TXOne Networks

2022 /Q4

Futureproofing Critical Services

Against Tomorrow's Cyber Threats

txOne networks

TXOne Networks

Futureproofing Critical Services

Against Tomorrow's Cyber Threats

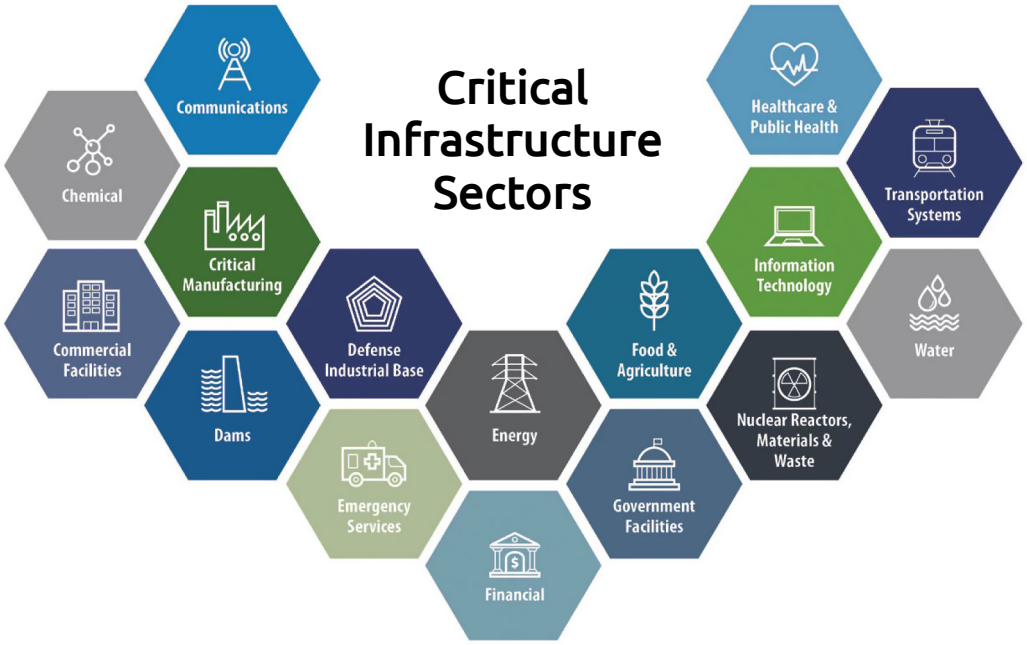
txOne networks

Futureproofing Critical Services
Against Tomorrow's Cyber Threats

Table of Contents

Introduction

Critical infrastructure (CI) encompasses everything that you don't think about until it stops functioning. As long as your cell phone has bars and the lights stay on, there is little attention paid to the communications and energy systems that power our daily life. We travel around our cities without considering that stoplights might malfunction or a metro train might get stuck in a dark tunnel. Packages with any manner of items are delivered to our doorstep. Most of the time, gas flows silently through gas pipelines without incident and the neighborhood nuclear reactor issues no alerts. Many systems are working behind the scenes to maintain the critical infrastructure that is vital to our well-being – when a bad actor shuts it down or destroys it, we are suddenly confronted with challenges at best and catastrophe at worst.



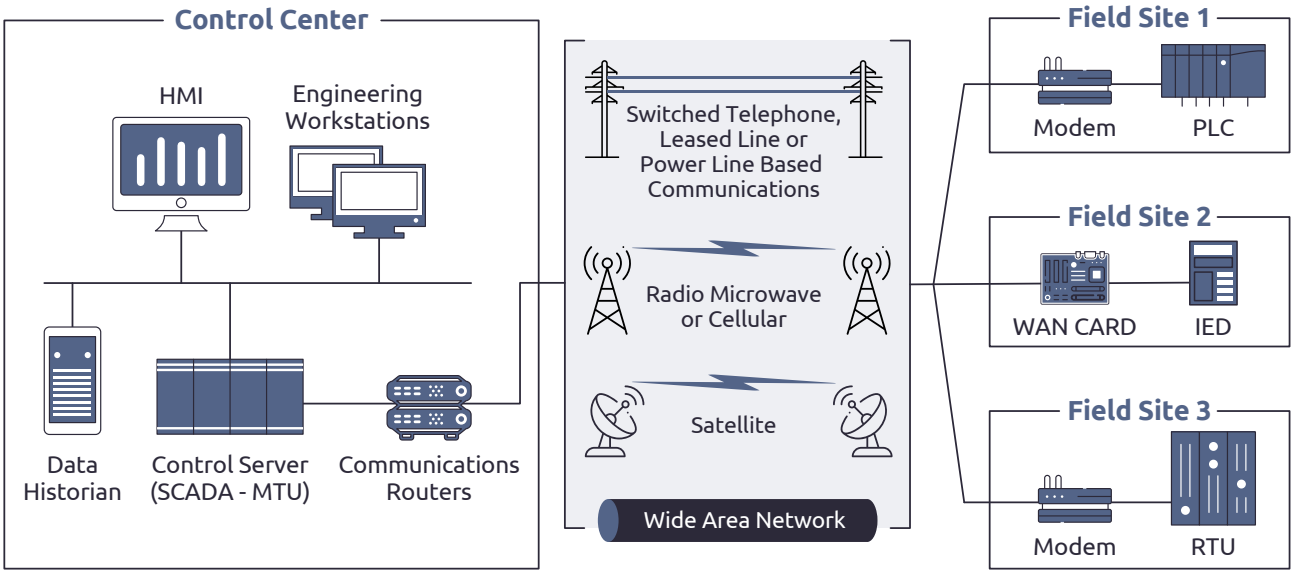
https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19

Experts must address needs for their population based on their geography and the natural resources in their country along with the unique aspects of their industry.[1] Therefore, CI is often divided into sectors.

[1] *Critical Infrastructure Sectors (2020), https://www.cisa.gov/critical-infrastructure-sectors (accessed May 18, 2022).*

Cyber-Physical Systems

Each CI sector relies on operational technology, the cyber-physical systems that employ machines to perform tasks in the physical world. OT devices receive and evaluate sensor readings. They then send control commands to machines, robots, cobots, other devices, or other systems. Machines do the work while operators monitor their performance. Ever since the famous Stuxnet worm, threat actors have been aiming to inject malware in order to lull operators into believing that plant operations are functioning normally when in reality they are under attack. They do this by patching into communications systems and replaying a loop of normal operations. At the same time, they send malicious command controls to poison water, explode equipment, or disrupt other critical operations.



SCADA System General Layout

SCADA systems often control critical infrastructure systems. Commands are sent from Human Machine Interfaces (HMI) over a network to programmable logic controllers (PLC) and remote terminal units (RTU) to control how machines perform work. Sensor readings inform how commands are executed.

OT Zero Trust Protects Critical Infrastructure

The foundation of OT zero trust is **never trust and always verify to keep the operation running**. Cybersecurity appliances must always be on the lookout for tricks by hackers. They must maintain 360 degrees of situational awareness so they can adapt to what's happening in the plant the instant it is happening. For regulated sectors, OT zero trust provides a foundation for achieving any risk-based compliance certification through its four cornerstones. Critical infrastructure can be protected when we inspect, lock down, segment, and reinforce cyber defenses.

OT Zero Trust: CI's Secret Weapon

Until recently, OT systems were isolated from one another. A bad actor had to travel to a facility in order to launch malware. There was no urgent need for security patches, so some valued equipment became outdated. These legacy or heirloom systems may still be running versions of Windows that are no longer supported by Microsoft. Such systems have become hotbeds for viruses and Trojans (two types of malicious code). Other systems may be separated from the network, either by design or because they lack the capability to be connected. Traditional IT anti-malware was never designed to safeguard these systems because there is no way to inspect a device without an internet connection. OT zero trust has a secret weapon designed specifically to help you extend the life of legacy and air-gapped systems by protecting them from cyber attacks.

OT zero trust portable security devices can stop ransomware and other attacks before they get started. A portable security scanner looks like a USB drive. An OT zero trust portable security device looks like a USB drive. Simply plug it in and inspect your device. It will wipe malware and take inventory of computer information, along with the software and firmware that has been installed. This inventory is automatically uploaded to a central OT defense console where it continually undergoes traditional and machine learning analysis to gather the best protections.

OT Zero Trust Cyber Safe Networks

More and more OT is being connected to the internet. Machines in one plant are interconnected with each other. Facilities in different CI sectors are also interconnected. It is now possible for ransomware to hijack one facility before cascading to take over other CI sectors too. The Colonial Pipeline attack is a good example of this type of attack. Hackers launched ransomware at only one oil and gas pipeline, but the disruption it caused had a ripple effect throughout other sectors until the president of the USA was compelled to declare a state of emergency.

Never trust – always verify. That is the fundamental idea of OT Zero Trust. CI networks that are segmented using OT firewalls can evaluate the current situation and only allow command controls to be carried out that are trustworthy under the immediate circumstances. They can quarantine infected systems and stop the spread of malware both within the plant and beyond. OT zero trust network security appliances such as IPSes and firewalls fit neatly into existing OT-field network topology. Trustworthiness is based on in-depth protocol analysis, machine-type, and your security policies.

OT Zero Trust Endpoint Protection

Allow lists lock down endpoint assets with the same trust analysis used by OT firewalls. Security patches stop known attacks before they start. Zero day attacks are stopped by using virtual patches. Advanced threat intelligence based on machine-learning is used to reason about new vulnerabilities that may be under development by hackers. Cyber defenses are reinforced through continual inspections and updates. Using OT zero trust portable security devices, even legacy or air-gapped endpoints stay safe.

CI Sector Protections

Security appliances based on the OT zero trust philosophy are being used to protect every sector of critical infrastructure.

Smart Buildings

Cybersecurity for commercial, government, and defense facilities focuses on building systems. OT zero trust appliances understand the KNX protocol, BASnet, and other protocols used in HVAC (heating, ventilation, and air conditioning), lighting, security, as well as building access specialty protocols. So far, there have not been many attacks on building systems, but in one case, bad actors cut off the heat in an apartment building in Finland during the winter. Another attacker locked hotel guests in their rooms until a ransom was paid. OT zero trust can "keep the heat on" cyber attackers by making sure your building systems are cyber safe.

Smart Factories

Critical manufacturing plants run complex automation such as assembly lines with robots that build every type of vehicle from ships to airplanes to heavy-duty earth movers and irrigation equipment. Chemical factories often use equipment that is under high pressure and can explode. They may also produce toxic chemicals that can be leaked into the environment.

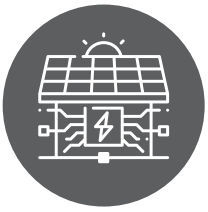
OT zero trust portable security devices are being used to stop supply chain malware from entering manufacturing plants. These security devices are protecting many varieties of legacy and air-gapped equipment. They can even detect cross-platform malware that infects both Windows and Linux devices. Sometimes data must be hand-carried from robot to robot or device to device. OT zero trust portable security devices provide secure data transport.

OT zero trust portable security devices are used for routine and surprise inspections to wipe malware and keep inventory up-to-date. They work with a suite of OT zero trust security devices that were built to withstand harsh environments that exist in manufacturing plants. They cover the entire production site so you can view the OT defense console to see what's going on at any given time. Security logs provide information. Emergency response teams can use this console to investigate and complete incident reports.

Trustworthy Communications

Communications and Information Technology sectors provide the main conduit for sending information to all the other sectors. Digital endpoints need more than IT anti-malware, they need endpoint protection to stop known malware before it starts. Virtual patches are critical to safeguard computers while waiting on a vendor solution. Imagine if your devices had enough threat intelligence to outsmart hackers and prevent new types of malware. OT zero trust devices can do this and more. They also collect and send data to your central OT defense monitor so you can see what's going on with communications every moment.

Smart Energy



The energy sector and nuclear sector have become popular targets of ransomware. The Stuxnet worm has been re-purposed to attack Triconex controllers. Versions of this malware have been launched at Middle Eastern oil and gas companies, as well as those in the USA and Eastern Europe. To combat ransomware, OT firewalls segment networks so that a single attack cannot infect the entire energy generation plant or pipeline. Trust lists and allow lists consider what's happening in the moment right now and make informed trust decisions based on your goals and risk tolerance. They will only allow trustworthy command controls to reach machines.

Safe Financial Services

Financial services rely on IT systems for banking, stock trading, and other services. However, Point-of-Sale (POS) systems have become a target after the REvil ransomware attack at a retail store. OT zero trust endpoint protection prevents future attacks from REvil. Endpoint protection also zaps zero day attacks even for resource-constrained devices by using virtual patches. OT zero trust gives central threat visibility along with threat intelligence based on insights from machine learning.

Traditional and Autonomous Transportation

The transportation systems sector is vast. There are several sub-sectors including aviation, maritime, mass transit, highways, railroads, and pipelines. Self-driving vehicles create new cybersecurity challenges. OT zero trust portable security devices are being used to protect a wide range of devices onboard vehicles and at vehicle service centers or manufacturing plants. These security devices provide portable protection with installation-free malware scans and cleanup. You can also use them for secure data transport and to detect cross-platform malware. They stop supply chain infections when used to inspect new devices before they are deployed or installed onboard a vehicle. Transient systems can be inspected so the production life of these assets is extended.

Another Mass Casualty Threat?

Inside a water treatment facility, a plant operator checks a monitor. Everything appears to be functioning normally. What they don't realize is that they are actually watching a pre recorded loop of normal operations. Inside the plant, an infected PLC is injecting dangerous levels of chlorine into the local water supply. That's the attack bad actors were attempting in April 2020 in Israel where hundreds of people could have become ill from drinking contaminated water.[2] In 2021, an insider attack was discovered at a water plant in Florida. The attack was thwarted because an operator observed strange mouse movements on his monitor.

Critical infrastructure (CI) is vital to our well-being. We expect safe drinking water to flow from fresh water reservoirs protected by dams through clean pipelines to our faucet. If the grocery store shelves are fully stocked, we spend very little time thinking about vegetables growing at a farm and being processed at the plant. An ambulance arrives quickly when someone has a heart attack. Many systems are working behind the scenes to coordinate these critical infrastructure sectors. If a bad actor tampers with the food, water, or medical sectors of critical infrastructure, we face another health crisis or worse.

[2] *IMA Webinar Broadcast: A Mass Casualty Threat? The Risk to Water Infrastructure from Cyber Hackers, InfraGard National Members Alliance Capital Region (accessed May 2022).*

Smart Healthcare Protections

The healthcare sectors protect us from infectious disease outbreaks and patch us up after natural or man-made disasters. Hospitals provide local treatments, and laboratories allow scientists to invent new medicines and perform all kinds of health tests. Laboratory and hospital equipment tend to be stand-alone, proprietary systems that are highly specialized and highly regulated. Anyone who has taken a vaccine, undergone laparoscopic surgery, or been enclosed in an MRI chamber understands how painful it could be if a bad actor were to disrupt medical equipment.

OT zero trust portable security devices are already at work in healthcare facilities supporting installation-free scans and malware cleanup. Device health checks are being performed routinely and on demand. OT zero trust portable security devices are also being used to guard against insider threats or unsuspecting vendors inadvertently bringing a dirty USB that injects malware. When every device is scanned before it enters a laboratory, hospital, or healthcare institution, these inspections can clean up malware along with unauthorized applications. They can also shine the light on shadow IT . Shadow IT has been a problem because it is difficult to share data between silo-ed healthcare systems. Well-meaning workers come up with clever "work-arounds" that most often downgrade cybersecurity out of ignorance of proper security procedures. OT zero trust portable security devices can replace these homegrown shadow systems and make sure data sharing is secure.

OT zero trust supports compliance with FDA, GMP, GLP, as well as similar international regulations. It transforms procedures for using OT zero trust into SOPs for rock-solid standard operating procedures with cybersecurity built-in.

Safe Emergency Services

Responding to emergencies requires a wide range of technology with a human in the loop. Robots or automated devices are not yet fully capable of independently performing search and rescue. However, fire inspection drones have been tested flying over rural fires in conditions too dangerous for human pilots. Law enforcement drones are being tested in cities. OT zero trust portable security devices can inspect both remote control and autonomous drones. OT zero trust devices have also been tested on board autonomous mobile robots to prevent brute force login hacks and denial of service attacks.

Food and Agriculture Safeguards

Contaminated food recalls are nothing new. Over the years, we've heard about E. coli in spinach, botulism in tuna, and recently, salmonella in peanut butter. Food processing plants are often highly automated. For example, at a potato processing plant, conveyors ferry potatoes from the farm truck through various processing machines where they are sliced and diced into potato flakes. Then, they are packaged and labeled before being loaded by robotic arms and driven to stores or fast-food restaurants. More and more these delivery trucks are autonomous. All of these machines report status to a central control console that sends corporate executives up-to-the-moment status reports to their phone anywhere in the world.

OT zero trust is providing endpoint protection for equipment in food processing plants to stop known malware before it starts. Virtual patches guard devices while waiting on a stable vendor solution. Threat intelligence looks ahead of attackers to reason about and predict new assaults. OT zero trust devices collect and send data to the OT defense console which provides real-time visibility. OT zero trust compliant security devices are designed to fit neatly into OT-field network topology. OT zero trust has been proven to support compliance with ISA/IEC 62443, a series of standards to mitigate security vulnerabilities in industrial automation and control systems (IACSs).

Safe Drinking Water

It goes without saying that we all need safe drinking water. In 2021, an outdated version of Windows and a weak cybersecurity network allowed a bad actor to gain access to the water plant at Oldsmar, Florida. He attempted to increase certain chemicals to toxic levels that would have poisoned the public. Due to password sharing and other poor cybersecurity practices, it was easy for him to gain entry and start making unauthorized changes using an HMI. Fortunately, a worker on duty noticed strange mouse movements on his screen and took action so that this disaster was averted.[3]

Cyber researchers investigated and reported that a malicious script set up a "watering hole" where attackers collected data for nearly two months. They observed the OS, CPU, browser, camera, microphone, and more. During this time, state and local government computers accessed the watering hole. They were also profiled by the hackers. The hackers were aiming to spread this attack throughout water plants throughout the USA.[4] This attack was not the first. A similar one occurred in Kansas in 2019.[5]

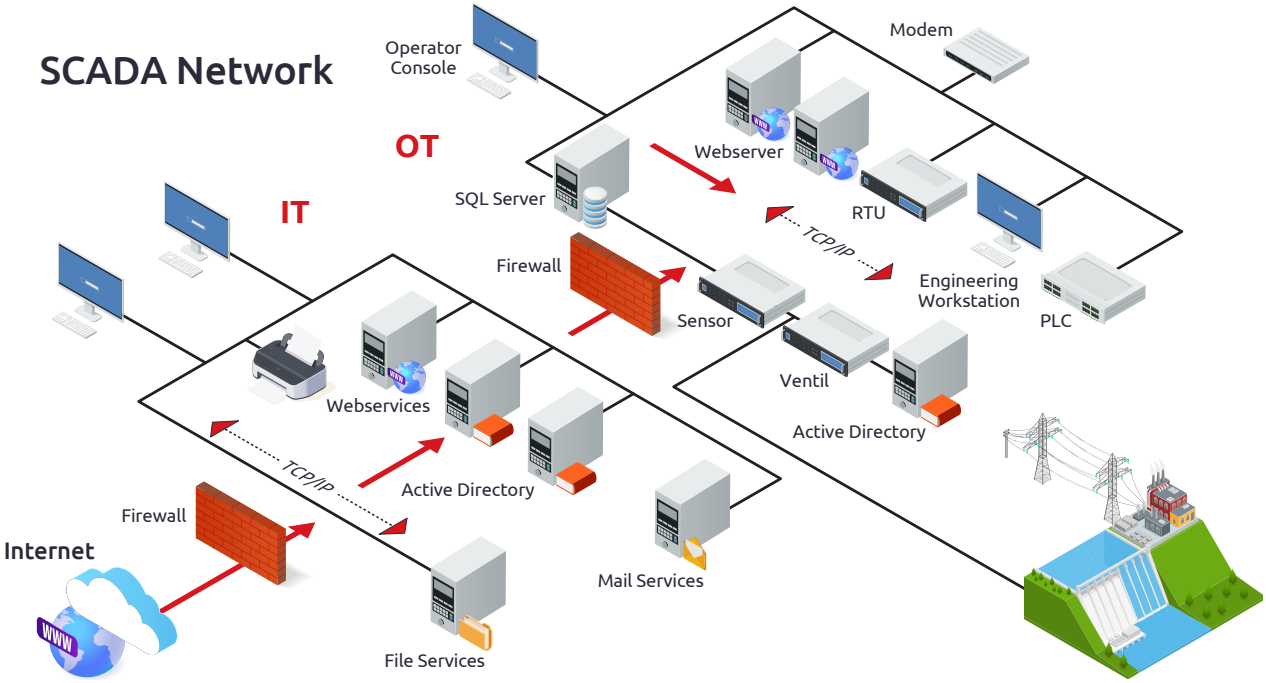
[3] *Josh Margolin and Ivan Pereira, "Outdated computer system exploited in Florida water treatment plant hack", abc News (2021), https://abcnews.go.com/US/outdated-computer-system-exploited-florida-water-treatment-plant/story?id=75805550 (access May 18, 2022).*

[4] *Eduard Kovacs, Probe Into Florida Water Plant Hack Led to Discovery of Watering Hole Attack, Security Week (2021) https://www.securityweek.com/probe-florida-water-plant-hack-led-discovery-watering-hole-attack (access May 21, 2022).*

[5] *Associated Press, Small Kansas Water Utility System Hacking Highlights Risks (2021) https://www.securityweek.com/small-kansas-water-utility-system-hacking-highlights-risks (accessed May 21, 2022).*

Smart Dams

The Salton Sea is a good example of why building and protecting dams is important. Early last century, engineers decided to irrigate crops in Southern California. They dug a gravity-feed canal from the Colorado river so water would flow downhill. They did not build a dam. The canal filled with silt. There was a heavy rain. With no dam to stop the flow of water, over 300 square miles of farmland was flooded. There was no way to move the water back into the river or to dig an outlet to the ocean. Over the years the Salton Sea has stagnated and become the largest and most polluted man-made lake in the world.



Not only do dams control flooding, they can also create water reservoirs for drinking water, irrigation, or industrial use. Technology inside the dam may generate hydroelectric power. OT zero trust can protect both legacy and modern dam systems.

Mining

While not specifically listed as a critical infrastructure sector, mining for metals, rare earth elements, and other substances is essential. OT zero trust supports ISA/IEC 62443 for control systems and other digitization and automation used in mining operations.

Global Perspectives on Critical Infrastructure

Taiwan

Taiwan's critical infrastructure, such as gas, water and electricity are highly digitized.[6]

In 2014, Guidelines for National Critical Infrastructure Security Protection were issued to regulate eight critical infrastructure sectors: Energy, Water Resources, Communications, Transportation, Banking and Finance, Emergency Relief and Hospitals, Central and Local Government Agencies, and High-Tech Parks.

CI protections have been developed for all these sectors. In 2018, the National Information Sharing and Analysis Center (N-ISAC) began operations. Information sharing through standardized formats and automated systems improves the immediacy, correctness, and integrity of information needed to reinforce the overall cybersecurity response and protection capabilities for Taiwan's critical infrastructure.[7]

India

The National Critical Information Infrastructure Protection Centre (NCIIPC) is an organization of the Government of India. NCIIPC has broadly identified the following as Critical Sectors:

- Power & Energy
- Banking, Financial Services & Insurance
- Telecom
- Transport
- Government
- Strategic & Public Enterprises
- Information Security[8]

[6] *Securing Taiwan Requires Immediate Unprecedented Cyber Action, (2021) https://www.lawfareblog.com/securing-taiwan-requires-immediate-unprecedented-cyber-action (access May 2022).*

[7] *NCCST, https://www.nccst.nat.gov.tw/NISAC?lang=en*

[8] *National Critical Information Infrastructure Protection Centre, https://en.wikipedia.org/wiki/National_Critical_Information_Infrastructure_Protection_Centre*

In Summary

This white paper focused on OT zero trust cyber defenses for buildings, manufacturing facilities, energy generation plants, financial systems, communications, IT, and transportation. It also addressed healthcare, food and agriculture, emergency systems, and water systems. The OT zero trust philosophy of basing trustworthiness on the current circumstance applies across all mission-critical cyber safety scenarios! It is a common sense approach that mitigates a real-world threat with a far-reaching potential for impact.

The OT zero trust portable security scanners were designed specifically to extend the life of valuable assets that have artificial, end-of-life restrictions because vendors no longer support security patches for them. They also protect devices that cannot connect to the internet to download virus signatures because of safety concerns or lack of capability. These portable security scanners are the OT zero trust CI's secret weapon because they are uniquely qualified to defend critical infrastructure against ransomware and other cyber attacks.

The entire suite of OT zero trust compliant security appliances from OT firewalls to IPSes to endpoint protectors work together to detect, prevent, and report malware continually to provide moment-by-moment situational awareness.

Never trust and always verify to keep the operation running.

txOne networks

txone.com