

# The World's Fastest and Most Effective Cyber Resilience Vault

## Proven operational resilience is more than an expectation.

## It's now a mandate.

### The Changing Face of Digital Resilience

It is no longer acceptable for organizations to shut down entire operations to prevent cyber attacks from spreading. Businesses and regulators have both realized that this approach is not sustainable. Understanding how business systems inter-operate, practicing how to safely fence-off individual services, and proving fast recovery of compromised environments–including the management plane–are crucial success factors in achieving digital operational resilience.

Proving digital operational resilience is more than hope and tools. It requires sustained cooperation by multiple teams to refine and test the processes that run a rapidly changing business. Features like immutability and air-gaps are important, but insufficient to achieve operational resilience. Are planned actions effective or will they cause undesired side effects? Are you building trust between teams, developing talent, and proving that security controls are effective? Organizations need automated and customizable recovery workflows that can be provisioned, customized, and decommissioned interactively to practice the actions meant for a live threat.

### Respond with more speed and less fear

Backup-based isolated recovery environments for on-prem critical workloads suffer from significant scalability and performance challenges. Their reliance on extensive data copying from slow, immutable storage over insecure IP links limits their effectiveness. Moreover, these systems focus on selectively recovering corrupted data without accounting for the possibility that an attack might still be underway. They also fail to address the needs of critical workloads that include IBM Power and bare metal servers, rather than exclusively VMware.

CyberVR helps organizations preserve evidence for forensics, while instantly delivering a multi-disciplinary, airgapped, and automated cleaning room where systems can be triaged, cleaned, hardened, validated, and reprotected. Teams can safely iterate infinite times before, during, and after the incident without fear, and without waiting for data to be copied from the desired point in time .

### Confidence in the Face of Attack

CyberVR automatically creates Thin Digital Twins from immutable snapshots of the entire data center stack (storage, compute, network, applications) for realistic sandboxing. This accelerates change management, pentesting, security validations, and production-grade recovery. Recovering in minutes instead of weeks lets organizations focus on refining processes and preventing vulnerabilities

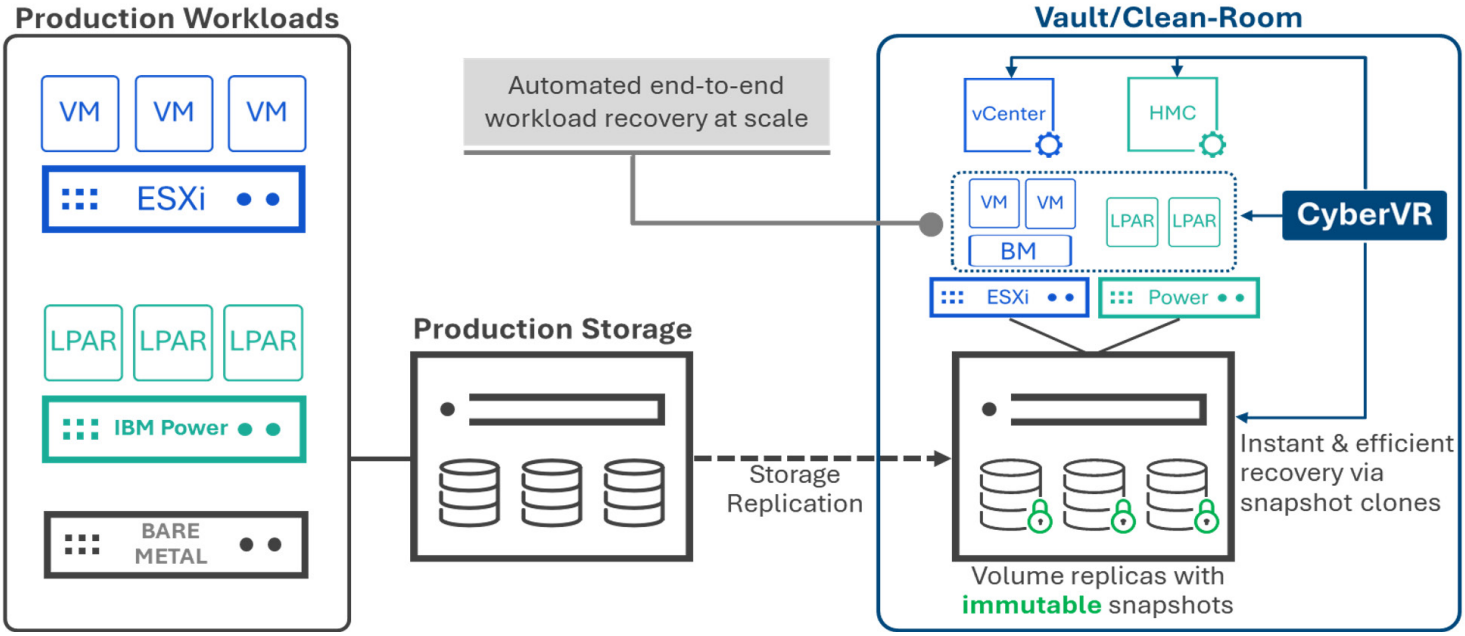
## Immutability is only the tip of the iceberg.

**CyberVR includes full automation for recovering x86 and IBM Power workloads at speed and scale**

## Automation, Cooperation, and Practice Deliver Digital Operational Resilience

Fencing off a compromised service during an attack is easier said than done. It assumes that organizations have implemented and tested network microsegmentation and zero trust, and have identified and fixed the side effects of making such drastic changes.

The confidence, trust, and skills built by practicing these adjustments safely are key to responding to sophisticated, destructive attacks. Organizations must consider threats that impact virtual and bare metal environments, as well as the management plane.




## Multi-layer automation delivers full IP isolation AND enterprise speed and scale

Prove the effectiveness of your security controls and the ability to recover quickly from destructive attacks

| Things to look for in a Cyber Resilience Vault | Things to avoid |
|---|---|
| **Low-level Immutability**<br>High performance and storage efficient. Immune from administrative deletion or NTP tampering | **Soft Immutability**<br>Software based immutability is prone to abuse, while password protected repositories are vulnerable. |
| **Instant and Automated Recovery**<br>End-to-end automation including capacity efficient data recovery, compute, network, and applications | **Manual and Data-Copy Based Recovery**<br>Results in immense recovery delays that require multiple recoveries. Lack of automation makes it hard to test. |
| **Scalability for all Required Workloads**<br>Predictable and proven recovery times for thousands of VMs and bare metal servers, that can be easily tested | **Limited Scope and Scalability**<br>Data recovery is not enough, functional services must be recovered, which require storage, compute, and network |
| **Automated Workflows with Any Tools**<br>Malware scanning, exploitability, full-force penetration testing, and management plane recovery | **Limited and Rigid Workflows**<br>Every environment is different. The workflows in the vault must be adaptable to various tools and workflows |

vm20/20

**Corporate Headquarters**
8201 Peters Road, Suite 1000
Fort Lauderdale, FL 33324 USA
vm2020.com

**Contact Information**
info@vm2020.com
1-954-282-5135
vm2020.com/contact-us