

Cloud primarily benefits the IT organization and provides little benefit to the industrial operation. An important driver behind the formation of hybrid cloud and hybrid IT architectures is the access to public cloud services. Organizations have been extending their on-premises environments to the public clouds to enable their development teams to benefit from platform offerings and reduce time to market when building applications. The rate of innovation for industrial operations vastly increases when they are part of a multicloud ecosystem.

It is not possible to enforce or maintain application and Service-Level Agreements (SLAs) when hosted from the cloud. Cloud and application monitoring tools, such as Cisco AppDynamics®, ThousandEyes, and Cisco Secure Cloud Analytics, work in real time alongside their on-premises and hybrid counterparts, providing the ability to measure and visualize application and network-layer performance between hybrid cloud, private cloud, and public cloud services. These tools can be leveraged when unifying large volumes of data across distributed locations, identifying anomalies and their root causes, and predicting potential risks or production outages.

While there may be some reluctance to use cloud services to support the operation, it does not negate the benefits cloud can bring, even to an industrial operation.

Cloud benefits

Benefits of the cloud include:

Elasticity, scalability, and cloud bursting. Cloud services are scalable and elastic in nature, allowing applications and services to easily expand and contract based on real-time demand. This is known as cloud bursting. The services provided by the different cloud providers, with some minor exceptions, are available globally and can be scaled according to fluctuations in demand, providing a consistent experience and the potential for uniformity in how a customer leverages those services.

The cloud allows for the rapid deployment of resilient and highly available services with a global footprint

Efficiency. Leveraging the cloud allows for the rapid deployment of resilient and highly available services and applications, based on the robust and redundant tools and resources accessible within the cloud environment. Since the responsibilities and maintenance of the physical hardware and underlying infrastructure are removed from the customer, the deployment of applications and tiered services can more readily be scripted and automated to quickly address evolving demands and new requirements from the business, while minimizing operational overhead and driving efficiency.

Global availability. There are multiple public cloud providers offering a variety of comparable services. Each cloud provider has an extensive global footprint and provides a consistent menu or set of services within each of the major theaters: Americas, EMEAR, and APJC. As an example, whether an office is in Germany or the United States, it is possible to consume the same services, helping drive consistency across the operation. In addition to delivering a consistent set of offerings globally, cloud providers are able to distribute services closer to the cloud edge, making it possible to push applications and content closer to the end user/consumer, which can facilitate the efficient and expedient movement and delivery of data.

In addition to the general benefits of cloud technology, there are unique benefits that can be realized by industrial operators.

Reducing onsite personnel. A primary concern for industrial operators is keeping personnel out of the "line of fire," with on-the-job and onsite safety being paramount above all else.

First, reducing noncritical applications and services hosted onsite and moving them to the cloud helps decrease capital expenditures. An operator can reduce the hardware footprint that is repeated on a per-site basis, along with the power, cooling, and space requirements, which can be extremely challenging and limited for operators in some industries.

In addition, personnel resources responsible for maintaining the onsite hardware and applications can be moved to a remote location, such as a regional operations center, thus reducing the number of people onsite and exposed to operational conditions. As an example, an operator capturing machine or vehicle telemetry data for predictive maintenance or process optimization may have personnel onsite to perform these activities, as well as to analyze data and maintain back-end systems and data repositories. However, moving telemetry services to the cloud enables associated personnel to be removed from the site, thereby helping limit the site to more key, mission-essential personnel.

Moving the IDMZ to the cloud streamlines communication and reduces downtime for operations

More efficient alignment with ecosystem partners and the supply chain. Through moving the IDMZ to the cloud and allowing the operation to have more direct control over assets, compute resources, and even connectivity, the industrial operator is now able to establish and securely manage direct connections with ecosystem partners offering services that allow the operation to perform more efficiently, or perhaps to provide insights that the operation was not capable of attaining on its own.

Returning to the previous example, if an operator wanted to analyze vehicle or machine data, previously it would need to add servers to store that data, compounding the costs of hardware, power, cooling, and trained personnel. In some cases, this equipment resided on-premises within an industrial setting, which could require escorted access and additional safety training to access it.

Moving these activities to the cloud not only affords an operator the opportunity to take advantage of the elasticity and scalability of the cloud and removes the responsibility of having hardware to maintain, but it also streamlines communication and facilitates the sharing of information with partners for applications such as predictive maintenance, as well as opens the potential to consume new Software as a Service (SaaS) or other services that can benefit the operation.

Independence from the enterprise network. For some industrial operators, the operation has grown organically over time, which has resulted in an environment shared by IT and OT, with limited controls and policies in place, providing an unclear demarcation between IT and OT assets and the operation.

The lack of a clear architecture, sharing of assets, and OT asset tenancy within the enterprise data center, as well as the inconsistency in how policies may be enforced across multiple locations and facilities, can result in increased risks and challenges to the operation, as maintenance schedules and administrative responsibilities can be misaligned or divided. Unfortunately, this can result in unwanted downtime for the operation, especially if it runs 24/7, or it could open backdoor vulnerabilities due to circumventing IT-developed security controls not aligned to the needs of the operation.

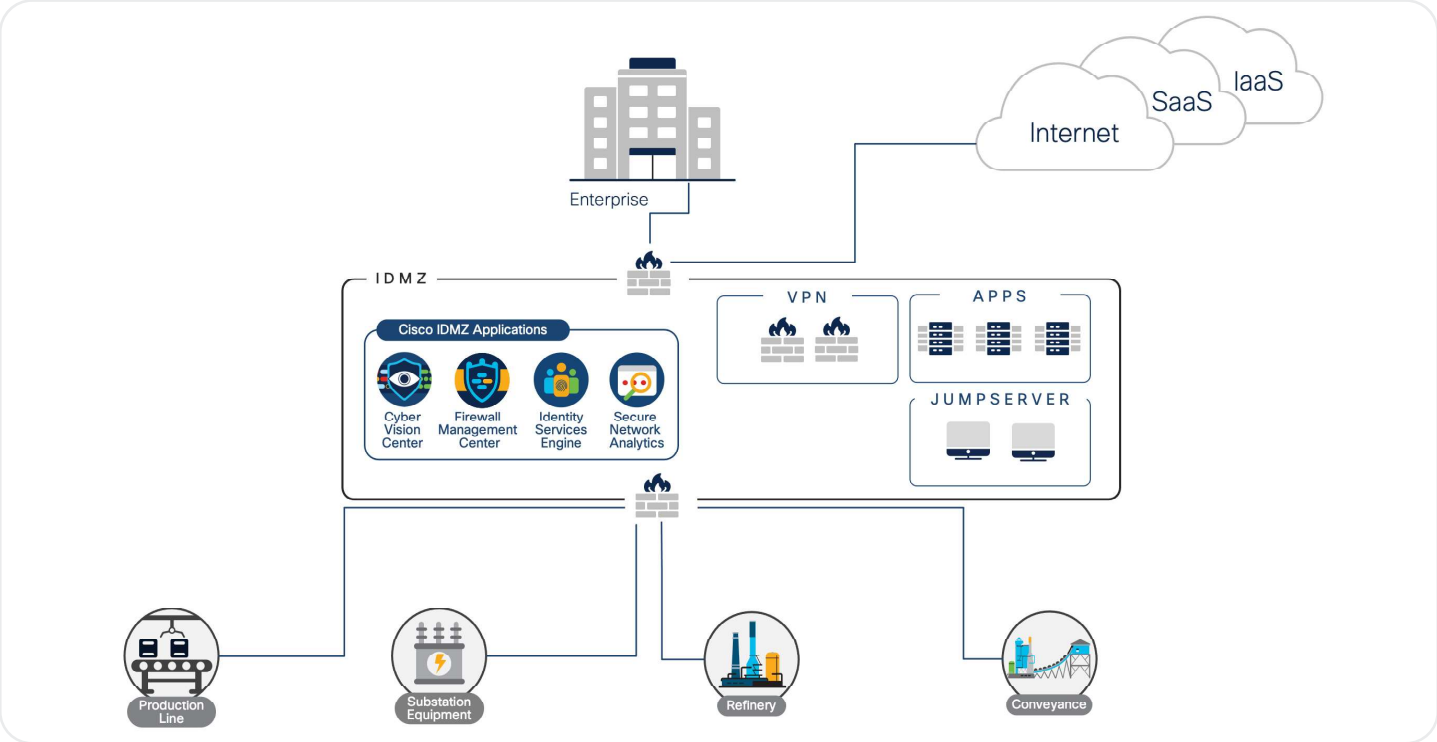
Moving services to the cloud could facilitate the decoupling of IT and OT assets and allow operations to have more control over the assets supporting the operation and the maintenance of those assets and establish centralized security policies aligned to the needs of the business. What this ultimately means is that OT can establish some degree of independence from the IT organization. Not only does this enable OT to manage its own compute resources, applications, and assets, it also allows OT staff to perform maintenance and administrative tasks based on a schedule and routine that better conforms to the operational tempo.

This could also result in OT-managed WAN services and connectivity, with the potential for OT not only to develop policies that align better to running the business, but also to manage its own WAN connectivity to consume SaaS offers, allow for remote connectivity for things like remote expert, or for tighter alignment to OEMs and other ecosystem partners who are offering their own cloud-hosted services or applications. Finally, instead of running leased lines and circuits directly from the enterprise into the operations facility through an on-premises IDMZ, that same connectivity can be facilitated through the cloud IDMZ, where the enterprise is essentially treated like another XaaS or application provider, where applications like Manufacturing Execution System (MES) and Enterprise Resource Planning (ERP) are commonly shared.

Hybrid cloud IDMZ

For industrial operators seeking opportunities to leverage cloud services for their operation, one area worth exploring is the deployment of the IDMZ in the cloud.

Figure 2. Deploying the IDMZ in the cloud



Services hosted in the IDMZ are not critical to the operation of the business. In industrial networks, determinism and continuity of operations are critical. There is an unwillingness to establish dependencies on resources and applications that may be outside the administrative purview of the operations team. Applications and operations within the industrial zone, consisting of levels 3 and below in the Purdue model, are critical to the operation of the business and likely need to remain on-premises. In contrast, the enterprise zone, associated with levels 4 and 5 of the Purdue model and maintained by the IT organization, could reside in a corporate location remote from the operation.

So whether there is a security event or a disruption in connectivity, an industrial operator should be able to sever its connectivity with the outside world and still maintain the ability to run the operation. Many of the applications and services hosted within the IDMZ, while important to the overall operation, do not have stringent SLAs or latency or real-time requirements, and therefore there is flexibility as to where these services and applications can be deployed.

Consistent policy across remote sites. Traditionally, the IDMZ is repeated per remote facility. Centrally locating the IDMZ allows for more efficiency and economies of scale. A process or manufacturing operator with multiple facilities and installations positioned within the same geographic area may treat each facility independently, with its own on-premises IDMZ security stack.

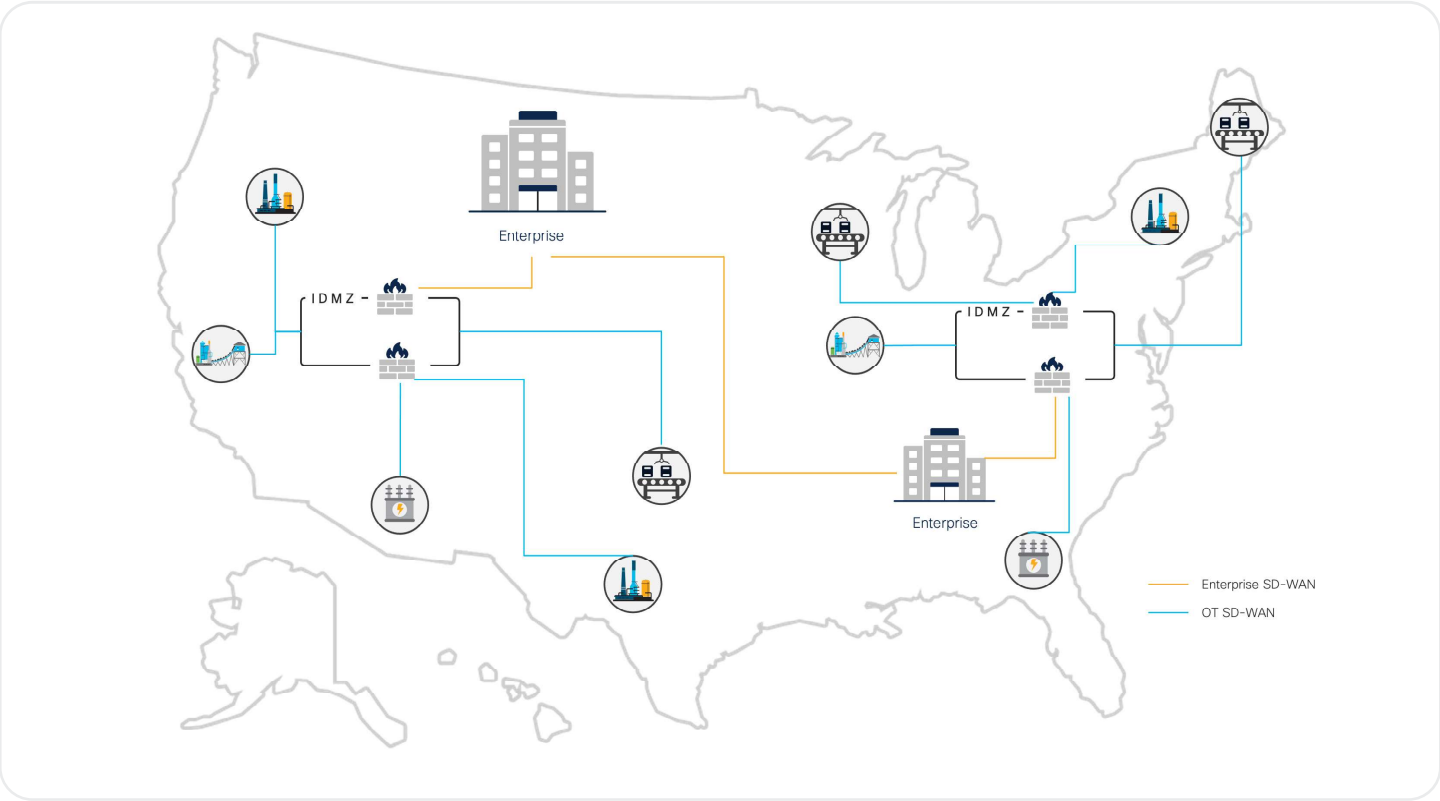
From a physical hardware standpoint, it is possible for the same physical hardware footprint to be consistently deployed across all locations. However, it is more likely that technology decisions will be delegated to the local site manager, and the hardware composition across sites can thus be very different. Added to this, there is no guarantee that a consistent set of policies will have been established across all locations, leaving potential gaps in the overall security strategy. With a single centralized, regional IDMZ solution, not only is it easier to create a homogenous and uniform security deployment, but it is also easier to enforce a consistent set of policies across multiple sites.

A centralized IDMZ solution makes it easier to enforce a consistent set of policies across multiple sites

Regional Operations Center. A Regional Operations Center (ROC) provides broader visibility across multiple sites and facilities within a region. A ROC decreases the headcount on site, improving the overall site safety and easing some costs, especially in a fly-in/fly-out situation. The idea of moving the IDMZ to the cloud supports the concept of the ROC model, in which the IDMZ leverages a multipronged layered security approach and is shared between sites across a given region.

The resources deployed within a hybrid cloud IDMZ are managed by a regional security team, promoting consistency from a policy development and enforcement standpoint, offering visibility to traffic originating from and destined to the different sites homed to the regional IDMZ, and enabling the operation to take advantage of the elastic services and capabilities of cloud infrastructure.

Figure 3. Regional IDMZs



It is important to stress that the deployment model being presented focuses on a central hub for a given geographic region, leveraging the global availability of cloud services offered by public cloud providers. Different strategies can be developed to define the size and scaling of the regional model. If an operator has facilities dispersed around the globe, the concept of a regional hub would be repeated per geographic area, with a group of facilities homing to their closest regional hub location. It should also be noted that a regional IDMZ would be deployed in a highly available configuration, as either active/standby or active/active.

Environments can be created with the appropriate virtualization and security controls within the IDMZ dedicated to specific partners and OEMs. This allows partners and vendors the opportunity to administer their own virtual space for managing and analyzing shared data or hosting specific services to the operation. Within these virtual environments, data lakes can be created to facilitate the collection and analysis of data. Since data would be aggregated from multiple facilities, unique insights can be derived both at the regional level and/or at an individual facility. From a regional standpoint, the IDMZ may service different types of facilities and therefore leverage different partners and/or machine/equipment vendors. In addition, each region may have different regulatory and compliance requirements it needs to conform to. Therefore, customization can be performed at the regional IDMZ level to adhere to local regulations and requirements.

A related point is that since every partner or contractor may not have a virtual presence within the IDMZ, the cloud IDMZ environment provides a scalable solution for managing remote connectivity, such as VPN connectivity for remote experts or a direct interface point for OEM and third-party entities offering services such as SaaS. Again, these connections can be centrally monitored and managed by ROC personnel, who can customize the solution based on the relationships and requirements for the region where it is deployed.

The hybrid cloud IDMZ offers tremendous flexibility and resiliency

As all connections come through the hybrid cloud IDMZ, not only does this manage third-party and outside connectivity and services, but it is also a way for the operation to control how corporate connectivity, applications, and data are shared. This provides a clear and concise security strategy regardless of who or what is connecting and minimizes the potential for backdoor connections that might circumvent security controls.

Finally, the hybrid cloud IDMZ, since the solution is software based, offers tremendous flexibility and resiliency. First, if a facility needs to isolate itself from the outside world, it can quickly do so by disabling its connection to the IDMZ. Since mission-critical and real-time functions continue to reside on-premises, it would be assumed that removing the outbound connectivity would offer no disruption to the actual operation. Once the problem is addressed, connectivity can be restored. In the extreme case where a catastrophic event impacts the IDMZ, rendering it nonoperational, since the IDMZ is not based on a physical location and/or set of hardware, with the assistance of automation it would be possible to eliminate the compromised IDMZ and rapidly instantiate a new IDMZ to maintain continuity of connectivity, minimize downtime, and quickly restore service.

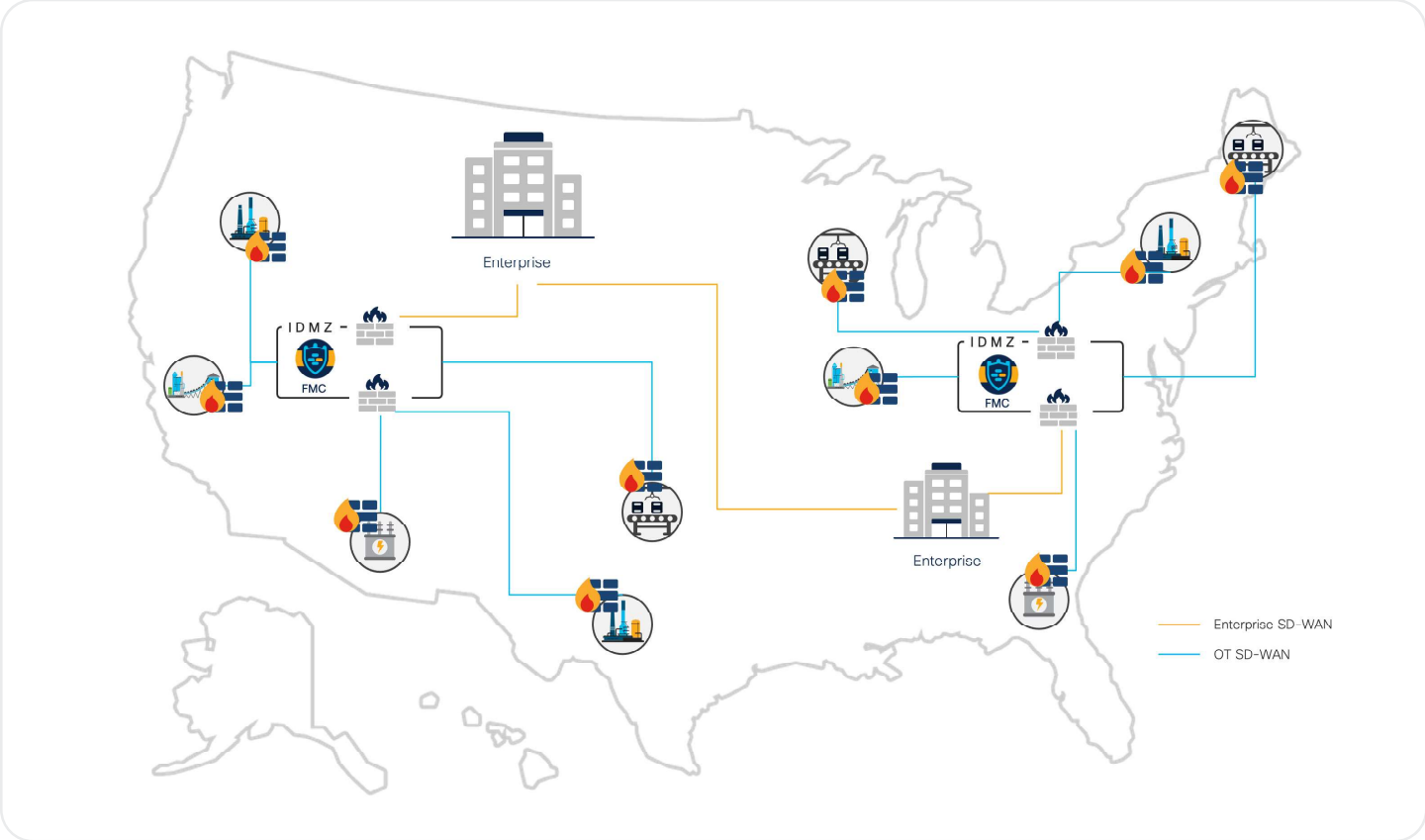
The ROC model unlocks numerous opportunities for driving consistency and operational efficiencies. A hybrid cloud IDMZ offers the ability to aggregate data across multiple sites for performing analytics and predictive maintenance, provides the ability to maintain consistent policy across different sites, and allows operations to make better-informed decisions, navigate around unforeseen challenges, and more accurately focus on the needs of the business.

Hybrid cloud IDMZ in practice

No single product, technology, or methodology can fully secure Industrial Automation and Control System (IACS) applications. Protecting IACS assets requires a defense-in-depth security approach that addresses internal and external security threats. Many design and implementation guides, including the Converged Plantwide Ethernet (CPwE) guide developed by Cisco and Rockwell Automation, detail the recommendation for a physical IDMZ to recognize application traversal between the industrial and enterprise zones. However, the modern network calls for a new approach, one that can leverage the cloud.

It is common for a corporate engineering team to support multiple sites. Today, sites may be managed separately, with an architecture team providing the blueprint of how sites should be implemented and onsite personnel implementing and maintaining the networks. As people move on and requirements change, sites begin to drift from their intended designs. Let's take an example in which security controls have been defined for northbound communications from the industrial zone. These policies, communicated via documentation to the individual sites, are implemented on the local firewall by the resident security expert. Even if firewall logs are sent to a Security Information and Event Management (SIEM) system, to gain full insight into these networks, the Security Operations Center (SOC) must access each individual site to audit the security measures that have been put in place.

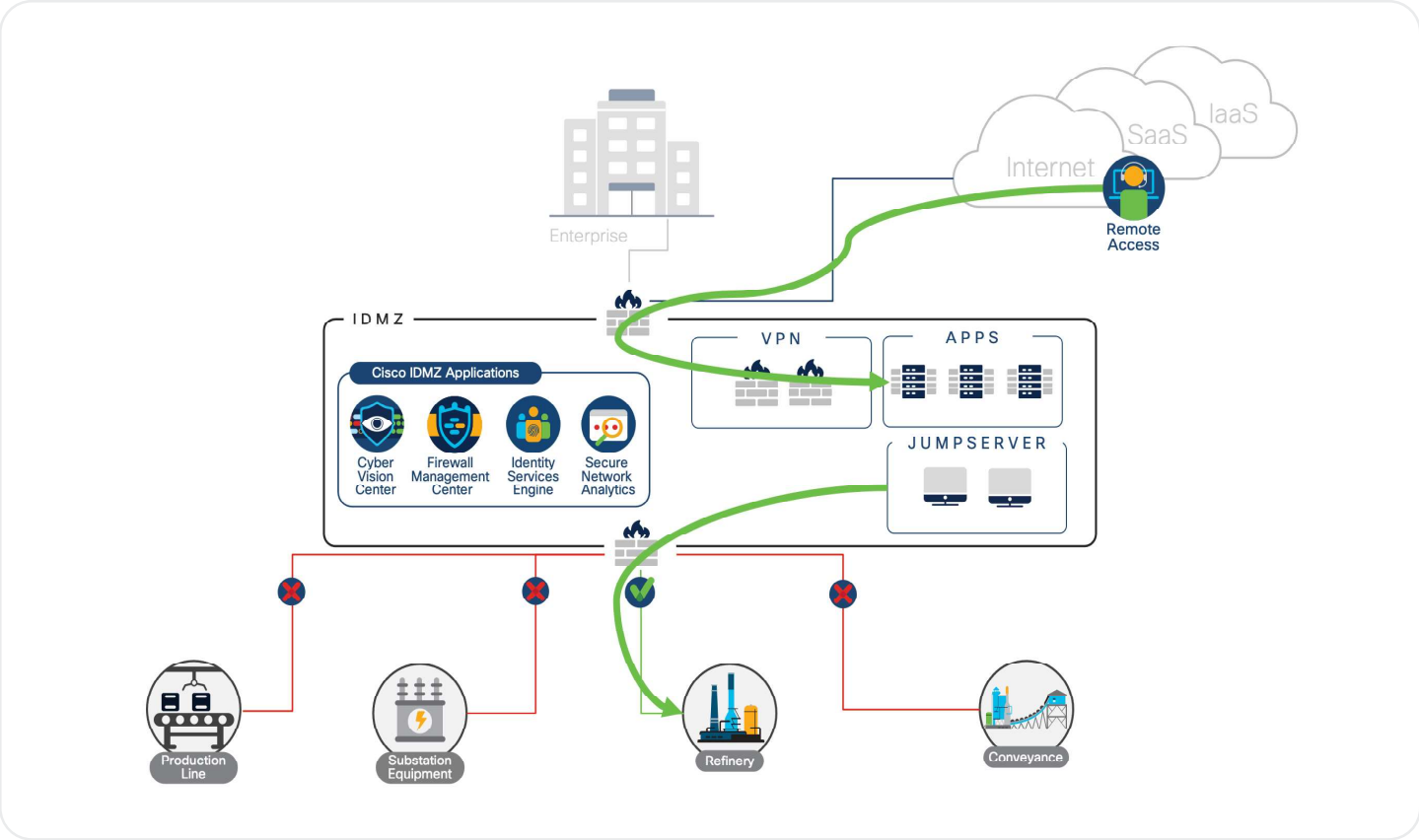
Figure 4. Centralized firewall management



By moving firewall management to a centralized IDMZ model, security operators gain a consolidated view of all security activity at each location they manage. Changes in policy can be deployed uniformly across all locations, and unique site deviations can be tracked from a single management platform.

Secure remote access is another use case that can benefit from a hybrid cloud IDMZ. When an IACS device is down or needs advanced troubleshooting, a remote expert may need to access the device and do further analysis.

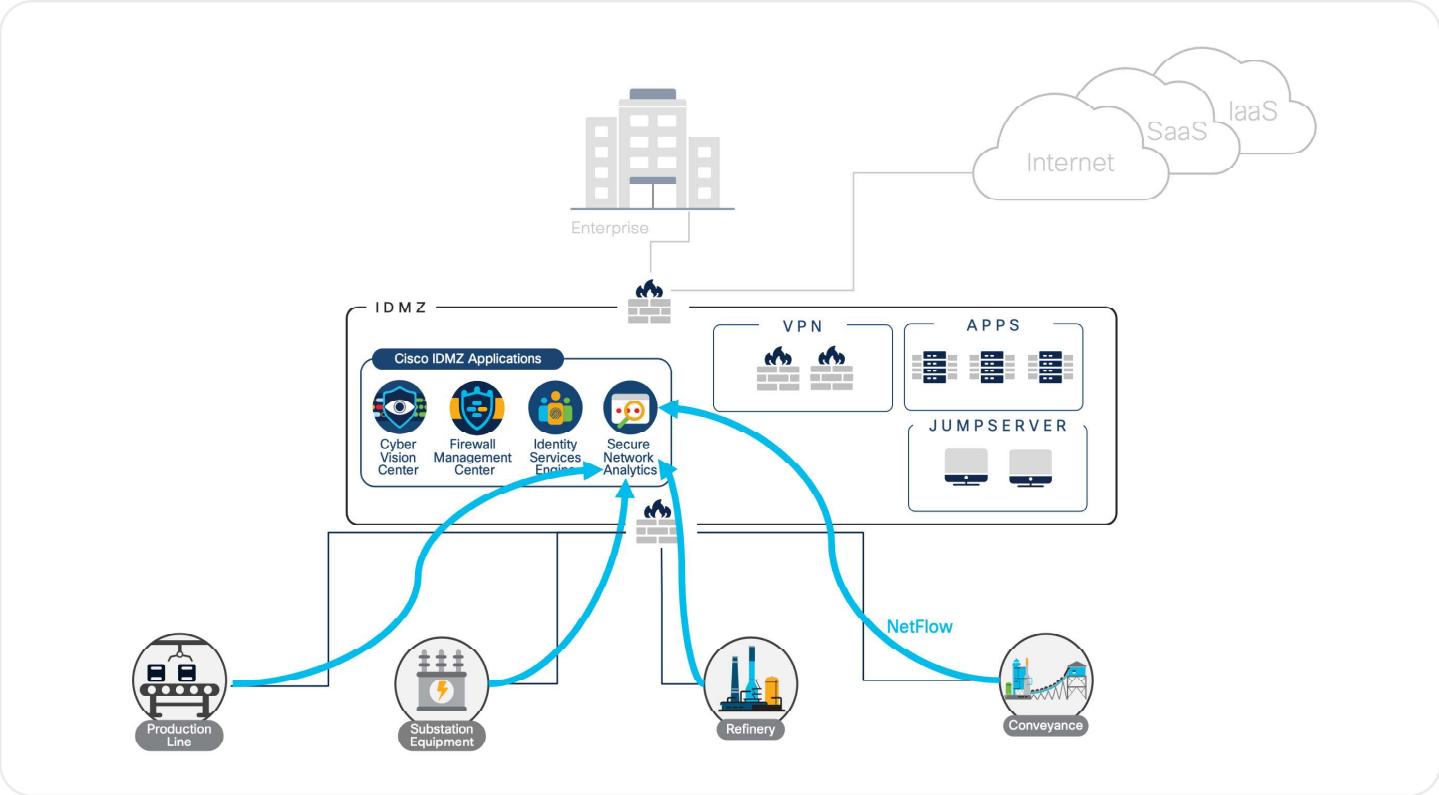
Figure 5. Secure remote access with a hybrid cloud IDMZ



The principles of secure remote access remain the same—use a VPN client to reach the remote access network, use Multifactor Authentication (MFA) to verify user identity, and make use of jump servers to control the device that vendors use during remote sessions. However, controlling access through a hybrid cloud IDMZ provides a single access point through which all connection attempts can be controlled while keeping industrial sites independent from the enterprise network. When a user terminates their session in the cloud, their identity is verified and their device posture is assessed. Once those initial checks have passed, the remote expert can be redirected to their intended network through user policy. At any point, the user's connection can be terminated and access to any given industrial network can be closed.

The benefits also extend to outbound communications. Network Detection and Response (NDR) solutions are used to detect suspicious network activity, enabling teams to respond to anomalous or malicious traffic. Deploying an NDR tool with context-rich visibility provides a full picture of network activity, with insight into the users on the network, what devices are interacting, and what kind of data they are sharing. This visibility enables security teams to not only detect threats but also determine their source, where else they may have propagated, and which users have been compromised.

Figure 6. Using a hybrid cloud IDMZ to aggregate and correlate telemetry



By aggregating and correlating telemetry across the entire network, incident management and threat hunting can be accelerated. Cisco Secure Network Analytics offers agentless deployment across an existing network infrastructure, while ingesting metadata from Cisco Identity Services Engine (ISE), Cisco Cyber Vision (for specialized visibility into industrial networks), and Cisco AnyConnect® for user, device, and application context to the network. If a malicious activity has been flagged in one facility, rapid action can be taken to contain the threat, while other facilities can be investigated using the same tool.

Conclusion

As a leader in Industrial Automation and Control System (IACS) security as well as cloud security, Cisco is in a prime position to help with a cloud migration strategy for the IDMZ. Wherever you are in your cloud adoption journey—looking to lower costs, gain access to artificial intelligence and machine learning toolkits, or take advantage of scalable infrastructure—Cisco has the tools and expertise to get you there faster, with minimal downtime.

Please refer to the following for more information and to get started:

- Visit the Cisco Industrial Security webpage
- Explore Cisco Secure Firewall solutions
- Read the Extending Zero Trust Security to Industrial Networks white paper
- Read the IT and OT Cybersecurity: United We Stand, Divided We Fall white paper
- Contact us