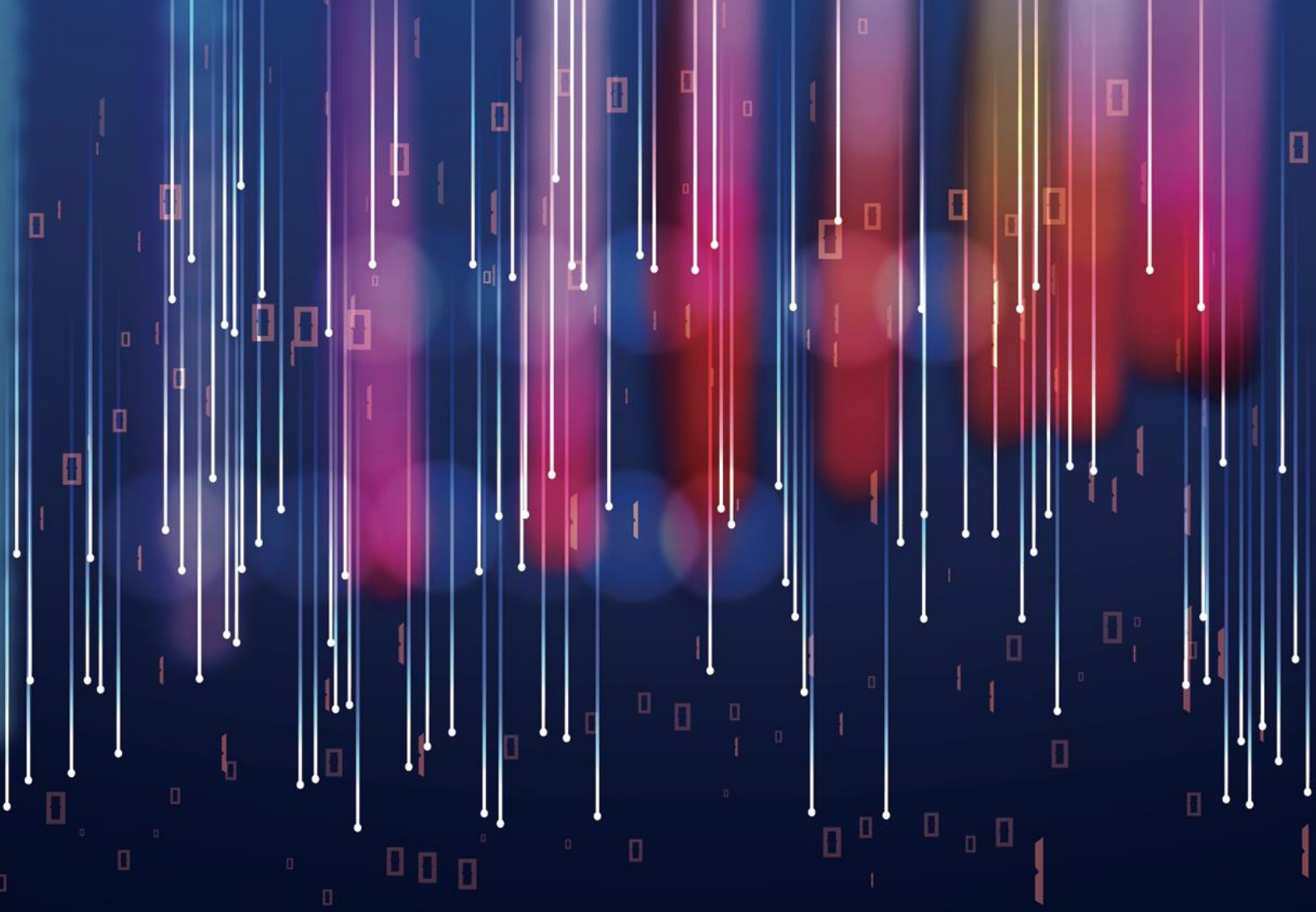


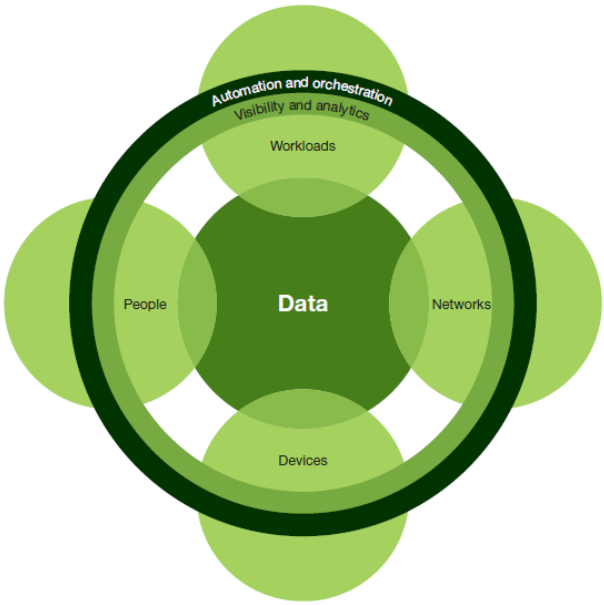
What is Clinical Zero Trust?

January 2021

MEDIGATE

What is Zero Trust?

Zero Trust is a term that was first coined 10 years ago by then Forrester analyst John Kindevarg as a new concept in computer networking. The concept began as a “trust nothing, verify everything” principle, but has since evolved into a comprehensive cybersecurity philosophy. Today, Zero Trust represents a networking approach that centers the design and implementation of IT networks around the identity and access rights of users and data.



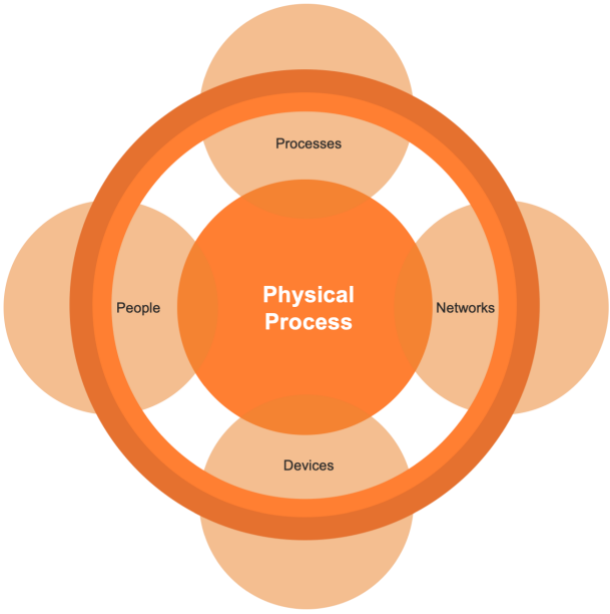
What Zero Trust is Not

Most technology vendors have adopted Zero Trust as a product marketing strategy, feeding the hype and promising a Zero Trust nirvana. The reality is that there is no such thing as a Zero Trust company or Zero Trust product. This is because Zero Trust is a strategy, not a technology; it’s an end goal, not a feature or capability. No firewall, NAC, end-point security solution, or micro-segmentation product is by itself a Zero Trust solution, rather these offerings help you create a Zero Trust environment. It is notable that technologies that can be used to enable a Zero Trust stance, can just as easily be misconfigured or misused to violate Zero Trust. That’s why it’s important to think of Zero Trust as a philosophy and approach, not a solution, so you can be vigilant about all the technologies you are using to implement a Zero Trust stance.

What is Clinical Zero Trust?

Clinical Zero Trust (CZT) applies a Zero Trust philosophy to the cyber and physical environments of healthcare organizations, also known as a health system’s clinical settings. Just like traditional Zero Trust, there is no specific product required or not required to build a proper CTZ environment. The key difference between traditional Zero Trust approaches and CZT is that CZT shifts the focus from protecting devices and data to protecting physical workflows, which are made up of the people and processes involved in delivering care, at the “end of the wire.”

Why Clinical Zero Trust



In healthcare organizations the stakes are high; underscoring the importance of ensuring patient safety and protecting personal health information (PHI). Traditional Zero Trust strategies architect the IT network, which makes up a health system's back office operations, to protect much of the health system's financial and PHI records. There are a number of technical resources you can easily locate to see how to protect these IT networks; you may want to start with Forrester's "Zero Trust Security Playbook for 2020," if you have not already.

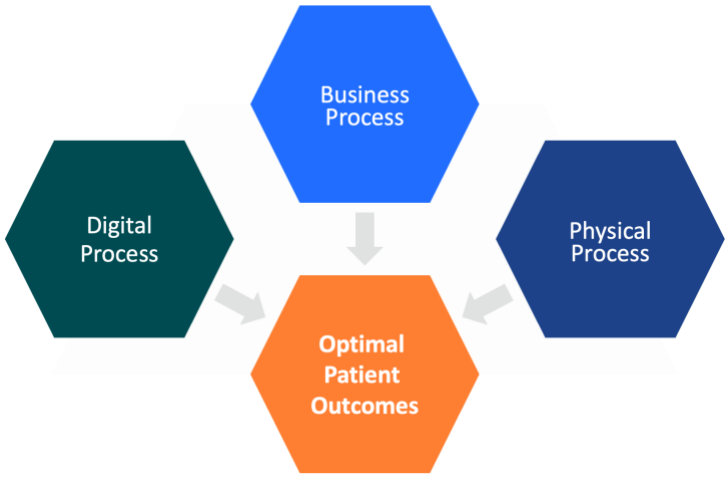
The clinical settings, however, where care is actually delivered, are more difficult to protect because you can't do anything that may block communications or disrupt care. In addition, access to resources can't be tied to a user's identity, which is how traditional Zero Trust implementations are architected (e.g., to control whether or not a user can access a particular resource or data). With medical, IoMT, and IoT devices there is no user attached or logged into it from a digital perspective, even if there is a person physically attached to it (e.g., patient monitor or IV pump).

To further complicate matters, these devices typically can't have an endpoint agent installed, which can make it challenging to get the visibility and granular enforcement needed to protect the environment it is being used in. Plus, these devices are highly mobile, as they are constantly moved, deployed, reclaimed, and redeployed, as needed, adding to the complexity associated with keeping security current. All of these reasons make it extremely important to develop and implement a Zero Trust strategy that can handle the specific requirements of the clinical setting—only Clinical Zero Trust can be applied to protect the clinical network.

What Does Clinical Zero Trust Involve?

The core mechanics of Zero Trust's "never trust, always verify" is still in play with CZT, unfortunately, it is often associated with a purely micro-segmentation implementation. Given the challenges associated with the clinical setting that we've already described, this can be a disaster for cyber physical settings, as this miopic approach seldom takes into account the physical reality of how care is delivered. At its core, CZT is about protecting the physical process, not the specific devices or data involved in that process, sometimes referred to as the care protocol.

This means the protected surface extends to the physical world, including everything associated with administering a procedure or delivering care. At first glance, it seems like an impossible task to protect physical things with cyber technologies, but in reality, when you look at the clinical setting holistically it makes it easier to identify interdependencies and develop strategies that will effectively protect the physical, business and digital processes to drive optimal patient outcomes.



Biomed and clinical engineering teams already function this way, building care protocols that can be executed daily to provide a prescriptive outcome. If you can shift security to think in these terms, it can help you decide when, where, and how to handle protecting the clinical setting. This paper describes a process (five phases), which is hopefully familiar, that can be used to start to implement CZT in a way that will keep patients and the business safe.

How to Begin with Clinical Zero Trust?

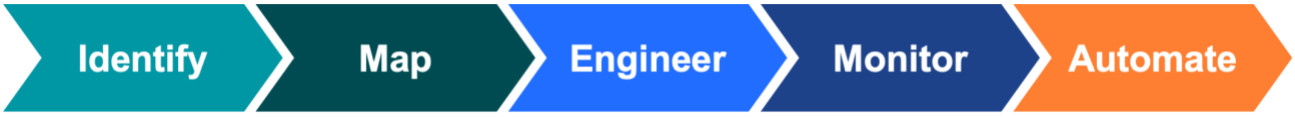
If you do not already have buy in within your organization around traditional Zero Trust, you can start here with the excellent resources that Forrester has to help you sell the strategy upstream.

Given the expansiveness of CZT, you are going to need to get buy in and support from many stakeholders. You cannot approach biomed with the notion of applying more cyber controls to their environment without complete cooperation—the knowledge they possess and the relationships they have with device vendors can make or break your project. Sometimes, getting clinical engineers to the table can be a challenge, papers like this one can help.

You will also need to approach your leadership team, from your CISO and beyond, to help them understand how applying Clinical Zero Trust will help the business, not just from a cybersecurity angle, but also from a bottom-line perspective, as the knowledge required for CZT can improve capital asset planning and management.

The phases of Clinical Zero Trust implementation and roll out are the same as Zero Trust, only the actions and specifics are altered due to the environment and focus.

The Five Phases:



Step 1: Identify

Once you have identified and gained the support of your biomed teams and executive leadership, the next step is to gain the deepest understanding of your clinical environment. For this, you need a discovery tool that identifies connected devices and provides details such as:

- Modality (i.e., type, make, model)
- Version (i.e., OS type and version)
- Unique Identifiers (i.e., serial number, hostname, MAC address)
- Location (i.e., SSID, Access Point, AP location)
- Utilization (i.e., Average usage, daily usage, etc.)

In addition, you need to be able to scan for vulnerabilities, using either a stand-alone solution or integrated capabilities, understand healthcare specific threat intel, like H-ISAC, and incorporate information from automatic recall feeds, like those issued from and linked to the device makers in your environment.

It is important to have the ability to accurately measure and score the risks posed by each medical, IoMT, and IoT device. The risk scoring absolutely must include criticality information, based in part on the FDA's guide on the impact to human life if a machine is damaged or somehow compromised.

Ultimately, you want to be able to assign devices to groups or individuals for ticketing, scheduled maintenance, prioritized mitigations, etc. You may consider integrating with your operational systems, such as your CMMS, to ensure everyone is working off of the same data and insights.

Step 2: Map

Granular visibility is only the start. Next, you must map the use of the device to understand which care and business protocols it is a part of, which can be tricky.

First, it takes understanding all the cyber flows: What does the device talk to, how, when, and why. Your chosen tool should really help here, but not all tools are alike; some provide purely machine learning and anecdotal evidence (e.g., only what's observed), while others invest in relationships with manufacturers and research teams, who are constantly developing their understanding of how these devices actually work, including their communications patterns and accepted use scenarios.

The second, slightly more tricky part, is understanding the physical flows of these devices: Where can, could, and should a device go. For example, an MRI machine is easy because it is pretty hard to move, but a crash cart poses more challenges. If it is quickly moved down the hall, from one patient to another, its security profile needs to follow it, in real time. Or imagine a patient monitor linked to a critical case patient moving through the ER at a rapid pace.

Mapping the cyber and physical flows is absolutely critical to support the next phase of engineering a Clinical Zero Trust architecture.

Step 3: Engineer

Healthcare Cyber Physical Systems (CPS) are deterministic in nature. That means, unlike users, a device works the same way, following the same communications paths and operating in predictable ways every day. Even patching rarely affects device behaviors (FDA certification assures this). The only variance is actually the physical path or area of use when a device is moved, sold, or decommissioned.

This level of certainty allows the environment to be engineered, via policy and process, to comply with appropriate physical use and mitigate cyber risks. Ideally your discovery and visibility tool could provide recommendations and clinically vetted insights that help you create policies. In addition, it could allow you to simulate or 'try out' policies, so you can monitor their impact before enforcing them.

In terms of enforcing those policies, the implementation will really depend on the environment and may even change from one clinical setting to the next. For instance, if you have broad open areas of clinical practice, where devices are moved about constantly, hectically, then a NAC augmented by an insight platform might be a good choice, as east—west firewalls are often too cumbersome to manage fast moving changes.

Firewalls are often best suited to enforce border control policies between core functions and back office systems, user spaces, or even, to some degree, control stations. However, it is critical to note that even in border control, not all firewalls are suited to protect all the applications and protocols within clinical networks. A true clinical firewall must be aware of the more than 150 medical protocols that might be found within a healthcare delivery organization. If it's not aware of the protocols you're trying to control, it doesn't have the context it needs to precisely enforce policies and could end up doing more harm than good.

Step 4: Monitor

The next phase is to monitor the environment to fully understand the impact of the policies you plan to enforce. As stated before, if you have an insight tool that allows you to trial policies this step is much more simple; if not, you have to rely on your infrastructure choices to do this for you. Luckily, most modern security products have a “monitor” mode. Once you are comfortable with the policies you have architected, you can move to enforcement mode.

At that point, this phase becomes the constant monitoring and improvement of your internal security processes. You are looking for failures of necessary communications, improper design, and other glitches, in addition to the perennial cyber threats that are targeting your organization. With all that’s at stake, it’s important to get it right.

Step 5: Automate

Once you are confident that you have engineered the proper architecture, verified the run state, via monitoring, and made whatever necessary changes are applicable, you are ready to go to the last phase, which is to automate. This phase allows you to apply cyber controls to your care protocols and processes, via your enforcement points, and start to reap the benefits of a Clinical Zero Trust environment.

What are the Benefits of Clinical Zero Trust?

Imagine a world where the next malware targeted at healthcare, like Ryuk, arrives and it gives you little to nothing to worry about. Now, imagine knowing exactly what devices you have in your environment, down to their version, location, utilization, and vulnerabilities/cyber security risks they pose. Then consider what it would be like if you were proactively informed of recalls, automatically alerted about new cyber risks, or better yet had those risks automatically mitigated. These can be just a few of the benefits that a CZT architecture can deliver.

It may seem fanciful to think a cybersecurity philosophy could provide device location, utilization, version or other inventory data, but these insights are a critical part of CZT. As you know, you cannot protect what you cannot see, and to do CZT it takes more than visibility. You must have clinical context, as well as actionable insights that allow you to perform functions and controls upon physical devices with confidence. When accomplished, however, this level of understanding provides both massive security and operational benefits for organizations who can harvest them.

The Outcome

A properly implemented Clinical Zero Trust network environment offers both cyber and physical resiliency. CZT takes into account the complexities and clinical context of the digital, business, and physical processes involved in the delivery of care to ensure optimal patient outcomes.

It ensures everyone is best equipped to effectively architect the network to implement safe, repeatable security measures that improve the operational efficiency and value-based business interests of your organization. It balances risk across functionality and availability, ensuring technologies can “protect to enable” the business, rather than blindly adhering to a strict security rubric that could do more damage than good.

With CZT, you can deliver operational impact, providing valuable data and insights into inventory, utilization, and risks, as well as clinically-vetted policy implementations to support the security and business objectives of your health system. Indeed, a properly executed Clinical Zero Trust strategy is a core component of a Real Time Health Strategy.

About Medigate

Medigate provides award-winning cybersecurity for connected devices in hospitals. The platform combines a deep understanding of manufacturers' protocols and clinical workflows with cybersecurity expertise to deliver comprehensive and accurate identification, contextual anomaly detection, and clinical policy enforcement. The resulting automated, rule-based clinically-driven security policies keep patients, networks, and PHI safe.

MEDIGATE

Get in touch

Email: **contact@medigate.io**

Visit: **medigate.io**