Protecting Critical Manufacturing Operations from the Inside Out

Case Study

SECTOR
Manufacturing
Critical Infrastructure

CUSTOMER
Large scale beverage company in the EU (CIC)

VOICES
Head of Infrastructure and Monitoring (HIM)

ICT System Specialist (SS)

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.

Operating Critical Infrastructure at Scale

As a large-scale European beverage manufacturer, CIC operates as designated critical infrastructure because they handle water, with strict requirements around uptime, resilience, and business continuity. Their IT environment spans roughly 100 hypervisors across 40 locations, each supported by its own IT team.

That structure brings scale—but also complexity when it comes to maintaining consistent security across the environment.

> **"We're coordinating across many different teams. We are still depending on the execution itself by the business unit. You can have security measures on paper, governance on paper, but it always comes down to how it is executed—and simple things, like using the same password, can still happen." —HIM**

Virtualization is foundational to CIC's operations, supporting both core IT systems and applications tied directly to production. Many of these workloads must remain on prem, where reliability and performance are critical. With that responsibility comes a clear expectation.

> **"You must ensure that your environment is safe, protected, and that people can't access systems they shouldn't. We have that responsibility, especially, because we are considered critical infrastructure. We have an obligation to fulfill business continuity."—HIM**

Despite strong controls in other areas, one critical layer remained exposed.

Realizing the Hypervisor could be a Target

CIC conducted a detailed analysis of how an attacker could move through their environment. What they uncovered reflected the reality of modern attacks.

> **"We were able to clearly see what could happen. With the new attacks on hypervisors, a threat actor could still abuse a vulnerability, even though the equipment was updated. They could get in, wait patiently, and eventually gain higher credentials until they reach the hypervisor." —HIM**

The team follows best practices—keeping systems updated and maintaining security controls—but that didn't seem like enough.

> **"We keep the environment as up to date as possible, but still…with the modern attack playbook, these things could happen." —SS**

valicyber®

The examination reinforced a mindset shared across the organization.

> **"This exercise showed us that it is not a matter of if—it's more like when." —HIM**

More importantly, it exposed a gap. While endpoints and networks were soundly protected, the hypervisor itself lacked visibility and active defense—leaving a critical layer vulnerable if attackers gained access.

Discovering ZeroLock®

CIC was introduced to Vali Cyber through colleagues in the United States, who had begun evaluating ZeroLock following similar concerns. The timing aligned closely with their own internal findings. After reviewing the solution, the value was clear.

> **"It's low effort to implement, and it immediately offers additional protection. So for us it was clear—let's continue and add that additional security layer." —HIM**

For CIC, ZeroLock addressed exactly what their analysis revealed had been missing: protection at the hypervisor layer itself.

Fast Validation & Deployment

CIC began with a small proof of concept in a lower-risk environment to validate the solution before scaling. The results were immediate.

> **"We deployed it in a small location first, configured everything, and tested whether it was working as expected. Given the positive results, we decided to move forward and make it standard." —HIM**

From there, rollout extended across multiple locations, coordinated centrally but executed locally. Deployment remained smooth—even across dozens of independent IT teams.

> **"It was fairly easy because everybody knew the importance. They mostly did it on their own. We sent instructions, they asked a few questions, and then implemented it. It went as smooth as it can be; which was surprising to me, because IT never goes as planned." —SS**

Protecting Against Modern Attack Paths

ZeroLock directly addresses the type of attack CIC analyzed—where threat actors leveraged a vulnerability, established persistence, and used stolen credentials to escalate access. By adding protection at the hypervisor layer, CIC is now able to reduce exposure across multiple stages of that attack path.

To HIM, one of the most valuable capabilities is securing direct hypervisor access through CLI MFA—especially given how the attack originally progressed.

> **"The SSH part of ZeroLock is very valuable. That is where all the root access is heading and having that secured makes a big difference. I was not aware that an attacker could use the operating system to try to break into the hypervisor. It's like, let's say, an attacker digging a hole into the ground. But with ZeroLock, you have someone in the basement that can tell you if someone is breaking into the deepest layer, the hypervisor." —HIM**

Beyond the technology itself, the onboarding experience also reinforced trust in the solution.

> **"What was very valuable to me was the responsiveness of support. If we had a question, we got an answer very quickly. And the training upfront, with a real environment where you can test things, helped us understand how everything works right away." —SS**

With both the technology and support in place, the team gained confidence in their ability to protect a previously exposed layer of their environment.

Real Security Means Peace of Mind

For CIC, the value of ZeroLock is not measured through alerts or events—it comes from knowing that a previously exposed layer is now protected.

> **"Knowing that ZeroLock is there, protecting the hypervisor, gives me comfort. It makes me sleep better at night. In the end, attackers will always try to find a way to bypass security measures—that is the difficult thing. But now that hypervisor itself is protected, I'm 100% confident that we are reducing risk." —HIM**

As a critical manufacturer, CIC is responsible for maintaining secure and reliable systems that support essential services. ZeroLock helps strengthen that responsibility by providing a preemptive layer of protection to the hypervisor that delivers both reduced risk and peace of mind.

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

valicyber®