Stopping a Cybersecurity Ripple Effect Without Breaking the Bank

Case Study

SECTOR
Finance

CUSTOMER
US-based, mid-sized bankers' bank (BB)

VOICES
IT Manager (ITM)

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.

The Critical Role of the Hypervisor

As a Bankers' Bank, BB plays a central role in financial transactions for hundreds of community banks across its region. While their environment may be relatively small—with fewer than ten hosts—it is also 100% virtualized, meaning their hypervisors form the foundation of every critical workload they operate.

In practical terms, this means their infrastructure reliability carries outsized consequences. A disruption at a typical bank might affect a single institution's customers. A disruption at BB could ripple across hundreds of banks and the communities they serve.

These realities shape the organization's approach to cybersecurity.

> **"If a normal bank has a problem, it impacts their customers. If we have a problem, it impacts a few hundred banks' customers, so we take our security seriously because we're not just impacting one community, we're impacting a lot of communities. The potential ripple effect that's inherent in our business means that if there were a security breach, the impact of that issue would be quite large. So, we want to make sure we're doing everything we can within a reasonable cost."**

Identifying a Hidden Security Gap

BB's IT team takes pride in adhering to security best practices across their environment. Firewalls, hardened configurations, and restricted services were already part of their defensive posture. But as they evaluated their infrastructure more closely, they realized there was one layer that remained largely unprotected: the hypervisor itself.

Traditional security tools focus on endpoints and workloads. That leaves the virtualization layer—the foundation that runs those workloads—without direct monitoring or protection.

> **"Obviously we had the standard protections and best practices like firewalls and turning off SSH, but we didn't have anything running on the hosts themselves that would detect anything happening. The only way we would have been able to know if something was happening on the hosts would be if the guest VMs started having problems."**

Exploring a New Approach to Hypervisor Security

BB's IT Manager (ITM) first encountered Vali Cyber through an event that included a hands-on lab demonstration of the ZeroLock platform. At the time, the team was not responding to a specific incident or threat actor. Instead, they were increasingly aware of industry trends showing attackers pivoting toward virtualization infrastructure. That realization made the lack of hypervisor protection difficult to ignore.

> **"We weren't worried about any specific threat actor at the time, but we've been seeing more threat actors who have started pivoting to target ESX. We realized we didn't have anything for the hypervisor, and then ZeroLock came along and we thought, 'Hey, this sounds great!'"**

Why ZeroLock Stood Out

As ITM tested ZeroLock and explored its capabilities, several features quickly stood out:

> **"One of the biggest selling points for us was that we could get MFA on the SSH. Everywhere else in our system we have MFA, so it was nice to be able to add that in as well."**

> **"We were also impressed with how lightweight ZeroLock is; it adds very little overhead for us. Plus, the speed at which it works is incredible. I was able to test it against different malware samples, and I was getting shut out just like that—in a snap of the fingers it was done—that was very interesting."**

> **"We also liked that ZeroLock is deployable both as a SaaS or on-prem. We prefer to keep things on-prem inside our network. With so many security vendors, they tell you to go to their cloud, but with ZeroLock, we don't have to open our network, and we can experience the same level of protection."**

Fast Deployment, Minimal Management

Once BB decided to move forward with ZeroLock, implementation proved straightforward. The team began by deploying to a small number of hosts before expanding protection across the rest of their environment.

> **"The deployment instructions are very well written, which made deployment very easy. We deployed on a couple of hosts first, and once that looked like it was running well, we expanded to the rest with everything fully turned on and active, and it worked."**

Since deployment, day-to-day management has required very little effort from the IT team.

> **"Honestly, we don't need to spend a lot of time in the console to actively monitor. It has notifications enabled, so it's pretty much been set-and-forget. We created one policy, made sure we turned on all the remediation and stuff like that, and then pushed it out to all of them and said, 'Go do your thing.' We haven't had to add any exclusions or tweaks. Everything has just worked very smoothly."**

Security That Works Quietly in the Background

For BB's IT team, the true value of ZeroLock lies in the confidence it provides. By protecting the hypervisor layer directly, the platform closes a security gap that previously had no practical solution.

> **"For my team, it provides an additional layer of peace of mind. It covers a gap we had—one we hadn't fully realized existed because there simply wasn't anything else addressing it. For management, it reduces risk, but because it's so well integrated, they've probably forgotten about it—and honestly, they should. They shouldn't have to worry about it; that's my job. We don't want employees or leadership wondering what's happening behind the scenes; everything for security should operate quietly in the background and do its job if something happens. ZeroLock lives up to that philosophy."**

> **"That said, if we are ever curious if it's still running, I can try to turn on SSH, and I'll get the ZeroLock notification saying I have to go through the MFA process. It's a quick test."**

Protection that Moves with Infrastructure

As BB evaluates potential changes to its virtualization platform, the team was pleased to learn that ZeroLock can continue protecting their environment even if they migrate hypervisors.

> **"We are considering a possible switch to another hypervisor. So, I was in a presentation learning more about it, and right there on their slide showed that it was compatible with Vali Cyber's ZeroLock. That was great to hear to know that we could migrate our hypervisor and still ensure protection."**

Clear Value for Security & Budget

For the leadership at BB, the business case for ZeroLock ultimately came down to value: addressing a real security gap at a cost that made sense.

> **"ZeroLock's price for the value is really good—good bang for the buck. The fact that you guys are so affordable makes it great. It makes it easier to implement and easier to sell to management. I was able to say, 'Hey, we have this gap, and they're the only ones to do anything for it, and their pricing is really reasonable even though they're the only ones with a solution.' So they said, 'OK, we'll trust your judgment. They sound good; they're the only ones doing anything to protect the hypervisor; and the price is reasonable. So we'll go with them.'"**

And for ITM, the conclusion is straightforward.

> **"I definitely see ZeroLock as a necessity. I would recommend it to any financial institution who runs hypervisors and VM loads on-prem because it covers a gap and helps reduce a real and significant risk. Nobody else in the security space covers hypervisor risks, so they just don't talk about it because they don't have a solution. Everybody knows the risk is there, they just don't talk about it."**

By securing the hypervisor, BB ensured that the infrastructure supporting hundreds of banks remains resilient against the growing wave of infrastructure-level attacks.

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

valicyber®