TECHTONICS ADVISORS

Marketing and Investor Content for Technology Companies

Securing Critical Infrastructure against Cyberattack

Gabriel Lowy

July, 2019

TECHTONICS ADVISORS

Marketing and Investor Content for Technology Companies

Securing Critical Infrastructure against Cyberattack

Table of Contents

Executive Summary

Converged infrastructure is only as valuable as it is secure. Attacks on critical infrastructure have grown in frequency and sophistication as bad actors, including nation states, seek to disrupt or disable essential services or to gather intelligence into strategic operations and planning.

The damages of a breach have been well documented. Billions of records have been compromised, costing an average of $148 per record, or $3.86 million per breach. These costs include regulatory fines, legal fees, and lost business due to downtime, remediation and reputational damage.

As more OT (operational technology) devices and industrial control systems (ICSs) are connected to IT (information technology) systems over the Internet, the attack surface expands exponentially. Attackers can use search tools such as Shodan to identify vulnerable devices, which when breached, can cause catastrophic loss.

This makes it imperative for OT and IT teams to work together to protect these assets and the trove of data they produce. ICS security systems need to be integrated with IT security if cybersecurity objectives are to be met.

Microsegmentation is a cybersecurity strategy to provide more granular protection in order to minimize an attacker's ability to compromise an entire network and wreak havoc with critical infrastructure. Host Identity Protocol (HIP) is a layered security approach to facilitate success with microsegmentation.

Traditional firewall and VPN solutions were not architected for Industrial Internet of Things (IIoT) initiatives. They were designed to protect against earlier generations of malware. As such, they are no match for the IIoT threat environment.

Securing this infrastructure requires a modern solution that can be implemented with relative ease, little to no disturbance to the operating environment, and at minimal cost, including headcount. When evaluating a solution for protecting converged infrastructure the key criteria for OT/IT teams to consider include the critical "ities" – availability, visibility, reliability, scalability, manageability and security.

Given the future growth of IIoT, demand is expected to shift towards purpose-built cybersecurity platforms that bridge OT and IT. Such platforms are better equipped to deal with the rising threats to critical infrastructure and the myriad of devices – up to 75 billion – that are projected to be connected to the Internet by 2025.

Will Catastrophic Loss Dive IT/OT Convergence?

- A cyberattacker intrudes a biomedical device at a hospital, and after exfiltrating sensitive patient data, takes the device – and all others it communicates with – offline, resulting in the death of numerous patients;

- The navigational system of a cargo ship is infiltrated by an attacker, who then takes control of the vessel with the intention of disrupting the supply chain and collecting ransomware – or using the ship for a terrorist or environmental attack;

- A pump and filtration system is compromised, enabling the attacker to disable plant safety and measurement systems that cripple operations and quality control, exposing millions of people to contamination.

These examples underscore the severity of risks to critical infrastructure, even as more companies seek to reap cost efficiencies and improved decision-making from their IIoT projects. Digitization transformation only accelerates the convergence of OT/IT infrastructures. In turn, this creates a new generation of high growth and ultra-permeable attack surfaces.

A Higher Purpose for Convergence

Smart buildings have no walls. They leverage pervasive wireless connectivity, sensors and IoT technologies to communicate and analyze data that is used to control and optimize building management and the ICSs within them. It is these same technologies that open vulnerabilities when building automation systems are linked with the Internet.

Interoperability among smart building elements is challenging enough. OT security was never designed to interoperate with data networks that ran the rest of the enterprise. The separation was deliberate. Now however, hackers launch successful attacks on industrial networks by exploiting connected sensors and gaining access to physical infrastructure.

Yet applying IT security to the OT environment can cause disruptions in equipment and devices. This can lead to self-inflicted denial-of-service attacks, as companies take facilities offline once elements in the system become inaccessible. In most environments it is untenable to do so; but for IIoT devices such as jet engines or hospital ventilators, it is impossible.

A Different Approach to Cybersecurity

Chief Information Security Officers (CISOs) and their OT and IT need to approach cybersecurity strategy from the perspective that they are already compromised. This vantage point enables them to prioritize the highest-value infrastructure assets that pose the greatest risk and danger if attacked.

A topography of systems assets and interrelations is a necessary first step. OT and IT teams are familiar with their own infrastructures and software. But each needs to have a fundamental understanding of the other's respective stacks, and how changes can impact both.

In the case of the OT teams, they have to learn the OSI model. In the case of the IT teams, it is the Purdue model. Deeper understanding of the interrelationships between layers in the stacks will enable converged teams to take a more holistic approach.

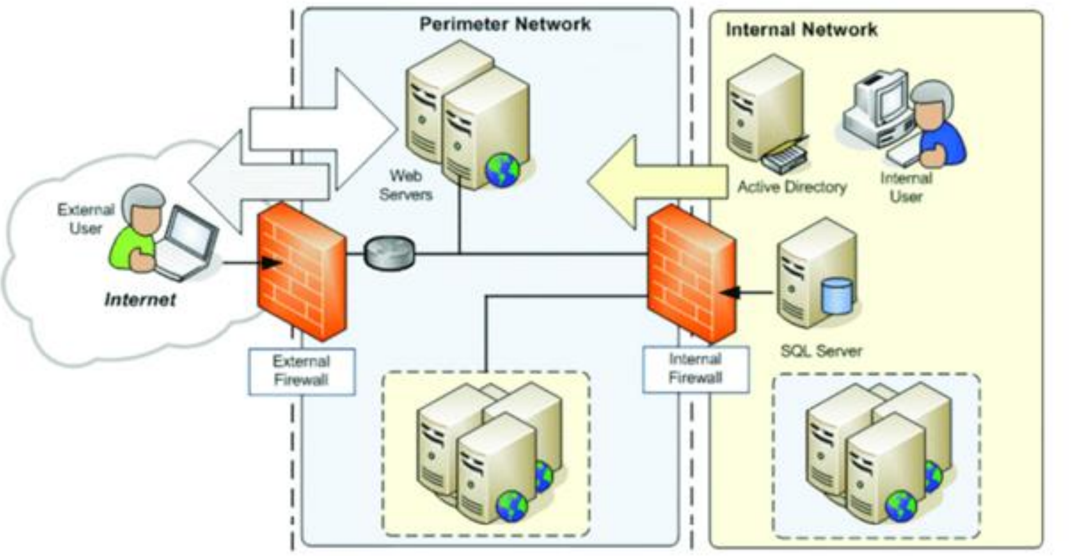
Granular Network Security with Microsegmentation and Host Identity Protocol

One of the most significant risks in a critical infrastructure breach is the potential for an attacker to not only compromise systems and exfiltrate data, but to take control over the physical infrastructure itself. This section explores microsegmentation as a strategy to provide more granular security in order to minimize an attacker's ability to compromise an entire network and wreak havoc with critical infrastructure. Host Identity Protocol (HIP) is a layered security approach to facilitate success with microsegmentation.

Microsegmentation for Greater Security

Network segmentation is a defense strategy to prevent an attacker from moving laterally within a network. This type of lateral movement is also known as east-west traffic.

The most basic form of segmentation is a host connected to the Internet with a firewall in between. The firewall is intended to protect the host from the Internet. This is commonly referred to as north-south traffic.



Source: Wikimedia

Security teams use VLANs and Layer 3 network interfaces to segment the network further. A firewall zone, or a DMZ, can also reduce the attack surface within a network.

But because there may be many hosts within a DMZ, none of these provide adequate security. First, the network allows all traffic to pass between VLANs. And since the Access Control Lists (ACLs) on routers differ from firewall rules, increased congestion and complexity can result.

East-west traffic bypasses firewalls and intrusion prevention systems (IPSs), which inspect and secure traffic coming into the data center in a north-south direction. If multiple hosts reside within a DMZ, an attacker can still move laterally if they've penetrated the zone.

Deploying firewalls – even virtual ones – at every interconnection point to inspect east-west traffic flows is expensive and adds to management headaches, including significantly increasing the number of alerts. And as more virtualized hosts become part of the infrastructure, not only does cost and complexity rise, but scalability can become an issue too.

Besides, hackers have learned how to circumvent firewalls to gain access to secure data, often using social engineering such as phishing to compromise a client and credentials. Once inside the internal network, the more east-west traffic they gain access to as the compromised host within a zone communicates with other hosts.

A more granular approach

Microsegmentation represents a more granular approach to preventing lateral movement between hosts. It allows secure communications policies to be configured down to the individual workload, virtual machine (VM) or network interface. Secure zones can be created around isolated workloads, with only necessary actions and connections permitted. Everything else is blocked, effectively limiting the attacker's ability to move laterally.

Moreover, these policies move with a VM or workload through migrations or network configuration changes. This ability to move makes the policies more persistent than with hardware-based firewalls, which restrict access based on IP addresses or other security policies.

Finally, microsegmentation delivers efficiencies. By defining granular security zones in software, it's easier to manage and scale than myriad access control lists, routing rules and firewall policies.

Host Identity Protocol (HIP): Built for IIoT Environments

HIP is one approach to successful microsegmentation. It was architected to address the networking and security requirements of IIoT environments.

HIP addresses the gap left by traditional security solutions that lack the functionality to mitigate modern cyberattacks. HIP only allows whitelisted communication between trusted endpoints that must mutually authenticate before a TCP session is established. This is all the more important in hybrid cloud environments, where persistence is critical as data moves over different networks and infrastructure.

Every device connected to the Internet has an address. This address provides two pieces of vital information about a device:

- The Domain Name System, or DNS, tells us which network the device is connected to (i.e. a government, corporate or personal home network);

- An IP address, which is a unique identifier for that device that tells other devices on the network how to communicate with it.

HIP provides a network layer alternative to using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for application security. HIP separates the role of host (device) identity and its physical location.

It replaces the unique IP address with a host identity (HI) namespace. This HI namespace is a cryptographic identifier, which is based on public key security infrastructure. It is most often self-generated by the device/host itself. Thus, the host, or device, can maintain its connection to the network, while its identity remains cloaked.

Since host identities are based on public key cryptography, they are computationally difficult to forge. As a result, HIP helps defend against DDOS, MiTM (man-in-the-middle) attacks, IP spoofing and other types of network and transport layer attacks. In essence, intruders cannot attack devices they cannot see.

HIP is easier to deploy and manage because it overlays the existing IT data network stack. It requires no configuration changes on the local devices it is protecting. It also enables host mobility and multihoming, or device/host connections to multiple networks.

Host mobility means that devices can be moved around a facility, such as biomedical equipment moves from patient to patient in a hospital. For devices that are sharing content with other remote devices and require quality connectivity with 100% uptime, multihoming enables each device to connect to several different networks, providing better resilience, redundancy, reliability and network utilization.

Criteria for Converged Infrastructure Cybersecurity

For OT teams that have largely operated free of data networks and rely on vendors for news about updates and vulnerabilities, cybersecurity is an unfamiliar, yet clear and present danger. Connecting OT devices to the IT network securely can overwhelm both teams due to the scalability and interoperability issues involved with connecting ICSs or smart building control systems (BCSs) to the IT network stack.

IIoT cybersecurity defense is beyond the scope of conventional IT security solutions, such as firewalls, intrusion prevention/detection, web gateways or endpoint/user anti-virus protection. And ICSs or BCSs were not designed for Internet connectivity, nor do OT teams have knowledge of IT security systems.

When evaluating a solution for protecting converged infrastructure the key criteria for OT/IT teams to consider include the critical "ities" – availability, visibility, reliability, scalability, manageability and security.

Availability (and Resilience)

Uptime is particularly critical for OT systems. Having visibility into devices and network provides the data to ensure availability. However, in the event of a cyberattack, OT systems, such as patient ventilators, purification and filtration devices, ship navigational systems, or jet engines simply cannot go down. A converged infrastructure solution must operate with the efficiency needed to facilitate uptime while protecting systems against cyberattack.

As part of an already-compromised approach to security strategy, resilience is more important for cybersecurity teams to quickly identify and respond to an attack to minimize the impact of risks. These risks include business interruption, intellectual property loss, private data theft, regulatory noncompliance, reputational damage, and physical plant and personal injury, including potential loss of life.

Visibility

Visibility consists of two components. First, teams must have visibility into the devices – both OT and IT – that are connected to the network. Knowing who your users are, including those users that are machines, drives policies and authentication rules about which “users” can access which systems.

Once users are identified, verified and authenticated, companies need visibility into the traffic flowing across their environments, including private and public clouds, and what users are doing with the systems and data they are authorized to work with. Modern self-healing IT solutions increasingly automate monitoring by leveraging AI, machine learning and real-time analytics technologies to ensure application performance and user experience.

Reliability

In the IT world, “five nines” reliability has been a required criteria in telecommunications networks for decades. In more recent years, this level of reliability has spread to e-commerce, video streaming and other applications where customer satisfaction and loyalty correlate to user experience.

While providing different “services”, OT systems have been built for reliability that extends to life-or-death situations. Protecting the expanded attack surface of converged infrastructure without sacrificing reliability is a key criterion for a converged infrastructure solution. Such a solution must cut across different operating environments and protocols subtly and without the disruption or a performance tax.

Scalability

Converging OT and IT systems implies scale. The reason for doing it is to realize cost efficiencies and improved decision outcomes by harnessing more data inputs from more sources. However, as we've seen in the IT world, scalability also often applies to costs. IT teams struggle to reconcile a do-more-with-less budgeting process with the mandates of meeting SLAs and GRC (governance, regulatory, compliance) and security requirements.

OT teams operate in a more cloistered environment that to date, has mostly escaped the scalability requirements and challenges faced by their IT counterparts. OT teams don't think about cloud, data centers, Internet transmission challenges, interfacing with business critical IT applications or user experience on a global scale. Meeting the cybersecurity demands of a scaled and converged OT/IT infrastructure is another top priority of a converged infrastructure solution.

Manageability

Each of the criteria above should come with key performance indicators (KPIs). KPIs provide the means to measure infrastructure performance against organizational objectives and quickly identify and remediate deviations from benchmarks. As network complexity continues to grow – especially as OT devices are added to the IT network – teams must deploy modern technologies that enable KPIs to inform processes.

An overlay cybersecurity solution for converged systems must be easy to manage, predicated on the ability to interface with both OT and IT management systems. But manageability also includes people. To effective ensure efficiency, safety and security of high-leverage infrastructure, OT and IT teams need to establish an environment based on communication, collaboration and trust, with clearly defined roles and responsibilities. This ensures agility and resilience for faster response times in the event of an attack.

Security

While IIoT initiatives are intended to advance business objectives, the principal objective of a cybersecurity solution is to protect critical infrastructure against catastrophic loss. Connecting more OT devices to the IT network significantly expands the attack surface, raising the stakes for OT/IT teams to an unprecedented level. OT and IT teams need to be versed in their respective stacks to better understand architectures and cybersecurity requirements.

AI-driven systems can teach machine users resilience. However, human users – the weakest link in the cyber kill chain – need training on techniques and policies for safe and secure operations. With a cohesive converged cybersecurity strategy, OT and IT teams can be instrumental in helping companies achieve the promise of IIoT.

Implications for Legacy Firewalls and Segmentation

IIoT cybersecurity is beyond the scope of traditional firewall and VPN solutions which struggle to keep up with the scale and variety of modern attacks.

These tools have many drawbacks:

- They are impossible to keep current, overwhelmed by the frequency, variety and scale of IIoT cyberattacks.
- They require time-consuming manual efforts, including writing custom scripts, configuration and implementing policies on physical devices.
- They come with a high performance overhead, making them inefficient and costly to maintain.
- They are error prone, and generate so many false positive alerts that beleaguered administrators either configure them to catch only the most basic known malware or ignore the alerts altogether.
- They increase risk exposure by allowing intruders to operate undetected and undeterred for long periods of time.

Due to these shortcomings, we've already seen a shift in consumption away from deploying and managing devices toward subscription-based models. This trend will continue as security teams seek to reduce hardware sprawl and complexity.

However, even as a subscription, these tools will still not provide adequate defense against IIoT attacks. Vendors may try to add functionality through bolt-on acquisitions or internal development. But as we've seen time and again in this industry, the usual outcome is a patchwork quilt of solutions that are not seamlessly integrated, causing more headaches for customers. As such, the market for legacy firewall segmentation solutions is expected to gradually slow and then decline over the next 5-7 years.

Given the future growth of IIoT, demand is expected to shift towards purpose-built cybersecurity platforms that bridge OT and IT. Such platforms are better equipped to deal with the rising threats to critical infrastructure and the myriad of devices that will be connected to the Internet. Over time, as firewall segmentation technologies further commoditize, that functionality may even be subsumed by these next-generation IIoT cybersecurity platforms.

Cybersecurity strategy for both OT and IT teams needs to evolve. OT/IT convergence facilitates a stronger cybersecurity posture for the entire enterprise. A different strategic approach that moves away from legacy thinking and technologies allows CISOs and their teams to deploy modern solutions that have been architected to specifically address the challenges of attacks in growing IIoT environments.

About the Author

Gabriel Lowy is founder of TechTonics Advisors, an independent technology research and writing firm with an expertise in network infrastructure, software and security. His unique capability is bridging the languages of technology and Wall Street by connecting the dots between vision, strategy, portfolio and markets. Gabe was an award-winning technology analyst for over 15 years with several Wall Street firms. Previously, he was with Andersen Consulting. Gabe has published over 1,400 reports and articles about the industry and specific companies. He holds a B.S. in Marketing and an MBA in Strategy, both from the Stern School of Business at New York University.