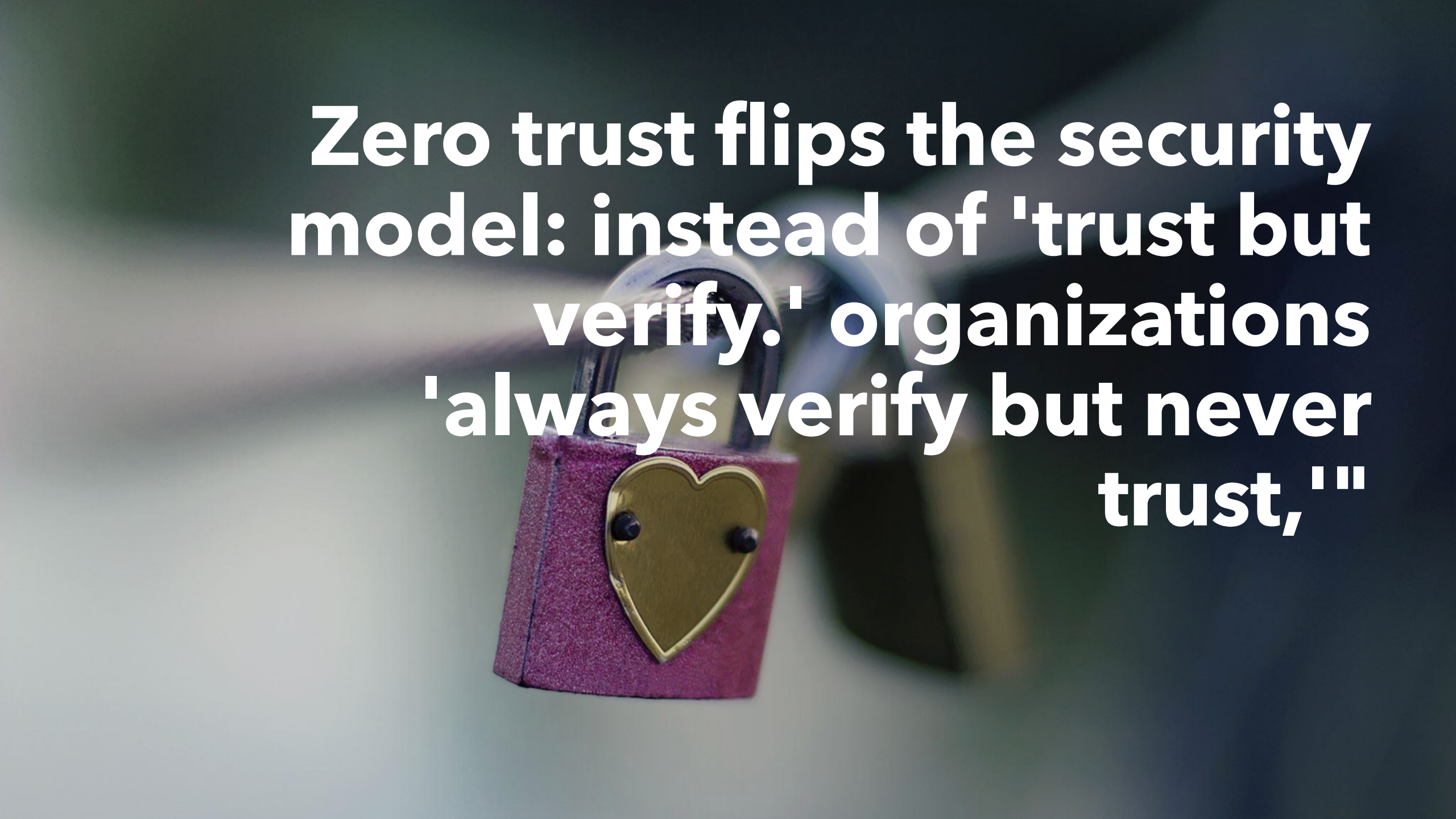
Zero Trust for Healthcare

Veronica Schmitt

WHOAMI

- Assistant Professor : Noroff University College (Norway)
- Director : DFIR LABS (South Africa)
- Independent Security Engineer : Medtronic CHRF USA
- Lethal Forensicator
- Hacker
- Cyborg


Zero trust flips the security model: instead of 'trust but verify.' organizations 'always verify but never trust,'"

- “It is essential to know that no single specific technology is associated with Zero Trust architecture. The Zero Trust is a security model based on the principle of maintaining strict access controls and not trusting anyone by default; a holistic approach to network security, that incorporates a number of different principles and technologies.”
  — **Ludmila Morozova-Buss**

If your users are accessing more IT services outside the security perimeter than inside, how protective can the perimeter really be?

Why Healthcare is a target?

- Hospitals and medical centers tend to privilege one key attribute in IT: access.
- At any one time, patient data, medical records, schedules, email and everything else is flying from one part of an organisation to the other.
- And in this environment, it matters even more, because the speed at which a medical professional can get access to that information could impinge directly on the health and safety of a patient.
- And because the health sector was largely disconnected from the wider online world, we could rely on that attribute.

- There are plenty of disciplines and fields undergoing similar transformations. With the rise of the Internet of Things (IoT) – industries which once only had to worry about IT doing its job effectively are now being forced to change their perspective.
- Take critical infrastructure – there are plenty of energy facilities that were designed to protect against failures and accidents but never attacks. In fairness, they never had to – many such facilities were completely air gapped from the outside world and for a long time, their primary concern was whether the computers could do their job and whether there were appropriate physical security controls in place.

Now, Digital Transformation is forcing those devices to connect to a world that is riddled with threats and cybercriminals looking to make their fortune or just cause disruption.

Medicine is not just being forced to reckon with the cyberthreats that so long laid off but are also on the verge of their own digital revolution which promises to transform the state of medical technology – but if handled poorly could spell disaster.

IoT has found a rich vein in medicine. And everything from insulin pens to cancer monitoring systems to inhalers to ingestible sensors to contact lenses will soon be connected into great glimmering endpoint-ridden medical networks – providing better information to healthcare providers and improving patient care. That is, if they can secure them.

Introducing IoT-enabled devices into an already lucratively insecure environment merely increases the attack surface and provides creative new ways to make money.

Perimeter Based Security

- Digital transformation has made the traditional perimeter-based network defense obsolete.
- Hospitals need to be able to move with agility, adapting quickly to changing market conditions and take advantage of new opportunities.
- As organizations drive their digital transformation efforts, it quickly becomes clear that the approach to securing the enterprise needs to be adapted to the new reality.
- he security perimeter is no longer just around the on-premises network.

Perimeter Based Security

- It now extends to SaaS applications used for healthcare critical workloads, internal systems and supply chain networks your employees are using to access resources while attending to patients needs.
- Inter-connected healthcare has become a big topic since Covid-19 reared its ugly head.
- We were forced to break down the perimeter and smash the norms.
- The traditional perimeter-based security model is no longer enough.

Perimeter Based Security

- The traditional firewall (VPN security model) assumed you could establish a strong perimeter, and then trust that activities within that perimeter were “safe.”
- The problem is today’s digital estates typically consist of services and endpoints managed by public cloud providers, devices owned by medical manufacturers, partners, and customers, and web-enabled smart devices that the traditional perimeter-based model was never built to protect.
- We can’t assume there are “threat free” environments.

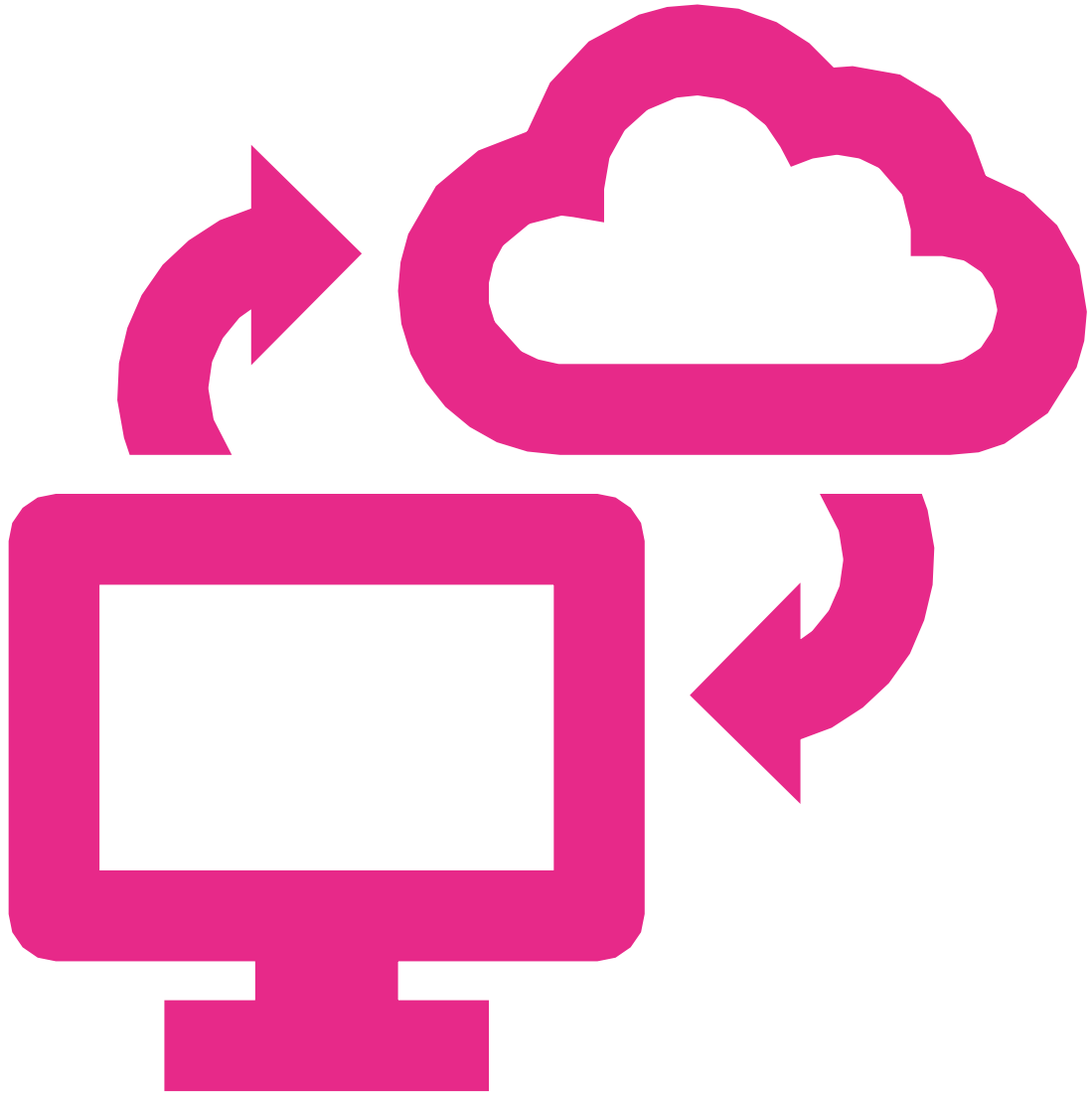
The Shift…

- As the network perimeter dissolves, healthcare organizations turn to highly segmented security measures for better visibility and restricted access.
- Cybercriminals haven’t been on lockdown during the COVID-19 pandemic.
- Healthcare IT organizations have been battling new waves of ransomware, phishing and other malware attacks as they work to keep critical information flowing within overstretched hospitals and to remote users.
- The concept of zero trust is literal: No actors, systems or services operating from within a perimeter should be automatically trusted, and instead must verify anything and everything when trying to connect.

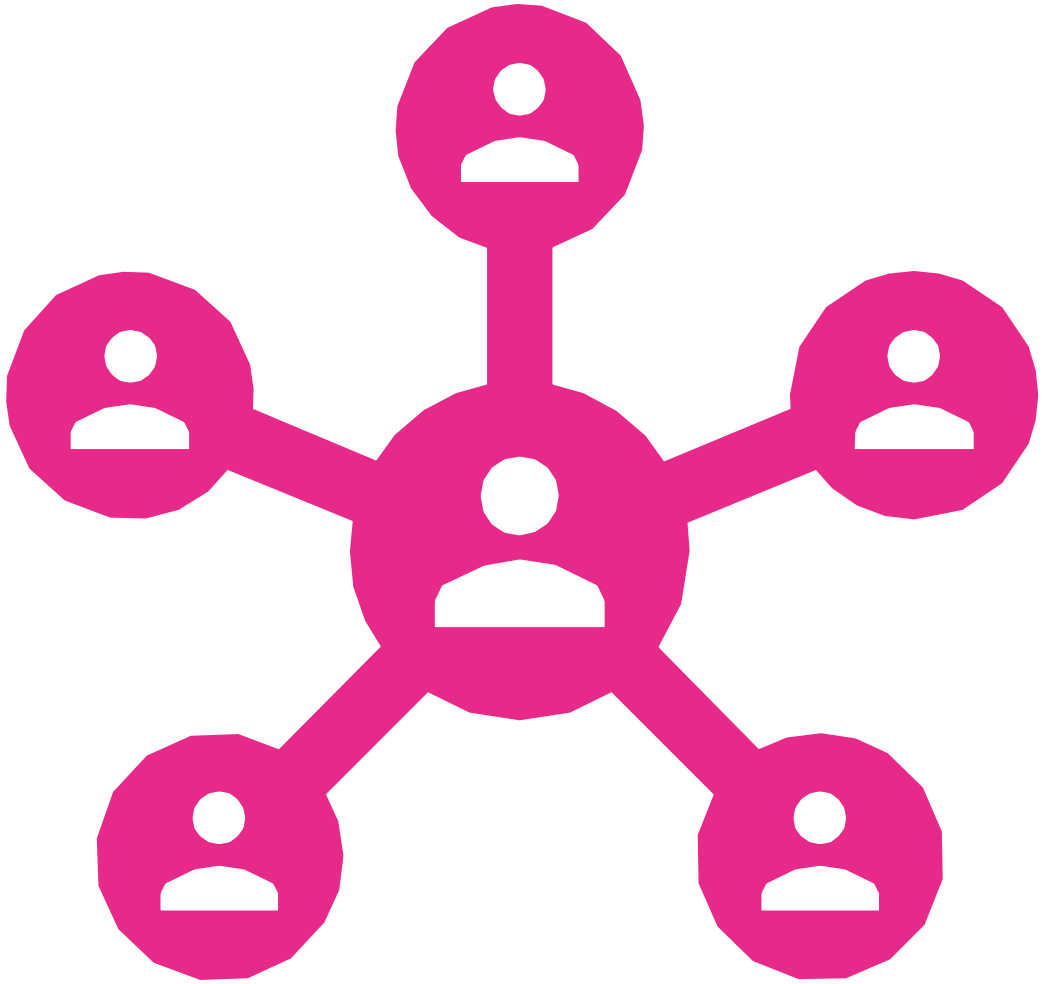

Rethink the Traditional
Security Architecture

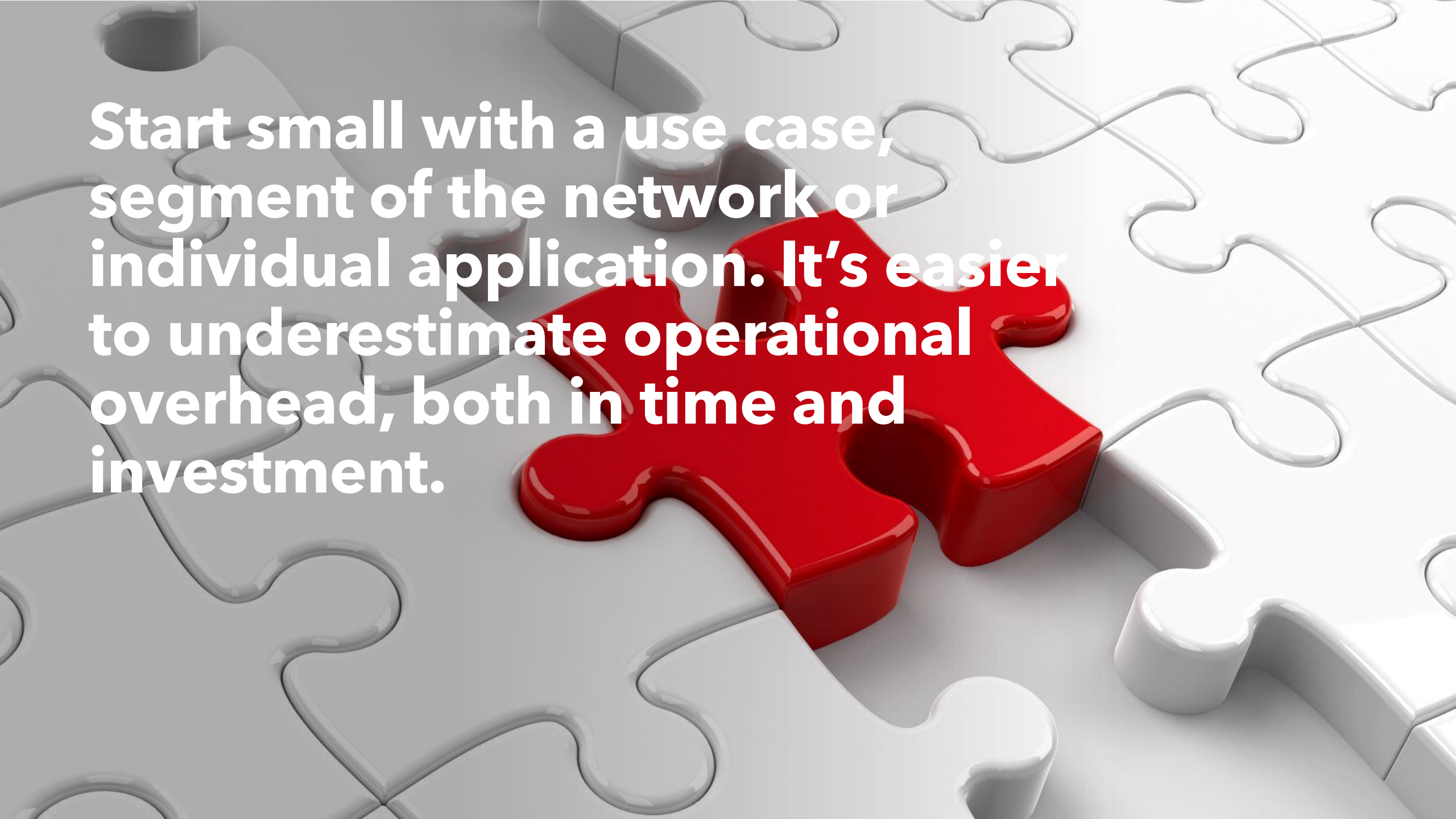
Starting the Zero Trust journey...

Deploying zero trust is a long and sometimes arduous process. Here's what to consider when getting started:



Identify and understand all devices, applications and traffic flows on the network. The information is valuable long before you achieve zero trust.




Start small with a use case, segment of the network or individual application. It’s easier to underestimate operational overhead, both in time and investment.

Communicate to everyone in the organization (users, management and IT staff) about the potential disruption and the ultimate benefits of zero trust.

Focus on the needs of patients and caregivers and then build your security architecture around meeting those objectives.

A LAYERED APPROACH TO SECURITY

Zero-trust security isn't accomplished by deploying a single tool or platform. The approach usually involves technologies from an array of categories:

- Device security
- Network security
- Data security
- Workload security
- Identity and access management
- Visibility tools
- Orchestration platforms


Segment the Network

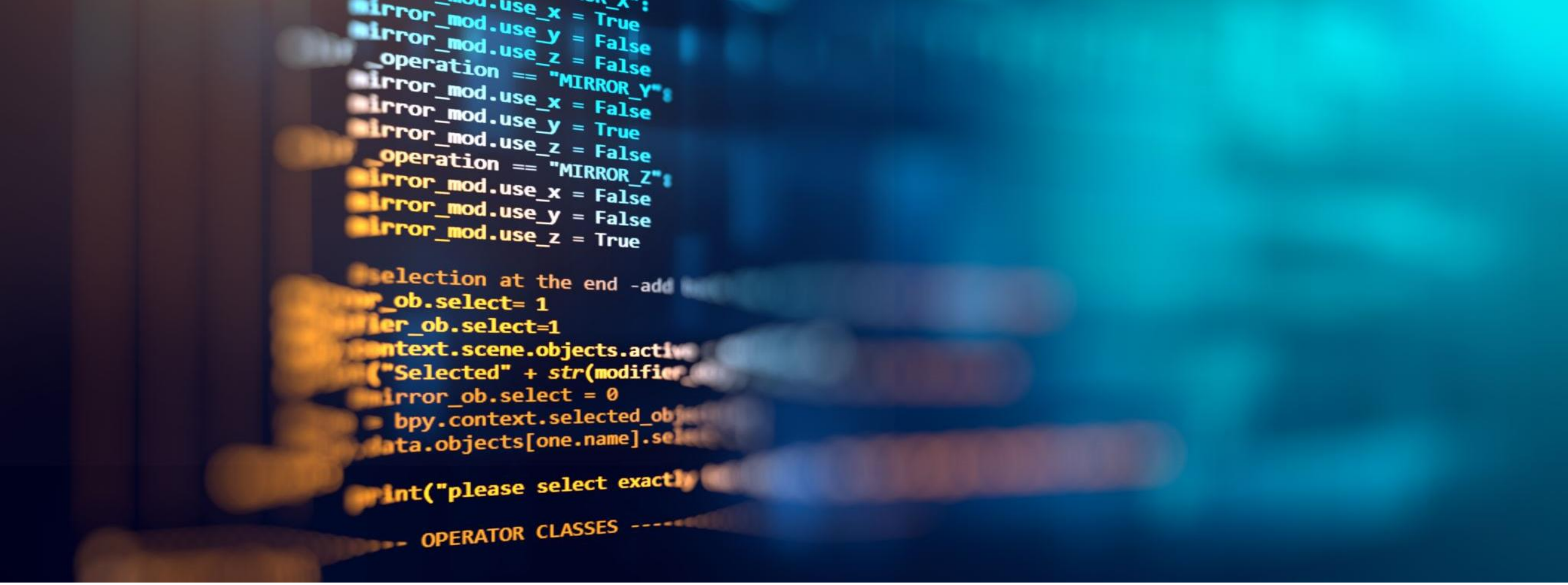
- Proper Segmentation is the cornerstone of a zero trust architecture.
- Organizations must segregate systems and devices according to the types of access they allow and the categories of information that they process.
- These network segments can then serve as the trust boundaries that allow other security controls to enforce the zero trust philosophy.

Enhance Identity and Access Management

- The second prerequisite for implementing zero trust is a strong identity and access management infrastructure.
- The use of multifactor authentication provides added assurance of identity and protects against credential theft.
- Deploying role-based access control allows applications to limit access in a manner that enforces the principle of least privilege.

Implement Least Privilege at the Firewall

- Least privilege also applies to networks. After building out network segments, cybersecurity teams should lock down access between networks to only traffic required to meet business needs.
- For example, if remote offices do not need direct communication with each other, that access should not be allowed by default.

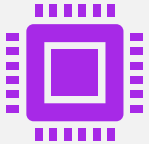


Add Application Context to the Firewall

- Modern firewalls go far beyond the simple rule-based inspection of years past. Cybersecurity teams should add application inspection technology to their existing firewall deployments, ensuring that traffic being passed over a connection bears appropriate content.
- For example, application context controls can verify that outbound Domain Name System traffic actually corresponds to queries and responses and is not being abused by an attacker to stealthily exfiltrate sensitive information.


Log and Analyze
Security Events

Security requires insight, and insight requires information.



Cybersecurity analysts can do an effective job only if they have a consolidated view of security events gathered from systems, devices and applications across the organization's network and cloud services.

Using a security information and event management (SIEM) solution allows for the rapid correlation of massive quantities of security information and provides analysts with a centralized view into that data.