ZIVARO

···· BRILLIANT IT ····

Cisco Zero Trust for IT and OT Integration

By Rian Powell and Jeff Hill, Consulting Engineers

INTRODUCTION

Traditional boundaries between IT (informational Technology) and OT (Organizational Technology) are being blurred or in some cases wiped out by new smart sensors and connected machinery and devices. Organizations in the utility, energy and health care spaces want to gain the competitive advantage from real-time information to accelerate business decisions, improve efficiency, gain cost savings, and reduce waste. The risk of this convergence is primarily in the cyber security of these organizations who represent services critical to society or sensitive information. Traditionally OT resources were not connected to any network or were part of an air-gapped OT network. This provided security but limited or eliminated the organizations' ability to gain information about productivity, asset health or use real-time information to inform decision makers about critical business metrics. Organizations are consolidating IT and OT to gain this visibility and need guidance for merging these two environments that result in a secure and performant network.

THE PROBLEM

Companies are converging their IT (informational Technology) and OT (Organizational Technology) networks to achieve better visibility, agility, and standardization. This change is being driven by business factors but exposes organizations to increased security risks. The devices in a traditional OT network enable or monitor critical infrastructure prevalent in industries providing utilities, water, public safety, national security, and critical commodities to name a few. Exposing these OT systems to today's cyber threats puts these industries, our citizens, and the economy at much greater risk for disablement or sabotage. Organizations need a methodology to enable this convergence with security controls and solutions which ensure safety and security of the data and the underlying devices and software.

BACKGROUND

The current cyber-security landscape is filled with bad actors using a variety of exploits to gain access to critical systems in a variety of businesses including utilities, government agencies, and critical pillars of national infrastructure such as hospitals, resource pipelines, water treatment and military programs. Industrial control systems that were designed with a focus on industrial productivity and sometimes proprietary protocols do not have the standard security protocol found in traditional IT platforms. As the OT systems are removed from the air-gapped OT network and attached to the IT network they represent an expanded attack surface. Several events in the media have highlighted not only the vulnerability of these systems, but also the importance of these services to public health and safety.

In May of 2021 President Biden signed an Executive Order on Improving the Nation's Cybersecurity known as Presidential Executive Order (PEO) 14028. This executive order outlines many initiatives to strengthen the security posture of utilities and businesses deemed critical to national security and public safety. This guidance specifically laid out plans for power grid cybersecurity in addition to Zero Trust, citing "The scope of protection and security must include systems that process data (information technology (IT) and those that run the vital machinery that ensures our safety (operational technology (OT)."[1] Released in April 2021, the Biden administration announced that the Department of Energy and DHS's Cybersecurity and Infrastructure Security Agency (CISA) would coordinate with our nation's electric utility industry to raise the bar on industrial control system cybersecurity in the utility industry. This 100-day action plan was focused on increasing OT visibility, detection, and response in ICS networks, and culminated with President Biden signing a National Security Memorandum focused on ICS technology adoption across other areas.

One sector that has come under attack from cyber criminals recently is healthcare, and the attacks have not only had a significant economic impact but have also affected patient care and in a few cases contributed to patient deaths. On October 14, 2021, the Hillel Yaffe Medical Center in Israel was a victim of a cyber-attack resulting in the hospital having to rely on “alternative systems to treat it’s patients”, and Israel’s National Cyber Directorate reports that one in every five businesses in Israel have been targeted in a cyber-attack. Attacks in France on hospitals and other public entities has prompted the National Cybersecurity Agency of France to earmark 500 million Euros to help boost cyber defense systems to respond to the 225% increase in ransomware attacks in 2020 compared to the previous year. In the US, the University of Vermont Health Network took months to completely recover from an October 2020 attack that they estimate cost $63 million and impacted patient care.

In February 2021, a hacker gained access to the water treatment plant in Oldsmar, FL. Once the hacker gained access to the water treatment control systems, he increased the amount of sodium hydroxide in the water. Fortunately, an employee at the plant noticed the change and reversed it, preventing any health impact to the public. Traditionally systems like water treatment or oil pipeline controls were in air-gapped OT (Operational Technology) systems, but to modernize and streamline operations, companies and utilities are connecting OT networks to IT networks, exposing them to heightened malicious activity. OT systems are often not maintained with the latest patches and firmware due to uptime requirements, and common security measures like encrypting data in flight were not followed in OT environments due to their air-gapped nature. As OT is integrated into the IT environment to take advantage of functionality such as monitoring, centralized logging, and data protection, the OT systems need to be aligned to current IT security control measures.

In another example, The U.S. Department of Homeland Security reports that the manufacturing industry is the second most targeted industry, based on the number of reported cyber-attacks[2]. Given how critical ICS are to operations, cyber-attacks against ICS devices present a real threat to safety and production, which can result in damaging economic impact to a manufacturing organization.

THE SOLUTION

Zivaro Consulting & Cisco Zero Trust Framework
Simply put, Cisco Zero Trust framework is a platform that permits “least privileged access.” Users are challenged at every point where they attempt to gain further access inside the enterprise network, including both Information Technology (IT) and Operational Technology (OT). Once their identity is confirmed, access is granted & monitored. This process is repeated across the enterprise to ensure network security.

Cisco highlights the “3 W’s” as the crucial elements necessary to harden an enterprise network & enhance the enterprise security posture. These “3 W’s” are defined as the Workforce, the Workload & the Workplace.

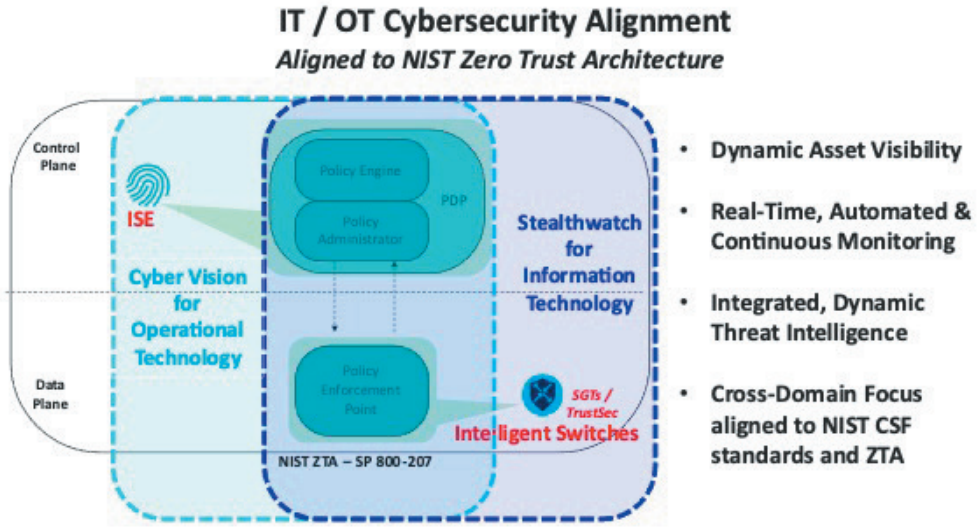
The Workforce, Workload & Workplace must be secured to limit the attack surface & block malicious threats. This approach protects the enterprise from both external threats as well as internal threats.

Cisco offers a comprehensive, Zero Trust approach that secures access across applications & environment, from any user, any device & any location.

Cisco's Zero Trust framework allows you to:

- Consistently enforce policy-based controls
- Gain visibility into users, devices, components, and more across enterprise environments
- Get detailed logs, reports, and alerts that can help you better detect and respond to threats
- Provide more secure access, protect against gaps in visibility, and reduce attack surface with Cisco Zero Trust
- Automate threat containment based on any changes at the "Trust Level"

CISCO ZERO TRUST ARCHITECTURE FOR INTEGRATING OT INTO IT



STEPS TO ZERO TRUST

The complex nature of IT and OT environments do not allow for a silver bullet solution. Rather than recommending a specific product at the onset, Zivaro's approach to implementing controls in support of PEO 14028 starts with an assessment. Detailed environmental assessment data is collected to help arrive at a defined state of categorization and giving a holistic view of the data landscape requiring safeguards. The design and implementation of technology is dependent on security boundaries, data classification and definition, and segregation of the internal and external systems.

Zivaro assessments identify necessary changes to ensure proper alignment with the objectives of the organization, providing the appropriate levels of CIA (confidentiality, integrity, and availability), and creating an executable foundation for Zero Trust. Zivaro utilizes various and applicable industry standards during reviews. As an example, standards could be IEEE 802.1x or IEEE 802.3ae-2002, FIPS 199, NIST (National Institute of Standards and Technology) 800-53, 800-60. As a Cisco Master ATP and Gold-certified partner, we may use best practice from a Cisco Validated Design, or Cisco Solutions Reference Network Design, or Cisco Preferred Architecture. If desired, Zivaro can apply the NIST Cybersecurity Risk Management Framework during the review process for recommendations.

Although specific products may utilize and support Zero Trust, there are important nuances in Zero Trust solutions. Zivaro understands these nuances and knows how to effectively architect Cisco's security portfolio while meeting the PEO objectives of prevention, detection, remediation, and lessons learned.

Key areas of Zero Trust strategy include consolidating agency identity systems, combatting phishing through strong multifactor authentication, treating internal networks as untrusted and encrypting traffic, moving protections closer to data by strengthening application security, and more. The selection of tools and products along with proper architecture processes are critical to ensure the design meets all federal requirements and controls. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure to focus on protecting data in real-time within a dynamic threat environment.

In any engagement Zivaro takes the approach of how to best leverage existing investments to help drive their transformation. It is common for any organization to technical 'debt' to be leveraged which will also come with interoperability and integration considerations. In any technology replacement, it is paramount to ensure that the solution integrates seamlessly and minimizes any technology or mission disruptions.

ZERO TRUST NETWORK ASSESSMENT GUIDELINES

Zivaro recommends assessing the following technology areas, policies, and procedures:

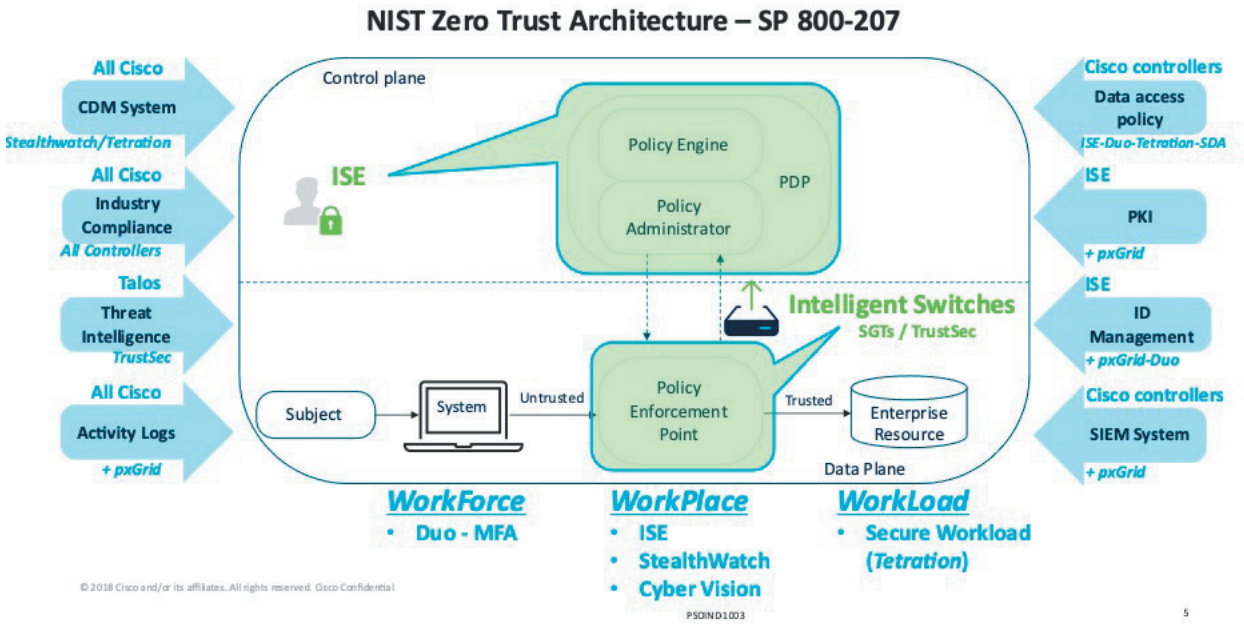
- Configuration of network infrastructure
- Maintenance of network infrastructure
  - Device Deployment methods
  - Configuration change management procedures
  - Centralized Configuration Backup
  - Centralized Configuration Automation
  - Configuration change capabilities
  - Configuration Change Management Workflow
  - Change Control Management
- Traffic Flow
  - Application Traffic Flow, Datacenter, Internet Edges, Client Access, WAN, Cloud
  - Routing
  - QOS Standards
- Existing network segmentation practices
  - Access control lists
  - Control Plane Policing/Security
  - Infrastructure Device Access, CoPP
- Firewalls:
  - Configuration and positioning on the network
  - Firewall Policies
  - VPN solution
  - Remote location and Client Access Capabilities
  - Attack Awareness (IPS/IDS)
- Infrastructure Monitoring and Management
  - Central Monitoring/Alerting Capabilities
  - Syslog Capabilities
  - Controls, retention, management
  - Host End Monitoring/Management
  - Deployment processes for upgrades/patches
  - Configuration validation capabilities
  - EoL/EoS hardware and licensing and process for Lifecycle and licensing compliance
- Review Automation possibilities within the LAN/WAN infrastructure

After the assessment data has been analyzed and following the review process, Zivaro would then provide a high-level roadmap for a more strongly secured environment, prioritized by level of risk and detailing recommendations. The report will include a rough order of magnitude cost estimate, timeline, and required activities and resources to fulfill the recommendations. Recommendations consider constraints, security objectives, organizational strategic objectives, existing investments, and current missions.

CISCO TECHNOLOGY PICKS FOR ZERO TRUST IN COMBINING IT WITH OT

Below is a categorical reference list of sample Cisco ZeroTrust solutions with reference to IT and OT categories:

1. Network Performance Monitoring
   a. DNA Center (internal networks)
   b. Cisco Secure Network Analytics (StealthWatch)
   c. ThousandEyes – (SaaS monitoring, external internet monitoring)
   d. AppDynamics (Internal Apps/Services)
2. Virtualization and Cloud Management
   a. Umbrella
   b. CloudLock
   c. Intersight and Workload Optimization Manager
   d. Cisco Secure Workload
3. Voice Network Quality Management
   a. ThousandEyes
   b. Cisco Secure Network Analytics (StealthWatch)
4. Network Configuration Management for Power Operations
   a. CyberVision
5. Identity and Access Management
   a. Cisco Duo
   b. Identity Services Engine / pxGrid
   c. Cisco SecureX
6. Threat Intelligence
   a. Cisco Talos



We will discuss some of the solutions in the Cisco Zero Trust framework below. Cisco Zero Trust Architecture (ZTA) starts with a comprehensive paradigm to secure all access across applications and environment, from any user, device, and location by securing the 3Ws:

- Workforce with DUO
  - Browsing Protection: DUO provides Endpoint Trust verification on browser versions as part of the authentication workflow for in-line browser applications
  - Remote Access Corporate Resources: DUO provides User and Endpoint Trust with MFA and OS, and allows for Endpoint Hardening policy during authentication workflow
  - Secure Access to SaaS: Secure Access to SaaS applications via 0365 integration
  - Zero Trust Network Access: Duo provides User and Endpoint Trust, per application, for every authentication, all the time
- Workplace with Cisco Identity Services Engine (ISE)
  - Cisco ZTA, combined with ISE, enables users to securely connect to networks from any device, anywhere while restricting access from non-compliant devices
  - Cisco's automated network-segmentation capabilities allow micro-perimeters for users, devices, and application traffic without requiring network redesign
- Workload with Cisco Secure Workload (Tetration)
  - Cisco ZTA, combined with Tetration, allows for secure connections to APIs, microservices, and containers that access applications, whether in the cloud, data center, or other virtualized environments.
  - Deployed on-premises or in the cloud, Tetration secures app stack, and micro-segmentation helps you contain threats and protect against lateral movement by providing visibility into applications, application segmentation, and application performance monitoring, as well as gain clarity into application architecture

THOUSANDEYES

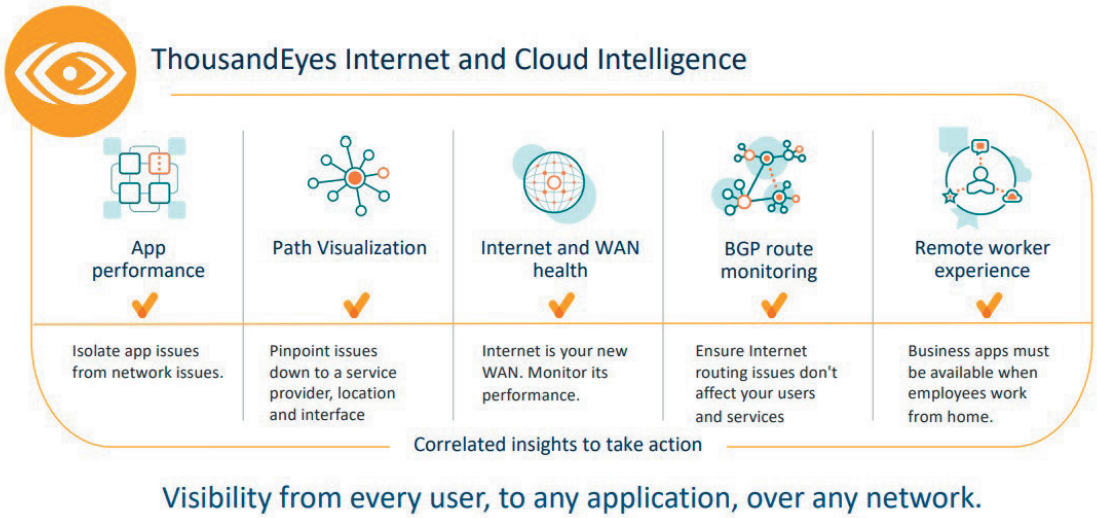
With the increased reliance on the internet and cloud services, more networks are outside ownership or direct control. Organizations need to ensure the performance and integrity of the underlying transport, even when you do not own the infrastructure or control how service providers route traffic. ThousandEyes gives companies a real-time map of how their customers and employees reach and experience critical apps and services across traditional, SD-WAN, Internet, and cloud provider networks. With ThousandEyes, companies can see beyond their edge and get visibility into networks and external dependencies outside of their control.

ThousandEyes not only gives complete visibility from the user to the application over any network, but also provides actionable insight into any performance issues so you can resolve incidents quickly to maintain reliable connectivity and optimal application experience. ThousandEyes is an Internet and Cloud Intelligence platform focused on monitoring and troubleshooting network performance for SaaS and cloud applications

Benefits

- Reduce Mean Time To Identify and Resolve (MTTI/MTTR) by immediately pinpointing the source of issues across internal network, ISPs, and cloud and application providers
- Gain successful escalations with service providers based on data that can be easily shared across internal and external stakeholders
- Eliminate wasteful finger pointing and effectively manage OLAs/SLAs across internal teams and external providers

By integrating Cisco SD-WAN with Cisco ThousandEyes, you can gain granular insights into network and application performance with full hop-by-hop path analysis across the Internet, and isolate fault domains for expedited troubleshooting and resolution.



While not an active security solution, ThousandEyes can provide visibility and support for the operational security teams in real time, and provide pre-post analysis via a ShareLink and share information with Splunk dashboards through REST APIs. For example, ThousandEyes can alert a SOC when part of an IP space is announced from a different AS (indicating a BGP leak going on). Or another example, alert when a domain-to-IP mapping is changed around the globe (catching tampering with DNS as it happens—a common attack that is hard to catch without an external view.)

CISCO APPDYNAMICS

ThousandEyes Digital Experience Monitoring and Internet Visibility coupled with AppDynamics Application Performance Management (APM) is a winning combination that ensures complete application service visibility and delivery with minimal down time utilizing a security overlay.

AppDynamics and ThousandEyes together complete the end-to-end service visibility challenge. AppDynamics provides insight into application-level performance - code, instrumentation, and business transactions. It focuses on everything “behind the public facing portal”. ThousandEyes provides the outside in visibility from endpoint, global vantage points, internet, and browser synthetics. AppDynamics can monitor all Applications and ensure Service Level Agreements of 99.8% availability on a 24/7/365 availability Window. AppDynamics monitors availability by Website URL monitor, TCP Port, and others.

CISCO SECURE NETWORK ANALYTICS (FORMERLY STEALTHWATCH)

Cisco SNA is a comprehensive network detection & response (NDR) solution that provides enterprise-wide visibility, from the private network to the public cloud & applies advanced security analytics to detect and respond to threats in real-time. As OT networks get merged into IT networks, SNA is an excellent tool for network traffic inspection, analysis, and threat detection. For those entities adhering to NIST security standards (which require all traffic to be inspected, logged, and analyzed), SNA will detect threats in NetFlow that may bypass traditional security controls, providing a defense-in-depth architecture which continuously verifies trust across the network.

Using a combination of behavioral modeling, machine learning & global threat intelligence, SNA can quickly and with high confidence detect threats such as C&C attacks, ransomware, DDoS attacks, illicit crypto mining, unknown malware, and insider threats. With a single agentless solution organizations get comprehensive threat monitoring across the data center, branch, endpoint & cloud, and even encrypted traffic. The SNA visibility also includes knowing every host—seeing who is accessing which information at any given point. This visibility is a critical element to achieve a Zero Trust Architecture.

As a ZT component solution, SNA has a specific purpose related to recent federal cyber guidance. In August of 2021 as part of President Biden's cyber executive order, the Office of Management and Budget (OMB) released Memo 21-31 to provide federal agencies guidance on required event logging and data retention. The guidance outlines an event log maturity model with 4 tiers: Not Effective/Basic/ Intermediate/Advanced. The memo included a one-year requirement (Aug 2022) to meet the Basic tier and 24 months to reach Advanced. As you can see SNA can easily help an organization meet and exceed these recommendations.

CISCO SECURE WORKLOAD (FORMERLY TETRATION)

Cisco Secure Workload achieves the security required for today's heterogeneous multi-cloud environments. Cisco Secure Workload protects workloads across any cloud, application, and workload--anywhere. Automate and implement a secure Zero Trust model for micro-segmentation based upon application behavior & telemetry.

Deployed on-premises or in the cloud, Cisco Secure Workload secures the app stack, and micro-segmentation helps you contain threats and protect against lateral movement by providing visibility into applications, application segmentation, and application performance monitoring, as well as gain clarity into application architecture.

CISCO UMBRELLA

Cisco Umbrella is the cloud-native, multi-function security service at the core of Cisco's SASE architecture. It unifies firewall, secure web gateway, DNS-layer security, Cloud Access Security Broker (CASB), and threat intelligence solutions into a single cloud service to help businesses of all sizes secure their users, applications, and data.

As more organizations embrace direct internet access, Umbrella makes it easy to extend protection to roaming users and branch offices. Umbrella provides global coverage with a broad set of high throughput data centers and peers with more than 1000 of the world's top Internet Service Providers (ISPs), Content Delivery Networks (CDNs) and SaaS platforms to deliver the fastest route for any request, resulting in superior speed, effective security, and user satisfaction.

Umbrella utilizes DNS layer security to block requests to malware, ransomware, phishing, and botnets before a connection is established. The secure web gateway provides logging and deeper inspection for all web traffic for greater transparency, control, and protection. The cloud-delivered firewall helps to log and block traffic using IP, port, and protocol rules for consistent enforcement throughout the environment.

CASB functionality is included to detect and control the use of cloud applications. With Cisco SecureX (included with all Umbrella subscriptions) you can accelerate threat investigation and remediation. Cisco Umbrella offers complete protection faster, with industry-leading security efficacy and performance.

Benefits

- Stop threats earlier before they reach network or endpoints
- Enforce broad, reliable security coverage across all ports and protocols
- Deliver rapid, scalable security protection on and off network
- Accelerate threat investigation and remediation with contextual intelligence
- Leverage a single security dashboard for efficient management
- Get reliable performance from a global cloud architecture with 100% uptime since 2006

Cisco Umbrella offers complete protection faster, with industry-leading security efficacy and performance.

CISCO CYBER VISION

Cisco Cyber Vision has been specifically developed for OT & IT teams to work together to ensure production continuity, resilience & safety. This enables deeper integration between IT, cloud & industrial control networks (ICS) to limit exposure of industrial operations to cyber threats. Cyber Vision expands many of the IT system functionalities in StealthWatch in the OT environment.

Cisco Cyber Vision provides full visibility into ICS, including dynamic asset inventory, real-time monitoring of control networks and process data, and comprehensive threat intelligence, so you can build secure infrastructures and enforce security policies to control risk.
Cyber Vision leverages a unique combination of passive and active discovery to identify all assets with no risk to devices and processes. As discovery is performed by industrial network elements, inquiries are not blocked by firewalls or NAT boundaries, resulting in 100% visibility.

Maintain system integrity and production continuity. Cisco Cyber Vision understands proprietary industrial protocols to keep track of process anomalies, asset modifications and variable changes. It is the "flight recorder" of industrial infrastructure.

Cisco Cyber Vision leverages a two-tier deployment architecture and unique edge computing capabilities that offer the simplicity and cost saving benefits industrial organizations look for when deploying OT security at scale. Cyber Vision sensors are embedded into Cisco's industrial network equipment, so that you can easily gain visibility on both east-to-west and north-to-south traffic anywhere in the network. Industrial application flows are decoded at the edge, so there is no need to mirror traffic, which can cause network congestion and jitter. Embedding DPI in the existing network hardware simplifies security deployment and makes it scalable.

Cisco Cyber Vision provides full visibility into industrial control systems so you can build secure infrastructures and enforce security policies to control risk. Combining a unique edge monitoring architecture and deep integration with Cisco's leading security portfolio, Cisco Cyber Vision can be easily deployed at scale so you can ensure the continuity, resilience, and safety of industrial operations.

Cisco Cyber Vision brings detailed information on OT assets and threats to Cisco Firepower firewalls, the ISE access controller, and the StealthWatch traffic analyzer so you can build and enforce security policies without disrupting production.

Cisco Cyber Vision logs all events from ICS for efficient audits, build incident reports, and work with both IT and OT teams to drive actions and provide and retain information to comply with the latest regulatory assessments, reports, and requirements (NERC CIP, NIST 800-53 Evidence, NIST FISMA).

CONCLUSION

Active data breaches, presidential and other regulatory mandates, and the need to reduce risk to national infrastructure require organizations to get serious about integrating IT and OT security architecture. Whether a utility, a hospital system, or a manufacturing entity, Zero Trust is the necessary and next evolution in securing critical national infrastructure. Cisco is a technology leader demonstrating significant market leadership both in its product portfolio and vision to help organizations move towards a sustainable Zero Trust Architecture. Achieving ZTA does not start by simply buying products, but understanding an organization's specific requirements, operating environment, and policies, then correctly applying specific technologies in a manner consistent with ZTA and best practices. Together, Zivaro and Cisco are ready to help secure the mission of any organization looking to fortify their OT environment with Zero Trust principals.

APPENDIX A REFERENCES

[1]. Executive Order 14028 of May 12, 2021 Federal Register :: Improving the Nation's Cybersecurity
[2]. Stouffer et al., Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology Special Publication 800-82 Revision 2, Gaithersburg, Md., May 2015. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.
[3]. CISA Supplemental Guidance on Emergency Directive 21-01 https://cyber.dhs.gov/ed/21-01/