# Securing the Infrastructure Behind Life-Saving Care

## Case Study

**SECTOR**
Healthcare

**CUSTOMER**
A US-based, large-scale healthcare institution (HI)

**VOICES**
Executive Director of IT (ED)

Principal Systems Engineer (PSE)

**ENVIRONMENT**
VMware

Please note, Vali Cyber anonymizes case studies to protect customer confidentiality—security isn't something you broadcast. References may be provided under NDA.

## Protecting Critical Care Infrastructure

As a prominent rural healthcare provider serving patients across five states, HI understands the importance of safety nets. As the only NICU and Trauma Center across more than 9,000 square miles, many patients have nowhere else within driving distance to turn. A system outage or cyberattack isn't just an IT issue; it carries real, potentially life-or-death implications.

> **"We're 24/7. Our Electronic Medical Record (EMR) has less than10 minutes of outage a month for maintenance." —PSE**

With that responsibility in mind, HI's IT and Security team has built a robust infrastructure: more than 100 VMware hosts running 99% of their workloads. They worked diligently to secure every layer, but the hypervisor remained at risk due to a lack of security tools.

> **"Our endpoints are protected with EDR. We keep them patched and up to date. But security is layered—you have to secure every layer. And for us, the hypervisor was the one layer where our security did not meet our standards."—ED**

> **"We weren't seeing any malicious activity at the time, but I knew the attack vector. In general, these hosts are barely protected—SSH turned off and a password, that's basically it—and they're absolutely critical to serving our patients. I've had close friends in the industry get hit, so I know it's not hypothetical. It's 100% possible. That's what kept me up at night." —PSE**

## Discovering ZeroLock®

PSE learned about Vali Cyber® through a mutual connection. After reviewing Vali Cyber's website, ED's response was simple: "Set up a meeting."

> **"We've done a lot of work over the last 10 years improving every layer of security, but the hypervisor was probably the biggest area where we didn't have a specific security tool. ZeroLock was intriguing because it's just one more layer of defense we could put in." —ED**

During the initial demo, the urgency became even clearer.

> **"One thing that was shocking was when Vali Cyber's SE showed how you can encrypt all the VMs with just a single command on the host. Just realizing that once a threat actor is in there, it's over. Seeing that in actuality—and then seeing how you mitigate that risk—that was really powerful to me." —PSE**

valicyber®

From there, momentum built quickly after evaluating their existing vendor.

> **"We went to our EDR vendor first, because why add to the stack if you don't have to. But they just provided documentation on putting a firewall in between. That looks good on paper, but as you start engineering the firewall solution it gets very complicated and expensive. Plus, it doesn't answer these new attacks that leverage stolen credentials." —PSE**

> **"We moved hypervisor security up the list once we found that there was a product. Honestly, from discovery to implementation, this may be one of our quickest turnarounds. Especially with recent attacks happening at the host layer, we realize our defenses must continually evolve because the attack methods are continually evolving." —ED**

## Fast-Tracked Approval

After a successful proof of concept which lasted about 45 days, HI decided to move forward—even though hypervisor security hadn't been budgeted for that year.

> **"Our executive leadership team is very receptive to cybersecurity needs. They trust us and give us the latitude to implement what we believe is necessary. Even though this wasn't in the approved budget, we were able to get a waiver once we explained where it fit and why it mattered. We had nothing protecting us at the hypervisor level, and until ZeroLock, there really wasn't anything available at that level." —ED**

## Deployment Under Pressure

Deployment happened to coincide with the end of the year—not typically ideal timing for major infrastructure changes—but the HI team didn't let that deter them.

> **"When I installed everything, I set it to come out of alert-only mode the Monday before Christmas. By then, we had most of it installed, and then someone we all know got hit. I pulled my team into the hall and said, 'Look, this is coming out of alert-only mode this week.' Normally, I would never roll out a change this big a few days before Christmas. But the vote in the hall was unanimous; we were enabling full protection ASAP. Looking back, I'd guess it took about 80 hours total to complete the full deployment. We put ZeroLock through crawl, walk, run phases in our environment, and it probably took me longer than a typical deployment because of how our environment is set up." —PSE**

> **"The thing I remember PSE telling me is that this is the first product he's ever worked with where he installed it, and it just worked. That's not always the case." —ED**

## Immediate Value and Reduced Risk

Today, the HI team is confident in their decision.

> **"ZeroLock's been able to help us reduce risk by protecting the keys to the kingdom for this layer that had not had this level of protection in the past. I think that's probably the biggest thing. Other features I really like are the exploit prevention and virtual patching features, which can remediate zero days before an update is released, as well as additional alerting on unusual activity or certain accounts." —ED**

> **"Yeah, the value is there. It's immediate value, and beyond the product there's quality support to work with if issues come up." —PSE**

**See what ZeroLock can do for you: info@valicyber.com.**

valicyber®