

Designing Network Architectures to Secure the Bioeconomy

Executive Summary

The last few years have seen a rapid increase in cyber-adversarial activities specifically targeted at the bioeconomy.

For the bioeconomy to continue to grow while maintaining the trust and safety in the products it produces, we must embrace new practices. Cyberbiosecurity blends the principles of cybersecurity and biosecurity, providing a trans-disciplinary approach that better reflects the risks and opportunities of a modern and technologically-driven bioeconomy. Higher levels of cybersecurity controls and requirements should be components of the entire lifecycle of a bioeconomy process or project – from inception to decommissioning. To mitigate the new atmosphere of threats and vulnerabilities, a more sophisticated security approach starts by accepting that a facility is already compromised.

This document is intended as a freely available guide for operators and executives in the bioeconomy who wish to improve the operational resilience of their organizations in the face of modern cyberbiosecurity realities. This document will provide concrete network architectures and principles to implement across your facilities to improve the assurance of operations and end-products. It is likely to evolve as attackers adapt and incidents come to light.

To successfully defend against cyberbiosecurity threats, an organization must invest in designing an advanced network architecture that includes the deployment of known secure-by-design, Defense-in-Depth, and zero trust network access principles.

Table of Contents

- The Case for Network Architecture in the Bioeconomy.....3**
- A Strong Foundation Builds Secure Facilities..... 3**
 - About this Publication..... 3
- Prioritizing a Network Architecture..... 4**
 - What is a Facility Network?..... 4
 - Why is Network Architecture Important?..... 4
 - Why do Bioeconomy Organizations need a Network Architecture?..... 4
- Designing a Secure Network Architecture..... 5**
 - Inventory the Facility..... 5
 - Defining Security Goals..... 6
- Traditional Network Architecture..... 7**
- Moving Beyond Traditional Network Architecture..... 15**
 - Understanding Zero Trust Network Access and Microsegmentation..... 16
 - Advanced Network Architecture with On-Premises Storage, Zero Trust Network Architecture and Microsegmentation..... 18
 - Advanced Network Architecture with Cloud Storage, Zero Trust Network Architecture, and Microsegmentation..... 23
- Conclusion..... 28**
 - Appendix I: Exploring remote access AuthN and AuthZ representation..... 29
 - Appendix II: About BIO-ISAC..... 30
 - Appendix III: BIO-ISAC and the Device Security Workgroup..... 30
 - Appendix IV: Definitions..... 31
 - Appendix V: Additional Resources..... 35

The Case for Network Architecture in the Bioeconomy

A Strong Foundation Builds Secure Facilities

A rapid increase in cyber-adversarial activities observed over the last decade has shown the importance of cybersecurity in the bioeconomy. Embracing cybersecurity requires accepting pertinent functions as integral to the end-to-end research and development and at-scale development processes. In other words, cybersecurity controls and requirements should be components of the entire lifecycle of a bioeconomy process or project, from inception to decommissioning. This involves the adoption of proactive and reactive cybersecurity controls—a combination of effectively utilizing system and network-level native capabilities and proven security tools and mechanisms. A successful network architecture and pertinent security best practices will assist the System, Network, and Security teams to deploy their processes in a secure manner, particularly when working through Zero Trust implementation.

The **Zero Trust model** operates on the principle that no entity, whether inside or outside the network, should be trusted by default. Implementing Zero Trust security methods, including **Microsegmentation in Zero Trust**, involves strict identity verification, minimal privilege access, and continuous monitoring of network activity. This approach is particularly important to the bioeconomy where both data integrity and confidentiality are important; loss of either could lead to dire consequences on drug development processes, patient safety, and regulatory violations. The attack surface and pertinent cyber risks are often rapidly changing as the organizations are embracing hybrid architectures involving on-premises and public cloud infrastructure leading to different views at trust zones and boundaries.

A typical bioeconomy facility has a mix of information technology (IT) and operational technology (OT) systems. While the integration of cloud services may optimize processes by focusing less on infrastructure maintenance and more on research and development or at-scale development. Recent cybersecurity attacks have shown the detrimental impact of exposed cloud systems (e.g., exposed sensitive data, exposed private virtual machines running critical experiments or processes, etc.), particularly in small and medium enterprises where dedicated IT staff have not been hired. A cybersecurity-centric network architecture is crucial to ensure long-term, secure research and development and at-scale processes.

About this Publication

This is not intended as a comprehensive guide for deploying and managing a commercial network architecture in the bioeconomy, nor should these illustrations be replicated exactly by a facility as that would, in fact, present a vulnerability. Instead, this offers a starting point of current best practices in designing a successful, secure network architecture, indexing current best practices and examples. This should inform an organization's strategy and work, it will not inventory the entire security needs of an organization. This effort provides the opportunity for scale to large facilities, recognizing larger biomanufacturing networks will face substantial complexities and considerations for SCADA, DCS, Historians, WES, MES, etc. For specific inquiries or for support on your organization's efforts, please contact help@isac.bio.

Prioritizing a Network Architecture

What is a Facility Network?

A Facility Network is the physical space, and the equipment within that space, utilized for production in the bioeconomy including research and development, manufacturing, and biological specimen testing. Networks may have devices that use traditional Information Technology (IT) protocols (e.g. HTTPS, TLS, etc.) but may also have Operational Technologies (OT) protocols (e.g. OPC UA and DA, PROFINET, PROFIBUS, Modbus, etc.). The Facility Network includes data storage (onsite or offsite) and the availability and types of access to both local networks for equipment and data transmission, and any connection points to the Internet.

Why is Network Architecture Important?

A Network Architecture is the foundational security element to understand and appropriately address the needs of a network of complex systems. A good architectural design exercise allows teams to understand and visualize that complex system. Teams can then ideate, propose, and build the network architecture they need, and deploy systems to optimize and automate functionality, without compromising security.

Why do Bioeconomy Organizations need a Network Architecture?

Bioeconomy organizations face a unique set of challenges in network security. Discovery is happening faster than the pace of manufacturing security and protective regulation. The world expects answers to the greatest challenges in agriculture, medicines, energy, and computation, while industry innovators face equipment or processes without regulation that encourages basic security controls to protect the data, intellectual property, and discoveries and in some cases, the regulations present an obstacle to contemporary, real-time security. While pursuing the horizons of invention, organizations in the bioeconomy are navigating an imbalance between security needs and equipment and training that provides those competencies. Often, a small number of vendors, sometimes only one, provide much-needed equipment. Facilities often have little choice but to accept the equipment as is, including known security gaps resulting from its own manufacturing. This often necessitates compensating controls which can increase setup and maintenance costs and increase overall risk to the organization. Deploying less-secure equipment in a secure fashion happens through meaningful design and use of security-centric network architectures.

Designing a Secure Network Architecture

To be successful in designing a network architecture, it is important to know the components involved, from data streams to data storage, from equipment setups to user training. Teams must also understand how systems are working together, what dependencies exist if a single piece of equipment or storage goes offline, and what individuals or equipment have access to the Internet or require that access for periodic updates. Both IT and OT equipment are the building blocks for any facility, while some newer facilities will also have Internet-of-Things (IoT) or similar components that can talk over the internet to Public Cloud Services.

With a long list of niche systems and disparities in vendor manufacturing processes, it is non-trivial to architect these networks in a security-centric manner, but it is nevertheless achievable. The key components of a successfully designed network architecture are:

1. Types of equipment
2. Training and staffing approaches
3. Data storage and compute location (cloud vs on premise)
4. Network segmentation (Zero Trust Network Access (ZTNA) and micro-segmentation)
5. Access controls and management: system-to-system and human-to-system access

Including defensible measures at the network and system level are expected in creating a network architecture at a bioeconomy facility. Both network and system hardening, and pertinent natively enforceable security controls, are part of a secure architecture. From a Defense-in-Depth¹ perspective, other significant security controls include using external tools such as Network Security Monitoring (NSM), endpoint and network defense and response (EDR and NDR), data loss prevention (DLP) tooling, SIEM, SASE, a long list of incident response and forensic tools, and the list goes on.

Inventory the Facility

The security and network architecture phase of the deployment allows the network and security engineers to evaluate the functionalities and feature sets of the equipment at hand and ideate deployment options. To begin the architecture process, a team is typically assembled, those able to answer questions about the equipment in use and the processes for manufacturing. These questions may include:

Equipment and Staffing As-Is:

1. What equipment is currently in the facility space?
2. What equipment is being added to the facility space?
3. What equipment has access to the Internet? To cloud storage systems? To other local equipment? To other facility systems?

¹ NIST "defense-in-depth" definition: https://csrc.nist.gov/glossary/term/defense_in_depth

4. What individuals have access to what equipment? What background screening and training is required for these users?
5. How do equipment software updates occur? Who does these updates? What background screening and training is required for these users?

Future State Activity

1. What new equipment is needed?
2. Can and should new equipment be added to the network?
3. Can and should new equipment be connected to the Internet? To cloud (or other data storage systems)?
4. What kind of directional connections are needed? (North-South or East-West)
5. Does the facility host any endpoint security agents?
6. Is any equipment on a private VLAN? Should it be?
7. Does the equipment support virtualization, i.e., can the software controller decouple from the equipment and run it on a VM?
8. Does the equipment itself or the facility outputs (data, product) need to communicate through any public IPs or URLs from the vendor or other third parties?
9. What is the business impact if the equipment is not able to operate?
10. What is the value of its data to the organization? To outside entities?
11. What does adequate security look like for the facility? What are the “good enough” security controls that must be in place?
12. What is the patch and vulnerability management process for the equipment? Are updates needed?

These discussions facilitate the adoption of a proactive cyberbiosecurity philosophy for organizations and are only a fraction of those important to review. For further guidance on the composition of a team or questions to answer during the introductory inventory work for designing a network architecture or during the procurement process, please review the ***Biosecurity Evaluation Questionnaire*** at isac.bio/device.

Defining Security Goals

Network architects should use Secure-By-Design and Defense-in-Depth models to balance approaches for handling the limitations of the equipment. Some equipment may not support endpoint agents while others may not support inter-VLAN communication. As part of the proactive network architecture measures, controls should be put in place to limit the impacts of a cybersecurity incident involving a single piece of equipment, a local network, or a dataset being rendered unusable.

Traditional Network Architecture

A traditional network is one that adopts basic security best practices such as the use of segmentation, firewalls with appropriate ruleset, the use of security tooling (network or endpoint monitoring) and other actions. A flat network corresponds to a combination of deployment methods such as: 1) firewall with “any-any” between all VLANs, 2) lack of a combination of VLANs, subnets, and ACLs and instead, placing all systems on one broadcast domain, etc. A flat network should be avoided. A traditional network architecture for a facility deploying basic cybersecurity practices is detailed in Figure 1.

Figure 1. Traditional Network Architecture

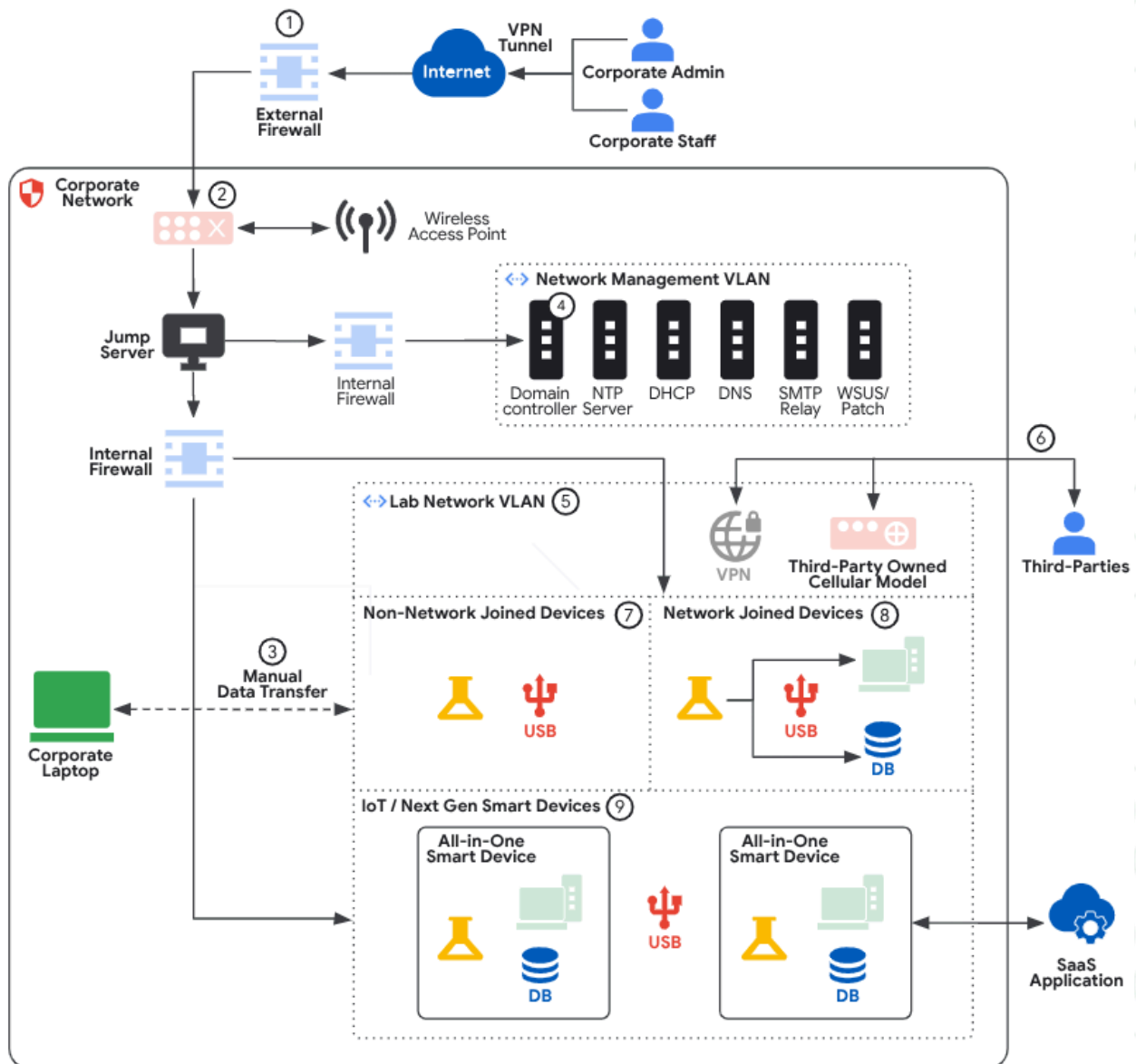


Figure 1 Legend:

- ① External/perimeter firewall separating the corporate network and the Internet. Note that if the facility network is part of a larger organization with shared applications, SD-WAN or SASE may be used. In such cases, pertinent SD-WAN devices may be used to the north of the edge/corporate firewall. Would the SD-WAN hardware device replace the edge firewall? In almost any case, that would be a NO but the answer may depend on factors (such as does the SD-WAN hardware device have firewall capabilities with the ability to accommodate rules with deep packet inspection/DPI)
- ② Corporate edge/core switches and routers followed by the internal firewall. Networks/subnets/zones beyond this are meant to serve the facility network (not the corporate network).
- ③ Manual data transfers using approved USB, external storage (e.g., equipment attached storage, NAS, etc.), or other similar remote media. The approved USB should be tied to the system that it is approved to be used on and the person that is approved to use that particular USB. To enforce this, the USB's unique serial number can be approved for use on a particular system ID/system name. Most endpoint security and XDR tools will allow to enforce such granular policy. For example: The user <user details> is approved to use the USB <USB serial number> on the device <Device identifiers>. Note that using IP and MAC addresses as the device identifiers may not always be prudent as they can be changed. This approval process should be tracked through Security's USB exception and tracking list for periodic auditing and review. Approval of use should be timeboxed as opposed to approving for permanent use. The USB should be treated as single-use systems for the transfer of data when no other alternative is available.
- ④ A Demilitarized Zone (DMZ) with shared internal network services and systems that facilitate interaction between different trust zones. Note that the internal DMZ shown in the figure is different from the "external DMZ" that would be between the external firewall and the corporate/enterprise network. These services should not be shared between the enterprise zone and the facility zone.
- ⑤ Lab zone networks/subnets - With multiple VLANS based on the processes, equipment type, etc.
- ⑥ Non-Cellular traffic would traverse the internal and external firewalls
- ⑦ Stand alone, non-networked, devices.
- ⑧ Network joined devices with connectivity to associated instruments. Data transfer can be manual or programmatic. Server apps (SQL, etc.) separated from workstation.
- ⑨ All-in-One smart devices (IoT, prepackaged units, etc) that contain embedded databases, Human Machine Interfaces (HMIs), full workstations, and/or cloud connectivity.

Everything within the "corporate network" box can be assumed to be as on-premises systems – in other words, these are the systems deployed within a facility's physical perimeter bounded by pertinent physical security controls. Everything outside the "corporate network" box goes over the internet, strongly preferable through VPN (e.g. TLS, IPSec, etc.).

The Traditional Network Architecture detailed in Figure 1 assumes the intricacies of peripheral security tooling are strongly considered and already in place offering these key aspects:

- 1. Good Use of Firewalls:** A "true" DMZ can be achieved using a physical firewall and creating a zone with well-defined rules to place services/systems that are shared between multiple trust-zones. It may not be uncommon to see a VLAN with shared services to be incorrectly referred to as a DMZ. In most if not all networks, establishing DMZ is a fairly non-trivial task but identifying and migrating systems appropriately to ensure secure traversing between trust zones may take some effort. Failure to migrate systems to appropriately increases the difficulty of monitoring, could expose systems that expose sensitive information, or be utilized to obtain unauthorized remote access to sensitive network segments.

A typical bioeconomy organization would include a corporate network/zone with enterprise systems (e.g. HR, legal, finance, marketing, etc.) that largely or only comprise IT infrastructure such as Windows and mac laptops, Windows servers, etc. Linux systems and servers are very rarely seen in bioeconomy facility enterprise networks. These systems depend on network services such as AD (typically Azure AD but Microsoft AD or on-prem AD may be active in older networks), DHCP, DNS, NTP, VPN, WSUS, Jump servers, etc. It can be seen from Figure. 1 that such services are placed within a DMZ/External-DMZ that is behind the external firewall (labeled as "1"). A facility network/zone, however, comprises IT, OT, and IoT infrastructure. The endpoints include a combination of Microsoft Windows, Mac OS, and Linux-based operating systems (including some embedded/RTOS) that not only speak traditional IT protocols but only heavily rely on OT/IoT protocols such as OPC (UA and DA), MQTT, EthernetIP, Profibus and Profinet, and even BACnet and Modbus.

These systems also rely on network services that are discussed earlier. Unlike IT protocols, many of the OT protocols were not designed with security in mind and in many cases lack even basic authentication and encryption capabilities. Therefore, a secure network architecture advocates for a separate deployment of these services within a facility network DMZ. This DMZ would be behind the internal firewall and will not have any trust relationships with the enterprise systems and services. Such defensible/segregated facility networks will continue to function even in cases where some of the enterprise systems are compromised.

Suggested Patterns/Solutions

- Establish DMZ with physical firewalls for Lab Network
 - Enforce web content filtering and geo-IP restrictions
- 2. Segmentation:** Segmentation using VLANing/subnetting can not only help with network management but will also assist with security to some extent. VLANing by itself is far from achieving a secure architecture. There are many ways to VLAN/sub-zone a facility network zone. For instance, VLANs can be created using multiple strategies:
 - a. per-location basis - *systems in room-1 are on VLAN 201, systems on room-2 are on VLAN 301*

- b. per vendor-basis - *vendor-1 systems on VLAN 201, vendor-2 systems on VLAN 301*
 - c. per functionality-basis - *freezers on VLAN 201, rocking bioreactors on VLAN 301*
 - d. per system basis (*micro-segmentation*) - *system-1 on VLAN 201, system-2 on VLAN 301*
 - e. per system type basis - *all controllers/PLCs on VLAN 201, all HMIs on VLAN 301*
3. **Segmentation.** The commonly used strategies are segmentations based on per-location/suite/room and functionality. Segmentation limits the adversary from laterally moving through the network and can highly optimize the recovery processes if systems/networks are compromised.

Suggested Patterns/Solutions

- Create zones for the Lab Network with per-location, per vendor, per functionality-basis, per system basis, per system type basis, and/or pattern(s)
 - Segment network management devices such as domain controllers, switches, APs, DHCP, DNS, etc.
 - Require the use of jump boxes or otherwise similar (or better) solutions for accessing network management devices
4. **System Hardening and Security Tooling:** System and network hardening, the process of removing unnecessary services and securing configurations, adds immense security value to the implementation of systems in a facility network. Often, facility networks use Windows and Linux-based virtual or physical machines. Misconfiguring these systems could increase security risks and maintaining unused system services increases your vulnerability management scope. Using and implementing Security Technical Implementation Guides (STIGs) and Center for Internet Security (CIS) Benchmarks wherever possible can ensure the use of hardened systems. This is an area where leveraging cloud services would significantly simplify - most cloud service providers (particularly AWS, GCP, Azure) provide virtual machine hardening capabilities while configuring the VMs in the cloud or the ability to purchase previously hardened images. Part of system hardening involves ensuring that the system has only necessary services, open ports, and protocols to support the needed operations. Everything that is not necessary should be disabled. One key risk that should be considered during hardening is a process such as STIG may involve making OS-level configuration changes and that sometimes could do irreparable damage to the VM. The hardening process should be evaluated in a test environment prior to use in production.

In addition to system hardening, use of security tooling will provide visibility into system and network health, enumerate traffic for anomaly detection, allow for evaluation of network and system activity using Endpoint Detection and Response (EDR) and Network Security Monitoring (NSM). There are a number of open source and commercial tools that allow for on-prem monitoring (endpoint level through EDR when supported; network-level through NSM when end-point agents cannot be deployed on an endpoint). Since the EDR

and NSM tools tend to come with built-in intrusion detection (IDS) while supporting the use of snort-like signatures, these tools provide tremendous value in terms of identifying the on-prem inventory, discovering vulnerabilities, determining network map, etc. The data from these tools can be combined with the data from native cloud security tools (e.g., AWS Security Hub, GCP Unified Security, Microsoft Defender family, etc.) to gain holistic view into both on-prem and cloud-based/ supporting facility systems and networks. Security Information and Event Management (SIEM) and security orchestration, automation, and response (SOAR) can be used for log consumption, semi-automated response, and activity querying. Another key security recommendation is to ensure that *internal* systems are not inadvertently exposed to the public internet. The systems that are supposed to be in a private network (on-prem or cloud) should not have a public IP address. If these systems need to be accessed, tools/technologies such as NAT should be used. For situations such as downloading upgrades, patches, accessing certain data, etc. some of these systems may need to reach a system over the internet. In such cases, proxies (e.g. web proxy, identity-aware proxy, etc.) should be used.

Suggested Patterns/Solutions

- System hardening is performed leveraging STIG, CIS Benchmarks, etc.
- Security tooling is used (open source or commercial) for endpoint monitoring and network monitoring with IDS
- Automation is achieved to possible extent to enumerate the network and systems while combining the data from on-prem and on-cloud security tools
- NAT and proxies are used to ensure mitigation of private systems exposure to public internet
- A SIEM is used for logging, aggregation, and querying

5. **Remote Access:** It is not uncommon to see both RDP and VNC shadow sessions in the facility environment and this is due to a multitude of reasons - to name a few: 1) a scientist may want to periodically monitor the experimental live data streams, 2) an engineer may want to assist an on-prem scientist to troubleshoot the equipment, 3) IT may want to make authorized system changes, and 4) a vendor may need to access the equipment either to patch or troubleshoot - this is often required of them through SLAs. Irrespective of the reason, it is imperative to differentiate between organizational personnel, contractors (temporary contract-based employees hired through third-parties), and vendors. Each of those personnel groups carry different trust levels and the organizational policies may apply differently. Remote access-based intrusions are one of the most preferred methods for the adversaries piggybacking a trusted session. This can be done through stolen credentials, compromised workstation that a third-party uses to access the facility system, exploiting known vulnerabilities in the remote access server, etc. Some noteworthy best practices are as follows:

- a. Ensure user roles and groups are strictly defined and enforced to limit system-level access on a need-to-know basis.
- b. Enforce Multi-Factor Authentication (MFA).
- c. Eliminate any persistent access to non-employees.
- d. If a contractor requires access, ensure it is revoked when the contract ends.
- e. If a vendor requires access, ensure the following: 1) access is defined to a vendor Point of Contact (POC); 2) access provision and revocation is strictly bounded by the scheduled task; 3) the system owner is required to monitor the whole session; 4) all activity is logged and strictly monitored for alerting on anomalous and unauthorized activity; 5) post-session thorough log review and analysis is conducted; and 6) system is scanned for any malware and OS-level configuration changes, etc.
 - i. **Note!** Avoiding third-party remote access to vendor systems is highly recommended since the organizational policies may not apply to the vendors or they may lack familiarity with the site policy. In such cases, a patch can be deployed or shared through a secure channel/location or a vendor is allowed to perform their duties in-person. Even secure patch sharing mechanisms (e.g., secure/trusted weblink) can be vulnerable to attacks. Therefore, user activity scanning may be useful.
- f. Ensure both RDP and VNC sessions are encrypted. Use remote access solutions that are more secure than the others in the market. Use a CVE database to evaluate the technology that is considered more secure.

Suggested Patterns/Solutions

- Differentiate Full-Time vs Contractor staff identities. This should be easily identifiable by any person in the company.
- Multi-Factor Authentication.
- Log all user and system access requests and activity
- Prohibit shared remote access credentials for any staff. If shared credentials are the only option, utilize a password manager to enable secure password sharing.
- Utilize groups and roles to manage user system access.
- Establish processes to decommission Contractor user IDs that align with contract termination.
- Require all methods of remote access to utilize Multi-Factor Authentication.
- Ensure RDP and VNC protocols are encrypted and closely monitored with logging/alerting of unusual activity.
- If self-hosting a remote access solution, monitor for newly announced vulnerabilities and develop processes to deploy. Deployment velocity is critical

- Consider the source and sustainability model of freeware solutions. Avoid use if coming from untrusted vendors and/or do not have regular security patches and updates.

6. Data Storage and Transmission: Traditional facility networks involve a combination of standalone databases (i.e., a database running on windows or linux systems connected to the specific equipment) and a centralized database. Historians that are often seen in Manufacturing and other environments are less traditionally used in facility environments. It is also common to see the approved USB usage (discussed in detail in Figure 1) to move data from the equipment to another computer for visualization and analysis. Given the nature of the bioeconomy facility processes and pertinent data generated, a *heavy duty historian* may not always be ideal. When deployed properly, often these systems are in the internal network (not accessed over the internet) and therefore hardwiring a storage or a laptop per equipment is fairly a common approach.

For instruments that cannot support direct connection to a windows or a linux system, approved USBs are used to transfer the data/files. Encryption involves using keys/secrets in addition to potentially common use of service accounts for humanless interaction between applications and systems. These communications involve using certificates - avoid self-signed certificates and use a trusted certificate authority (CA). The secrets (e.g. keys, passwords, certificates etc.) should be secured in a trusted secrets manager and key management services.

Suggested Patterns/Solutions

- Enforce data-at-rest and disk encryption for all servers and user workstations to protect against theft and improper disposal
- Enforce encryption for data-in-transit for all database communications, web traffic, web services, and SMB.
- Depending on the business need, enforce data-in-use encryption (e.g., using trusted execution environments/confidential computing, etc.)
- Perform data/file integrity checks with hashing if files are transferred
- Dedicate one computer to one piece of equipment and use wired connection with Network Interface Cards (NICs) configured to prevent connections to other networks or devices
- Dedicate removable media to a device (Computer A is assigned USB A) or single-use USBs
- Centrally manage all USBs
- Require all remote media to utilize encryption
- Monitor network for large data transfer with Data-Loss Prevention tools
- Retain syslogs for log analysis in SIEM

- Enforce WAP security measures to ensure secure wireless transmission
- Secrets managers, key management services, and trusted CAs are used

7. Third-Party SaaS Applications: Third-Party SaaS Applications frequently push the limits on the boundary protections. Lab systems with SaaS requirements may or may not support proxied traffic and thus having uninterrupted north-south traffic from the device to the provider's Cloud Application. Architecting for security with these solutions in a typical "good network" leaves many feeling as if they do not have the tools they need to properly secure the device and this may not be far off but there are things that can be done to mitigate these concerns including:

- a. Implement Single Sign-on (SSO) to the SaaS solution
- b. Perform a Third-Party Risk assessment (see the [BIO-ISAC BSEQ for support](#))
- c. Isolate the device to a dedicated VLAN.

The North-South traffic traversal including or not including the ability to be proxied and monitored is a critical factor to determine the level of isolation the device should be subject to. For example, if the traffic cannot be proxied it may be best to avoid joining the device to the domain.

Suggested Patterns/Solutions

- Require and implement Single Sign-on (SSO) for access to all SaaS solutions
- Perform a Third-Party Risk assessment (see the [BIO-ISAC BSEQ for support](#))
- Properly segment devices with Third-Party SaaS connectivity
- Implement NDAs with all SaaS providers
- Contractually require Third-Party SaaS providers to maintain security standards (e.g. SOC 2, Type 2, ISO 27001, etc.) and breach notifications

8. Disaster Recovery: While not represented in Figure 1, Disaster Recovery (DR) should be considered in all network designs as it is critical for business operations after a systematic, human error, or after a security event. DR will be discussed in two parts: 1) Business Criticality Functions and 2) DR Strategy and Design. When determining the DR strategy it's critical to understand what holds the most value as it pertains to the business' ability to operate critical functions. A critical function may be foundational IT systems that enable enterprise communications, knowing a manufacturing line that supports the highest revenue generating product, or services otherwise critical for day-to-day operations. The identified critical systems should drive the DR strategy and design so that it supports operations but is also cost effective.

Consider the following questions when determining a DR strategy for a system:

- 1. Can the system be restored without third-party assistance?

2. What is the contact information for the vendor support?
3. What data-loss can be tolerated for this system?
4. What's the maximum amount of time the process/business can operate without this system?
 - a. Do note, if it's on a manufacturing line consider the delivery timelines for a product. If Device A is at the end of a manufacturing line and if an in-progress product takes five days to get to Device A the maximum offline thresholds starts to become clear.
5. Can a snapshot of the system be used or will separate configuration and data backups be necessary?
 - a. Consider the cost implications of both based on how the number of snapshots needed or the amount of data included in a backup.
6. How to quickly test restoration procedures on a frequent basis?
 - a. Systems that have been changed without testing restoration procedures do not have trusted DR plans. With these questions in mind the organization can begin to consider what needs to be backed up and how. The backups must be isolated from the general environments and use unique credentials/service accounts to take backups. For these credentials use the longest unique support password and implement MFA wherever possible. Backup isolation can be achieved by using a separate account with the Cloud Service Provider, third party DR speciality firms, dedicated in-house hardware, or others.

Suggested Patterns/Solutions

- Establish data retention requirements based on business need
- Establish a Recovery Time Objective (RTO) otherwise known as the maximum time an organization can withstand system downtime.
- Establish a Recovery Point Objective (RPO) otherwise known as a data-loss tolerance
- Encourage business lines to develop business continuity plans
- Frequently test all recovery plans
- Isolate backups
- Require MFA for access to all backups systems

The traditional “good” network is what many companies have due to a number of factors such as budget or a system being acquired. Sensitive data-loss (e.g. intellectual property, Personal Health Information (PHI), etc.) has been unphased by these controls, something more secure is required.

Moving Beyond Traditional Network Architecture

Traditional networks face a problem. While they can restrict access between VLANs, if they do not have the appropriate tooling, they do not have the ability to restrict server-to-server access within a VLAN. Further, they cannot posture an asset, identity, or otherwise important information to determine if ingress and egress traffic is appropriate. Microsegmentation and Zero Trust Network Access (ZTNA) were developed to help moderate lateral traffic to only permit communications between two trusted points.

Understanding Zero Trust Network Access and Microsegmentation

Traditional security approaches, including perimeter-based security, segmentation, and Defense-in-Depth models, tend to fall short in the implementation of security solutions from a threat-centric manner. Zero Trust Network Access (ZTNA) addresses the problem of monitoring for malicious activity by building on a philosophy that embraces the fundamental assumption that the facility's network is already compromised and/or the adversary is already involved and accessing important materials. From there, the team designing the network architecture makes threat-centric security decisions to minimize, mitigate, or address consequences from a cyber incident. With traditional approaches, authentication and authorization are performed at the network perimeter and once greenlit, an entity is trusted to access any/all resources within a perimeter (be it a network zone, segment, or a VLAN). The entity's further actions inside the perimeter aren't always, if at all, re-authenticated and re-authorized as/when needed. Attacks coming through semi-trusted channels into critical network zones, including some that include compromised VPN access, compromised RDP access, and insider threats have been documented. ZTNA assumes this behavior is happening and that actions within a permitted perimeter limit the entity from performing any and all actions. Accessible actions are controlled through granular policies at the organization, using a mix of technologies such as next-gen firewalls, zero-trust solutions, and security tooling.

ZTNA is not one technology, it's a strategy that removes inherited trust from ownership and assumes every device, connection, user, etc. is compromised from the start. A ZTNA strategy generally relies on one or more tools to create, enforce, and monitor the policies that test if something or someone can be trusted.

Example 1. John Doe, employee of Company X, is SSH'ing into Company X's Production Cloud account from a personal mobile device. A ZTNA strategy would define if John Doe's user ID + non-corporate device + protocol for access, geographic location, and MFA status achieve the policy-defined trust criteria to access their Production Cloud services and prevent misuse or compromise.

Microsegmentation is the implementation of well-defined access policies at the application workload level (Layer 7) opposed to traditional transport policies (Layer 4). A traditional firewall is designed to manage north-south traffic but as IT teams are pressed to move more quickly to deploy cloud and on-prem resources, complex Layer 4 security models have struggled to keep up

with business demand without sacrificing velocity and security. While East-West segmentation can be achieved through Layer 4 policies, it tends to be achieved with multiple layers of firewalls that each contain complex VLAN structures. The utilization of Layer 7 policies allows the organization to move beyond using IP addresses and ports to define access. The network team can rely on additional software defined attributes that better align to the segmentation strategy.

Devices are manufactured with an expectation that they reside behind a firewall with granular policies at the facility and organization. The introduction of remote work and Software as a Service, the traditional network perimeter as a geographic, physical barrier, is deteriorating. To counteract the threats from an extended network perimeter, tooling with policies that can enforce microsegmentation and other ZTNA policies will be needed to protect facility network operations from evolving threat actors.

Advanced Network Architecture with On-Premises Storage, Zero Trust Network Architecture and Microsegmentation

The illustration in Figure 2 shows an advanced network architecture, a version updating a traditional network to include ZTNA and microsegmentation. This particular example of an advanced network architecture relies heavily on on-premises systems with minimal usage of cloud services.

Figure 2. Advanced Network Architecture with On-Premises Storage, ZTNA, and Microsegmentation

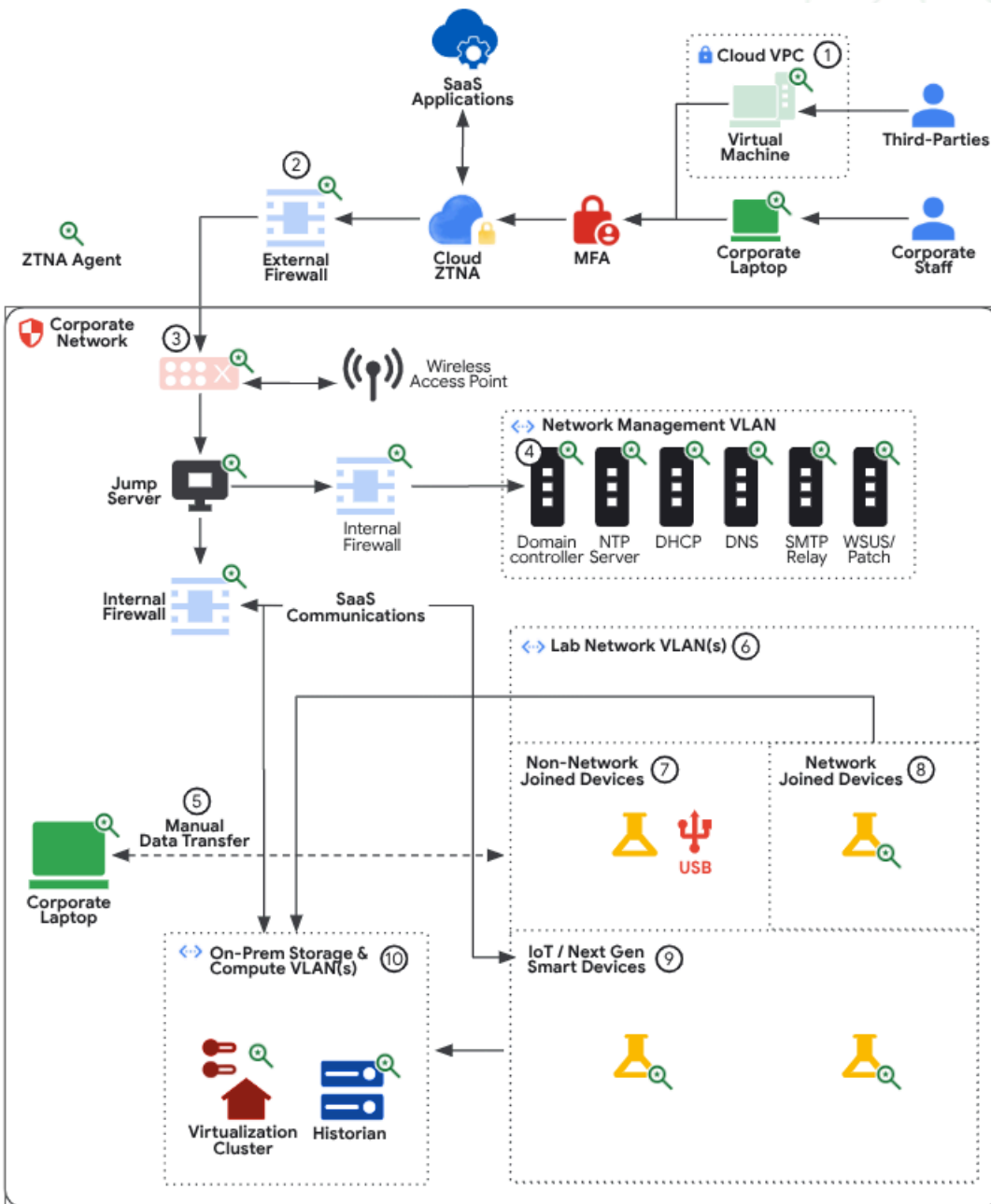


Figure 2 Legend:

- ① Remote access provisioning through cloud VMs (e.g., AWS Workspaces, GCP Virtual Desktops, Azure Virtual Desktop)
- ② External/perimeter firewall separating the corp network and the internet. Note that if the facility network is part of a larger organization with shared applications, SD-WAN or SASE may be used. In such cases, pertinent SD-WAN devices may be used to the north of the edge/corporate firewall. Would the SD-WAN hardware device replace the edge firewall? In almost any case, that would be a NO but the answer may depend on factors (such as does the SD-WAN hardware device have firewall capabilities with the ability to accommodate rules with deep packet inspection/DPI)
- ③ Corporate edge/core switches and routers followed by the internal firewall. Networks/subnets/zones beyond this are meant to serve the facility network (not the corporate network).
- ④ A DMZ with shared internal network services and systems that facilitate interaction between different trust zones. Note that the internal DMZ shown in the figure is different from the "external DMZ" that would be between the external firewall and the corporate/enterprise network. These services should not be shared between the enterprise zone and the facility zone.
- ⑤ Manual data transfers using approved USB, external storage (e.g., equipment attached storage, NAS, etc.), or other similar remote media.
- ⑥ Lab zone networks/subnets - With multiple VLANs based on the processes, equipment type, etc.
- ⑦ Stand alone, non-networked, devices.
- ⑧ Network joined devices with connectivity to associated instruments. Data transfer can be manual or programmatic. Server apps (SQL, etc.) separated from workstation.
- ⑨ All-in-One smart devices (IoT, prepackaged units, etc) that contain embedded databases, HMI's, full workstations, and/or cloud connectivity.
- ⑩ On-prem Storage and Compute VLAN. Ideally as few people as possible need to digitally access Lab Devices and they only need the data. The data can be retrieved by users from here instead of on facility instruments.

Compared to the Traditional Network Architecture Model in Figure 1, the Advanced Network Architecture with On-Premise Storage, ZTNA, and Microsegmentation in Figure 2, offers these key enhancements:

- 1. Third Party Management:** Third-Parties are not permitted to connect to corporate or facility networks with their devices. A virtual machine is provisioned through Cloud VPC virtual machines (e.g., GCP Virtual Desktops, AWS Workspaces, Azure Virtual Desktop), an on-premises jump server (e.g., Apache Guacamole, Dispel, etc.) or a combination of both is available. If exceptions are made in critical circumstances (e.g., a facility instrument is malfunctioning and onsite and physical connections are necessary for repair) utilization of corporate devices with supplier's tools may be used but with close monitoring and logging. In such cases, robust post-activity log analysis should be performed to

investigate for inadvertent and anomalous file/data transfers, application execution logs, unauthorized system access, etc.

Suggested Patterns/Solutions

- Prohibit the use of third-party devices on the corporate network and enforce with network access controls
- Provide third-parties corporate physical workstations or virtual machines with the required tooling
- For work on critical devices, visually monitor all third-party actions

2. Zero Trust Network Access: ZTNA has a foundational prerequisite for success that is not represented on this diagram, *identity*. A clearly defined identity strategy must be in place and functional to operationalize some of the major benefits of ZTNA, see Appendix I for more information on considerations for this strategy. ZTNA will be a combination of tools and processes including microsegmentation, user and machine posture analysis, and Secure Web Gateway (SWG) that deploy agents to endpoints that facilitate policy evaluation and enforcement.

- a. Microsegmentation:** At the beginning of the microsegmentation journey the organization should spend time discovering and mapping network traffic. This data will drive the logical segmentation strategy. The following questions can be used to determine appropriate measures and address key questions: 1.) Do humans need to interact with resources in a segment? 2.) Does data follow a classification strategy? 3.) Are systems only required by certain departments? 4.) Do some systems need access to the public internet? 5.) Are the systems in scope identity, network, or security management tools? 6.) Do we have a list of the resources that support an application? (e.g. databases, web servers, etc.). Once segments are developed, it may be best to temporarily allow traffic between segments of concern before enforcing deny all except for permitted traffic.
- b. Posture Analysis:** Workstations have become more dynamic with users accessing corporate resources with tablets, smartphones, personal laptops, work laptops, and more. Different systems may require different levels of security that allow for more flexibility. For example, a device being used to access a domain controller must have the highest degree of security but access to a cloud based graphics design system may need significantly less control. The organization can posture endpoints with the ZTNA solution to check against certificate validity, OS version, geographic location, encryption status, firewall status, MFA enrollment, and various other factors to meet the required trust level. If a user doesn't pass the defined trust criteria, access can be blocked until the issue is corrected.
- c. Secure Web Gateway:** Most of the devices should be restricted from accessing the public internet except for organizationally approved services such as remote access, updates, etc. The SWG will be used for on-prem workstations and general

user workstations to filter outbound internet traffic and protect the users from known malicious domains and IPs as well as block inappropriate sites such as gambling, pornography, etc. It is possible that other components of the networking stack already enforce this for devices on the LAN.

- d. Secure Email Gateway and Email Monitoring/Sanitization:** A Secure Email Gateway (SEG) is very similar to an SWG except it's designed to prevent phishing attacks, identify malware and, if supported, protection against data exfiltration through email. With an SEG or email services that offer the functionality natively, organizations can enforce email encryption for all communications (internal and external) or programmatically detect appropriate scenarios for encryption such as communications containing Personal Health Information (PHI) or Social Security Numbers (SSNs).

Suggested Patterns/Solutions

- Identify Central Identity Provider
- Identify all user points of access
- Define user groups and define firewall rules per allowed application access across the user groups
- Microsegmentation and Posture Analysis - Catalog all assets
- Microsegmentation - Identify data flows and utilized protocols
- Microsegmentation and ZTNA - Identify and purchase solution provider
- Microsegmentation - Define and implement access policies in microsegmentation
- ZTNA - Posture Analysis - Establish trust criteria (e.g. disk encryption, network zones, updates, etc.)
- ZTNA - Posture Analysis - Deploy Agents
- SWG - Content Filtering
- SEG - Phishing Protection
- SEG - Encryption Enforcement
- ZTNA - VPN-as-a-Service
- ZTNA - IP Restrictions or other policy checks for SaaS Access

- 3. Data Storage and Transmission:** Database silos and isolated per-equipment databases are nearly eliminated. Instead, secure data transmission mechanisms are in place for centralized storage. This can be through a Historian or simple on-premises database management system (DBMS).

Suggested Patterns/Solutions

- Enforce disk encryption for all servers and user workstations to protect against theft and improper disposal

- Enforce table or column level encryption for databases with sensitive information
- Enforce encryption in transit for all database communications, web traffic, web services, and SMB.
- Secrets managers, key management services, and trusted CAs are used
- Programmatically manage encryption keys and rotate every two years
- Perform data/file integrity checks with hashing if files are transferred

4. Network Simplification, Segmentation, and Asset Management: Virtualization and decoupling layer-2 (L2) and layer-3 (L3) network processes provide operational flexibility and security improvements, if configured correctly. In this case, software controllers that can be dissociated from directly running on a wired hardware computer to the equipment are moved into VMs on a virtualization cluster (e.g., ESXi, Hyper-V). In doing so, the equipment would be in an L2 network while the controllers are virtualized in an L3 network. This also eliminates the use of several standalone computers and the need to hardwire them to the equipment. Handline patching, vulnerability mitigation, and overall network management would be significantly simplified. As needed for segmentation, Private VLANs (PVLANS) can be utilized.

Suggested Patterns/Solutions

- Identify the facility assets and associated computer systems
- Use detection tools to identify network joined devices and asset management solutions for ongoing management
- Identify opportunities to dissociate the electrical and mechanical instruments from pertinent software that runs on the computer systems and interacts with the instruments. Engage with vendors to explore dissociation opportunities.
- Deploy an IP-routable VM for benchtop equipment and configure the equipment software
- Test the software and equipment interactions and record metrics such as latency, throughput limitations, etc. to check for availability, consistency
- Configure backups to support disaster recovery functions. Have fail-over, if possible, to ensure high availability and reliability
- Add necessary storage and remove the existing/legacy attached computer system. This concludes dissociation

Advanced Network Architecture with Cloud Storage, Zero Trust Network Architecture, and Microsegmentation

Cloud solutions offer a multitude of options including optimizing the need and use of on-premises systems, management of infrastructure while simplifying security functions (e.g., patching and vulnerability management) and require an adjustment in designing a network architecture. Gearing towards more virtualization, centralization, simplification of the network while maintaining same or increased levels of security in the Traditional Network Architecture, the Advanced Network Architecture with Cloud Storage addresses these issues in Figure 3.

Figure 3. Advanced Network Architecture with Cloud Storage, ZTNA, and Microsegmentation

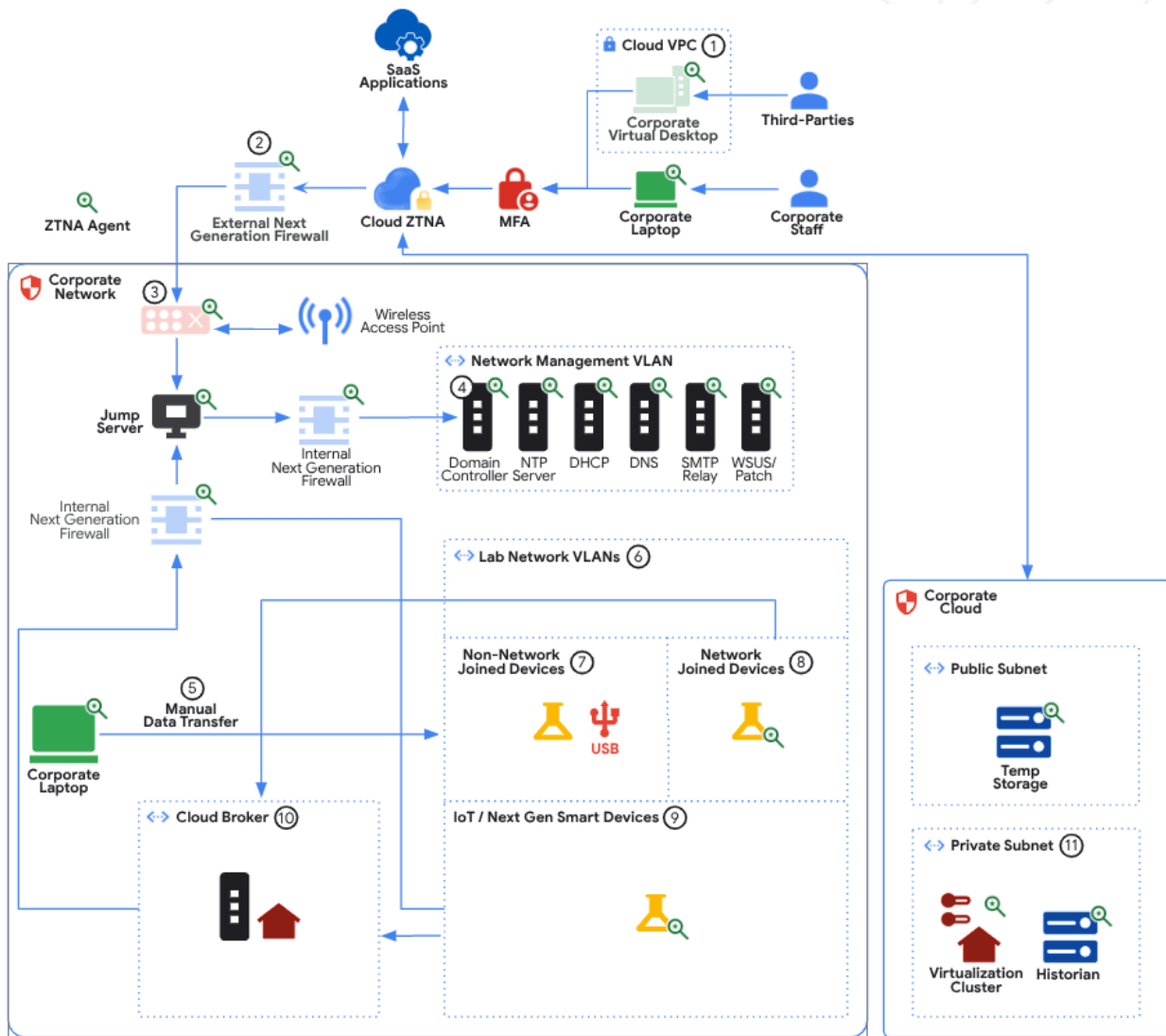


Figure 3 Legend:

- ① Remote access provisioning through cloud VMs (e.g., AWS Workspaces, GCP Virtual Desktops, Azure Virtual Desktop)
- ② External/perimeter firewall separating the corp network and the internet. Note that if the facility network is part of a larger organization with shared applications, SD-WAN or SASE may be used. In such cases, pertinent SD-WAN devices may be used to the north of the edge/corporate firewall. Would the SD-WAN hardware device replace the edge firewall? In almost any case, that would be a NO but the answer may depend on factors (such as does the SD-WAN hardware device have firewall capabilities with the ability to accommodate rules with deep packet inspection/DPI)
- ③ Corporate edge/core switches and routers followed by the internal firewall. Networks/subnets/zones beyond this are meant to serve the facility network (not the corporate network).
- ④ A DMZ with shared internal network services and systems that facilitate interaction between different trust zones. Note that the internal DMZ shown in the figure is different from the "external DMZ" that would be between the external firewall and the corporate/enterprise network. These services should not be shared between the enterprise zone and the facility zone.
- ⑤ Manual data transfers using approved USB, external storage (e.g., equipment attached storage, NAS, etc.), or other similar remote media.
- ⑥ Lab zone networks/subnets - With multiple VLANS based on the processes, equipment type, etc.
- ⑦ Stand alone, non-networked, devices.
- ⑧ Network joined devices with connectivity to associated instruments. Data transfer can be manual or programmatic. Server apps (SQL, etc.) separated from workstation.
- ⑨ All-in-One smart devices (IoT, prepackaged units, etc) that contain embedded databases, HMIs, full workstations, and/or cloud connectivity.
- ⑩ Cloud broker inside the corporate network architecture.
- ⑪ Corporate cloud, featuring a public and private subnet, with the historian in the private subnet.

The Advanced Network Architecture with Cloud Storage in Figure 3 offers the following enhancements from the Traditional Network Architecture:

1. **Data Storage and Transmission:** Data storage is further optimized by using a combination of an on premises cloud broker (e.g., AWS IoT Greengrass, GCP Manufacturing Data Engine, Azure IoT Edge). The broker serves as a gateway between the on-prem facility equipment and the data storage infrastructure on a virtual private cloud (VPC) deployment. Such architecture comes with several out-of-the box security and optimization options:
 - a. All communications are encrypted with customer-desired key management options

- b. Granular authentication and authorization permissions definitions using predefined identity and access management (IAM) policies
 - c. Auto-scaling storage and compute infrastructure
 - d. Simplifying on-prem to cloud connections through serverless code (e.g., AWS Lambda, Google Cloud Run functions, Azure Functions, etc.)
 - e. Automating compliance checks per applicable security and regulatory standards with streamlined enforcement of Security in the CI/CD pipeline
 - f. Simplified and built-in log monitoring, security and network metrics, and other security solutions such as cloud-service provided cloud security posture management (CSPM)
- 2. Security monitoring and testing.** Note that often the use of security monitoring and testing solutions are only a click of a button away (e.g., GCP Unified Security or AWS Security Hub or Azure Cloud Security services that comes with a prebuilt security tooling stack). Unlike traditional networks where the infrastructure scaling, data management should be done/handled through a mix of automated and manual processes, leveraging cloud or hybrid architectures would allow for significant automation through infrastructure as code (IaC). Depending on the use-cases and equipment capabilities and the real-time control requirements, further migrating the control applications from an on-premises virtualization cluster (as described in Figure 2) to cloud is not unreasonable.
- 3. Electrical and mechanical controls.** Note that in such a hybrid setting, the electrical and mechanical controls pertaining to the facility equipment (e.g., through digital circuits, embedded systems, PLCs, etc.) are untouched, they remain on-prem. Lab equipment may not have as stringent of near-zero latency requirements as often seen in Manufacturing environments - this opens up more flexibility or possibilities for hybrid architectures.

Suggested Patterns/Solutions

- Enforce disk encryption for all servers and user workstations to protect against theft and improper disposal
- Enforce table or column level encryption for databases with sensitive information
- Enforce encryption in transit for all database communications, web traffic, web services, and server message block (SMB) protocols.
- Perform data/file integrity checks with hashing if files are transferred
- Use Infrastructure-as-Code (IaC) to enforce encryption at rest and in transit policies for all cloud resources (e.g. volumes, buckets, HTTPS, etc.)
- Secrets managers, key management services, and trusted CAs are used
- Programmatically manage encryption keys and rotate every two years
- Monitor all resources for non-compliant configurations

- Utilize granular access models to enforce resource access (IAM, etc.)

4. Infrastructure Management: A non-technological differentiator is the optimization of personnel resources. If the organization has more than one facility location spread across different geographical areas, there is often a nonnegotiable need to have network and security personnel at each site leading to redundant efforts, siloed and inconsistent workflows. In cloud-first or cloud-based architectures, personnel resource use can be significantly optimized by keeping the on-prem infrastructure lean and automating the processes/infrastructure provision and deprovisioning within the cloud. In such cases, facilitating internal and external audit, security assessments, etc. can be simplified.

Suggested Patterns/Solutions

- Use IaC to deploy all resources and prohibit user access to production environments
- Use IaC to enforce approved security patterns (Ex. All public VPCs must use WAF and API Gateway, prevent inbound and outbound traffic from any non-listed IP/CIDR blocks, etc.).
- Use IaC to automate patching and other updates

5. Networking Enhancement Using Unidirectional Data Flows: Depending on the sensitivity of the data and the business value, organizations could use Unidirectional Gateways (UGW) / Data Diode to allow one-way communication from on-prem equipment to cloud-based storage infrastructure. This is not shown in Figure. 3 but from an architecture point of view, the UGW can be in between the Cloud gateway and the equipment. It is always worth checking if the cloud gateway has data diode or UGW capabilities.

Data flow. Note that if a gateway has software-only based methods to limit the data flow, it may not be considered as a true UGW and instead it can be treated as a mechanism available to facilitate one-way traffic. A true UGW has physical hardware-level restriction/limitation to facilitate the flow of traffic in one direction. Compromising such a network would require physical access and tampering with the device. For high risk facility networks, UGWs could add an additional layer of perimeter security in cloud-based or hybrid environments.

Suggested Patterns/Solutions

- Identify critical business data and required data flows i.e., need for bidirectional vs. unidirectional (e.g. push vs. pull, pub-sub, etc.) between systems
 - Unidirectional enforcement can also be used for Third-Party SaaS utilized with benchtop equipment.
- Identify the trust zones associated with these systems.

- If in same trust zone, configure the data flow through standard port-and-protocol based restrictions
- If the systems are in different trust zones (e.g., a system in the high trust zone talks to a system in medium trust zone), identifying the data flow requirements and the data sensitivity or data classification will inform the need of software-based vs. hardware based data diodes
- If high user traffic to view or use data is expected, consider data diodes for replicating data into your IT networks and reduce network connections into high trust zones
- If a hardware data diode or a unidirectional gateway is needed, place the device between the Tx and the Rx node - the UGW serves as a gateway for traffic traversal between two trust zones.
 - Ensure that the physical access is strictly restricted as gaining illegitimate physical access leading to UGW tampering is the bottleneck of this solution
- Per data classification and business need, if a software-based data diode-like capabilities are sufficient, use NGFW to configure application-to-device data flow and access controls/restrictions

Conclusion

Given the wide-spread dependency on susceptible supply chain technologies and the myriad of service integrators essential for daily operations, safeguarding systems poses a significant challenge, even for well-resourced teams. In response, BIO-ISAC has crafted this document to assist organizations in formulating a strategic roadmap for an effective network architecture. This guidance is tailored for organizations striving to navigate the complexities of cybersecurity, whether they have access to cutting-edge security solutions or work with fundamental resources by determining where timely improvements are possible and creating the opportunity to plan for, or actively pursue, advanced network security controls.

Designing an Advanced Network Architecture that aligns the organization's goals for security and safety with the types of equipment, facility use, data sharing and storage, local/global connectivity, and user access and training is the starting point for any organization looking to address cyberbiosecurity. Assessing the needs, reviewing the risks, and evaluating the vulnerability realities for the facility, product, and end-user will start the journey to launching a safe, secure bioeconomy through an Advanced Network Architecture.

Appendix I: Exploring remote access AuthN and AuthZ representation

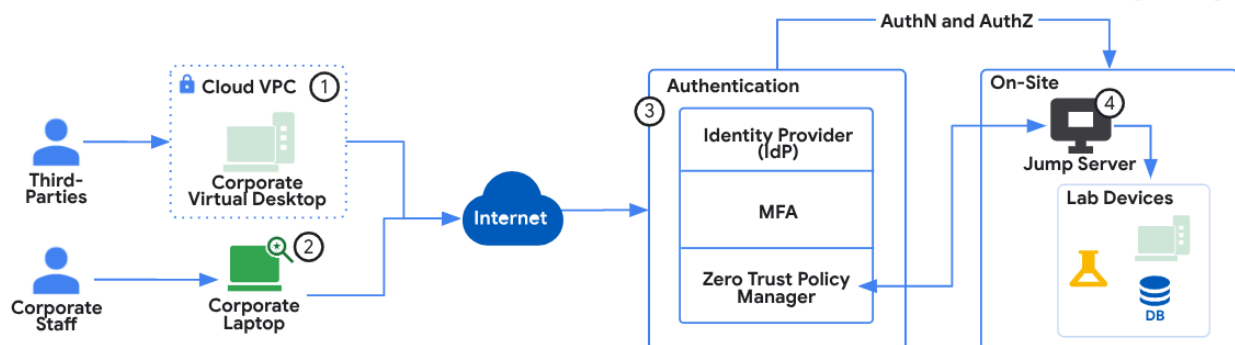


Figure 2 and Figure 3 discuss secure remote access processes.

To address this in designing a network architecture, this should be deployed:

- As shown in the figure and as discussed in the above sections, Third-Parties are not permitted to connect to the corporate network with their devices. A cloud-based virtual machine can be provisioned with corporate infrastructure. The organization's employees could access the on-prem infrastructure through organization-issued computing infrastructure/laptops with endpoint security agents and ZTNA agents.
- The authentication and authorization process/layer is applicable identical irrespective of the user attempting to access a resource. Both the Corporate Users or Third-Parties will authenticate against the corporate IdP and satisfy MFA requirements/checks when connecting to the corporate network. The Zero Trust solution will validate the policy against their user profile to permit (authorize-approve or deny) the access to the on-prem resources.
- Once approved, the access to the target resource is always through a Jump Server. The Jump Server will also validate with the Zero Trust Policy Manager that the ID and Device are permitted to perform the action that the user has initiated. If the security best practices are followed, the organization may have both a corporate active directory (e.g., Azure AD) for all enterprise zone systems and a traditional on-prem active directory for the internal facility network. Trust should not be established between the two ADs. Therefore, when an external entity (organizational entity or third party), multiple levels of policy checks might likely be in scope. The jump server pertaining to provisioning access to the facility system would check against the on-prem AD but for the user to reach the jump server, the AuthN and AuthZ would likely first happen at the enterprise AD level. Beyond those, once the user is authorized, the system would be available for use.

Appendix II: About BIO-ISAC

The **Bioeconomy Information Sharing and Analysis Center** (BIO-ISAC, isac.bio) is a nonprofit organization dedicated to advancing cybersecurity resilience within the life sciences, biotech, and broader bioeconomy sectors. By fostering trusted collaboration among stakeholders, the BIO-ISAC serves the world as a hub for confidential information sharing, ethical coordinated vulnerability disclosure, workforce development training and education, and practical tools for navigating the intersection of cybersecurity and biology.

BIO-ISAC provides a central resource for gathering information on threats to infrastructure impacting and forming the bioeconomy including the two-way sharing of information between and among public and private sectors in order to identify, protect, detect, respond, recover, and build resilience from attacks on public and private bioeconomy infrastructure. BIO-ISAC helps spur the development and evaluation of defensive tools to address these incidents and includes vulnerability identification and mitigation, as well as education, training, and outreach, aimed at reducing risk to the nation's biosecurity infrastructure.

BIO-ISAC is a 501(c)3 nonprofit organization, formally chartered in 2021. For more information, visit isac.bio/.

Appendix III: BIO-ISAC and the Device Security Workgroup

Authors

Vincent Cervone, Purple Raven Consulting

Sri Gourisetti, Google Cloud

David Molik, Kansas State University

Whitney Zatzkin, Bioeconomy ISAC

Charles Fracchia, Black Mesa and Bioeconomy ISAC

This report concludes an inaugural, multi-year charge to the Device Security Workgroup, created to translate the comprehensive landscape of cybersecurity practices, standards, and theories by developing easy-to-use guides focused on Shared Responsibility with Equipment Vendors, Device Acquisition and Contracting, Instrument Disposal, and Advanced Network Architecture using the Zero-Trust Framework for both On-site and Cloud Storage. For more information on these materials, visit isac.bio/device.

Appendix IV: Definitions

Asset(s). Network capable equipment or software that supports the manufacturing of biological products for human consumption, agricultural, and/or livestock, or affects other critical infrastructure as defined by the Department of Homeland Security, and any of the following:

- a. Processes or stores PII, PHI, genomic information; or
- b. Reasonably carries intellectual property; or
- c. Connectivity to the public internet; or
- d. Is connected to industrial control systems required for manufacturing processes; or
- e. Carries, modified, transports, or stores the material that is being manufactured; or
Generates the offline record, batch record information, or other regulatorily-required record

Authentication (AuthN). AuthN is the process of verifying the identity of a user or system, typically through credentials like passwords, biometrics, or security tokens..

Authorization (AuthZ). AuthZ is the process of determining and granting permissions or access rights to a user or system, defining what actions they are allowed to perform or what resources they can access after their identity has been authenticated.

Bioeconomy. The bioeconomy refers to a segment of the total economy utilizing and/or derived from biological resources, and includes manufacturing processes, technologies, products, and services. These may encompass, wholly or in part, industries and products including fuel, food, medicine, chemicals, and technology. Advances in biotechnology and biomanufacturing play a substantial role in addressing a range of issues including health, climate change, energy, food security, agriculture, labor opportunities and economic growth. For more information visit:

isac.bio/bioeconomy.

Biomanufacturing. Biomanufacturing is the use of biological systems, such as enzymes, microorganisms, or advanced biological cells, to produce commercially important biomaterials and biomolecules for various applications.

Biotechnology. Biotechnology is the manipulation (through genetic engineering) of living organisms or their components to produce useful, usually commercial products (such as pest-resistant crops, new bacterial strains, or novel pharmaceuticals). Additionally, biotechnology encompasses various applications of biological science used in such manipulation.

Cloud Applications. A cloud application simply refers to any software application that is deployed in a cloud environment rather than being hosted on a local server or machine.

Cloud Service Provider (CSP). A cloud service provider is a third-party company offering a cloud-based platform, infrastructure, application, or storage services. Much like a homeowner would pay for a utility such as electricity or gas, companies typically have to pay only for the amount of cloud services they use, as business demands require.

Common Vulnerabilities and Exposures (CVEs). A dictionary of common names for publicly known information system vulnerabilities.

Cyberbiosecurity. Cyberbiosecurity is the study of activity at the intersection of cybersecurity and biosecurity. Cyberbiosecurity threats are defined as those having a biological effect, either degrading or altering the biological function of a particular product, service, or data. The most devastating cyberbiosecurity attacks are those that employ a cheap, accessible, deniable digital channel to erode the trust and integrity of the biological layer. For more information, visit isac.bio/cyberbiosecurity.

Data Diode. Data Diode is a cybersecurity device that ensures unidirectional data flow, allowing information to travel only from one network to another and preventing any data from returning. This is used to protect critical systems from cyber threats by physically enforcing a one-way communication path.

Defense-in-Depth. Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. For more information visit: https://csrc.nist.gov/glossary/term/defense_in_depth.

Demilitarized Zone (DMZ). A perimeter network or screened subnet separating an internal network that is more trusted from an external network that is less trusted.

Data Loss Prevention (DLP). A systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (i.e. data storage) through deep packet content inspection, contextual security analysis of transaction (e.g. attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of data.

East-West. The lateral flow of communications between servers within a data center, or across private and public clouds

Endpoint Detection and Response (EDR). An anti-malware system that performs behavioral analytics on endpoint events to identify potentially malicious behavior

Historians. The Historian server is the central point for managing all of the client and collector interfaces, storing and (optionally) compressing data and retrieving data

Internet-of-Things (IoT). The sensors, instruments, machines, and other devices that are networked together and use Internet connectivity to enhance industrial and manufacturing business processes and applications.

Facility Network(s). Facility Network refers to research and development, process analytics and development, biomanufacturing or other biotechnology environments that may have Operational Technologies such as benchtop facility equipment. Not to be confused with large scale

manufacturing lines which will be considered traditional Operational Technology (OT) environments.

Microsegmentation. Microsegmentation refers to a security method involving the isolation of secure zones in a data center or cloud environment. This enables IT administrators to gain more granular control over applications and workloads.

Multi-Factor Authentication (MFA). Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

Modbus. Modbus is a serial communication protocol developed by Modicon published by Modicon in 1979 for use with its programmable logic controllers (PLCs).

Network Address Translation (NAT). NAT is a service that enables private IP networks to use the internet and cloud. NAT translates private IP addresses in an internal network to a public IP address before packets are sent to an external network.

Network Architecture. Network Architecture is the way network services and devices are structured together to serve the connectivity needs of client devices and applications.

Network Detection and Response (NDR). A solution that ingests network traffic and uses machine learning to detect malicious activity and understand security risks and exposure. It combines detection for known attack behavior with the ability to understand what is normal for any given organization, flagging unusual shifts that can indicate an attack.

Network Security Monitoring (NSM). The collection and analysis of security information to discover the presence or fact of an intrusion in the IT network.

North-South. Any communication from a device that is physically located inside the data center has to perform north-south communication to interact with a device that is physically outside of the data center.

OPC UA. Open Platform Communications United Architecture (OPC UA) is a data exchange standard used in industrial automation and communication.

OPC DA. OPC DA (Open Platform Communications Data Access) is a standardized interface for access to process data in industrial automation and is based on the Microsoft standard COM/DCOM2 (Component Object Model/Distributed COM).

Operational Technologies (OT). Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

Private Virtual Local Area Network (PVLAN). Private VLAN (PVLAN) is a subdivision of a VLAN that enhances security by isolating ports within the same VLAN, allowing devices to communicate only through a designated router.

PROFIBUS. PROFIBUS links controllers and control systems with sensors and actuators on the field level (field devices) and also enables simultaneous consistent data exchange with superordinate systems.

PROFINET. PROFINET is an open Industrial Ethernet solution based on international standards. It is a communication protocol designed to exchange data between controllers and devices in an automation setting.

Public Cloud Services. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Remote Desktop Profile (RDP). Remote Desktop Protocol (RDP), a secure network communication protocol offered by Microsoft, allows users to execute remote operations on other computers. It facilitates secure information exchange between remotely connected machines over an encrypted communication channel.

Secure Access Service Edge (SASE). Secure access service edge (SASE) is a cloud-native architecture that unifies SD-WAN with security functions like SWG, CASB, FWaaS, and ZTNA into one service.

Secure-By-Design. A software design and development methodology that aims to create systems that are impenetrable to cyberattack.

Secure Web Gateway (SWG). A secure web gateway (SWG) is an on-premises or cloud-delivered network security technology that filters internet traffic and enforces corporate and regulatory policy compliance.

Security Information and Event Management (SIEM). Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

Shadow Sessions. Shadow Sessions enable users with the proper system privilege to remotely connect to a different user's session on a device.

Unidirectional Gateways (UGW). Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another but is physically unable to send any information at all back to the source network. The software replicates databases and emulates protocol servers and devices.

Virtual Network Computing (VNC). Virtual Network Computing is a technology that enables remote access and control of a computer over a network.

Vulnerability. A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. The inability to withstand adversity. A condition that enables a threat event to occur. ([NISTIR 8286](#)). A known weakness in a system, system security procedures, internal controls, or implementation by which an actor or event may intentionally exploit or accidentally trigger the weakness to access, modify, or disrupt normal operations of a system resulting in a security incident or a violation of the system's security policy. ([CNSSI 4009](#)).

Zero Trust Network Access (ZTNA). A security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The zero trust security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

Appendix V: Additional Resources

1. <https://www.isac.bio/>
2. <https://www.nist.gov/publications/zero-trust-architecture>
3. https://www.imprivata.com/sites/imprivata/files/2022-10/2022-0718_zero-trust-checklist-portrait.pdf
4. <https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture>
5. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.20.pdf>
6. <https://www.portnox.com/blog/network-security/zero-trust-checklist/>
7. <https://www.cisa.gov/resources-tools/resources/microsegmentation-zero-trust-part-one-introduction-and-planning>