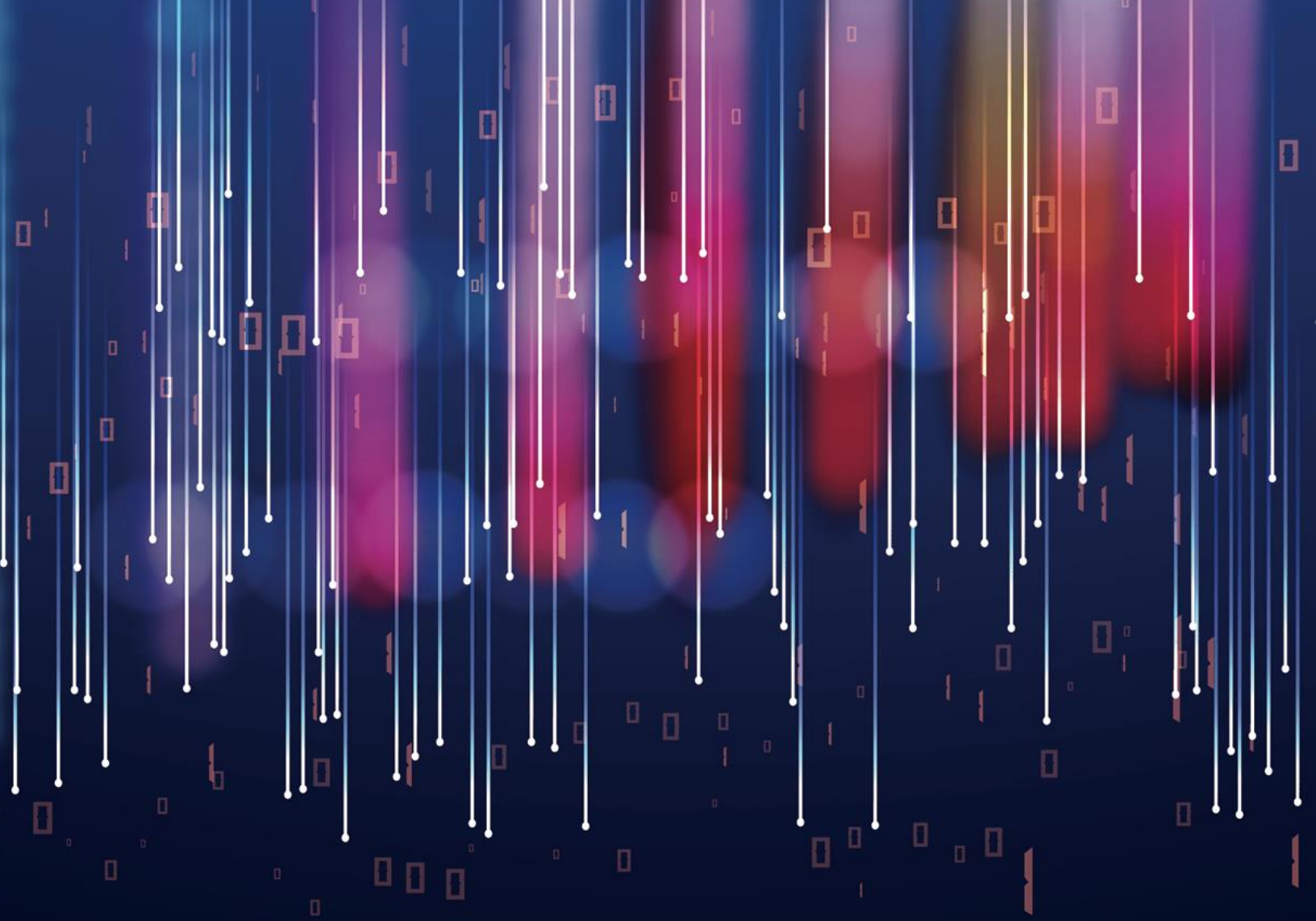

The 5 Benefits of a Zero Trust Strategy for Biomed Engineers

January 2021

MEDIGATE

Executive Summary

“Trust nothing, verify everything,” which is the Zero Trust model, can garner a lot of benefits if applied correctly as a strategy by healthcare organizations. Unfortunately, security teams often look to implement it prescriptively, applying a perimeter around each and every entity to try to tightly restrict access to only what is necessary. In healthcare organizations, this can be extremely problematic, even dangerous.

People and devices in a hospital or clinical setting are constantly moving, sometimes even rushing down halls and floors in the course of delivering care. If access to a ventilator is blocked or an IV pump is prevented from communicating with a patient monitor, simply because it has been moved or just powered up, the consequences can be critical. Within healthcare, Zero Trust is not about protecting each device, but rather each protocol. It is not about protecting things, but rather the process that the things are involved in.

What this means is that security teams can’t work in isolation. To effectively protect the clinical network, they need the input of clinicians and biomedical engineers, who understand the physical and digital workflows associated with administering patient care. And clinicians and biomed professionals should want to be involved in setting the strategy to ensure that access and availability to the devices and settings that provide care are never interrupted.

When applied correctly, a Zero Trust strategy can garner a ton of benefits for both security and biomed teams. Improved visibility and operational efficiencies are just a few. This paper looks at how security and biomed professionals within healthcare delivery organizations need to start thinking about Zero Trust and the benefits they can reap when they get it right.

The Business of Healthcare Needs a Different Approach to Security

The cost of security incidents in healthcare are well known—data breaches cost the healthcare sector $6.5 million on average, according to the most recent IBM-sponsored Ponemon Institute report. Due to the wealth of personal, medical, and financial information stored and flowing through health systems, there is no reason to believe that attackers are going to stop targeting healthcare organizations anytime soon.

In fact, it appears attackers are doubling down on their efforts. 2020 saw a rising wave of attacks on the healthcare sector, so much so that the Cybersecurity and Infrastructure Security Agency, the Department of Health and Human Services and the FBI issued a joint advisory stating there is "credible information of an increased and imminent cybercrime threat" to hospitals and healthcare providers.

What this means is that health systems are going to need to ramp up their own defensive efforts and potentially take more drastic measures to try to protect the privacy of their data and the integrity of the operations and patient care. Security as usual is simply not an option.

The Promise of Zero Trust – Why Biomed Needs to be Involved

A lot of organizations are hoping the answer to many of their security problems lies in Zero Trust. The concept is to 'never trust, always verify.' This goes for anything and everything in the IT infrastructure, from users and devices to connections and transactions. It makes sense that if you verify everything, you can ensure nothing happens that shouldn't, but, in practicality, it is problematic for healthcare organizations.

In health systems, it may mean that cybersecurity is being inserted into processes (between endpoints and medical devices) that can't afford any disruption. If access to a ventilator is blocked or an IV pump is prevented from communicating with a patient monitor, simply because it was moved, powered up, or made a new connection, an unnecessary point of failure has just been introduced that can have serious, even life-and-death, consequences. Put simply, we don't want cybersecurity to become a "Sword of Damocles" hovering above the clinical network.

In fact, good security practices should reduce risks, not introduce them. What this means is that clinicians and biomedical engineers are going to have to get involved to ensure any Zero Trust strategies being considered by their health system take into account the clinical context of all the devices in the environment. They are going to have to help their cybersecurity teams understand what they are really protecting—good care for patients, not just access to devices.

What Zero Trust Looks Like in Healthcare

Within healthcare organizations, Zero Trust needs to be recalibrated to protect each care protocol, instead of each device. The surface that needs to be protected must expand beyond any one device to include the processes and procedures within each service line that the device (or set of devices) is involved in. This takes looking at both the physical and digital flows of processes and procedures to understand exactly what is involved and what needs to be protected.

Healthcare services lines are a compendium of care protocols that rely on different staff, devices and systems. They may exclude independently, in well-established sequences, interdependently, or on ad hoc basis, based on patient responses to treatment. The point is, cybersecurity provisioning must be scoped in this context so that it can facilitate and protect care, not restrict it.

For each device in the environment, questions like, “what does that device do?”, “how is it connected?”, “what information does it share?”, “what other devices does it communicate with?”, etc. must be asked and answered. These questions are designed to identify and enable the smallest area of uninterruptible protection (within the care protocol) before a security control point can even be considered. In other words, the care protocol’s integrity and flow must be preserved.

If it is broken, it could impact patient outcomes. For instance, if communication between a BD Alaris pump and the System Manager is broken or blocked, it could impact the continuity of care and adversely affect the health and recovery of the patient. Other items, a disruption to the care protocol could have consequences to the business of the hospital. For example, if communication is lost between the different devices used to administer care and the hospital’s EMR, charge master, billing system, etc., the hospital will not be reimbursed for those services.

In summary, the care protocols are defined and hopefully, continuously improved. Cybersecurity should be a facilitator and implemented in a sensible way that is not only sensitive to the needs of staff and patients, but to the business as well. It requires a shift in mindset. From thinking about the security of devices to the security of processes. When Zero Trust is done right, it’s a strategy that pays dividends, both in terms of value based patient outcomes and operational efficiency.

Top 5 Benefits of a Zero Trust Strategy that Protects the Care Protocols of Hospitals

When done right, based on protecting the care protocols of hospitals rather than each and every device, hospitals can generate a number of benefits that support the needs of both the cybersecurity and biomed teams. The following are the top five:

1. Better Visibility

The ongoing implementation of a Zero Trust strategy is predicated on detailed, real-time inventories of all the devices and network communications within the IT environment. Ultimately, this visibility leads to better management and security for all the hospital's assets.

Details on the makes, models, serial numbers, communication protocols, embedded software versions, as well as location utilization of the devices can be used to make data-driven decisions that improve the efficiency of the hospital's operations. Vulnerabilities and indicators of compromise (IoC) are easier to map to the inventories of health systems, allowing teams to be more efficient and effective in their patching and vulnerability management plans and protocols.

Insights into how devices are being used and the frequency of that utilization can improve procurement, maintenance, and end-of-life planning and decisions. Updates can be scheduled, according to usage, and devices can be deployed to where they are needed most to optimize the life and value of the hospital's asset and capital investments.

2. Improved Collaboration and Orchestration

Biomed cannot protect the care protocols without security, and visa-versa. By implementing a Zero Trust strategy, these departments can work as a team, as they're finally talking the same language and sharing the same objective—protecting patients.

Interdepartmental silos can be broken down and real, productive working relationships between teams can be forged. Plans and decisions around patching, maintenance, product recalls, etc., can be discussed within the parameters of the care protocol to ensure all sides understand the implications of the change and ensure it doesn't have an adverse impact on security or operations.

3. Value-Based Care

Connected medicine is critical to value-based care delivery aimed to reduce costs, while improving patients outcomes. Although fee-for-service isn't dead, alternative payment models (APMs) are defining a new era of reimbursement that clearly assumes networked care delivery, which is evident in the explosion in spending on IoMT, telemedicine and Remote Patient Monitoring (RPM). In this context, Zero Trust can be an enabler.

When developing a Zero Trust strategy, health systems can engineer their care delivery networks to maximize the robustness and agility of their service delivery. This means that new device onboarding and device-dependent service provisioning should be defined by security-ready processes. The network should take care of security—not the device, nor the biomed professional charged with maintaining that device, and certainly not the clinical engineers and physicians who are collectively charged with using it to provide the networked care.

4. Attack Mitigation

The whole point of implementing a Zero Trust strategy is to improve the health system's security stance. By implementing control points to protect the care protocols, the environment is inherently more resilient and more impervious to attacks. Successful attacks will be discovered and prevented from propagating, which greatly limits an incident's damage potential.

Sensitive information, such as personally identifiable information (PII), electronic medical records (EMRs), and financial data within health systems is protected, as exfiltration is stopped at the demarcation of the care protocol. This keeps health systems and patients from the emotional and financial toll that a data breach can take.

5. Efficiencies

In defining the care protocols, hospitals are forced to take a good hard look at what they are doing and how they are operating. It is highly likely that inefficiencies and opportunities for improvement will be uncovered that can lead to advances in how the hospital runs and the quality of care. Chances to consolidate multiple, disparate systems and controls can lead to streamlined operations and reduced management costs.

By its nature, a Zero Trust strategy can help reduce the effort and scope associated with compliance initiatives. Protect surfaces are identified and rationalized, thereby increasing the health system's ability to pinpoint where sensitive, regulated data and processes are. This can ease the traditional pain of compliance audits and reduce the overall effort.

Conclusion

The CISO of a major US hospital asked: "How can I implement a security policy for a connected medical device when I don't manage or control it? All I know is I have a big black hole in my network. I have knife-wielding robots, radiation, nuclear, and drug dispensers, all on my network—high-powered stuff that I own but don't manage." The short answer to this CISO would be to implement Zero Trust as an enabling strategy. Only then will the underlying investments they have made generate long term benefits.

The long answer is to implement a Zero Trust strategy that takes account of the complexities and clinical context of each protected surface area. That means care protocols, not just devices, and that requires the inputs of those charged with each and every aspect of delivery. Together, they are best equipped to inform an enlightened, repeatable approach that not only ensures efficient operations and effective delivery of patient care, but supports the value-based business interests of financial leadership.

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

Email: **contact@medigate.io**
Visit: **medigate.io**