HITACHI
Inspire the Next

SOLUTION PROFILE

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

Traditional cyber vault solutions are copy intensive and focus on recovering raw data to pre-encryption points. Recovery of workloads to a hardened state is an afterthought. They assume incorrectly that the management plane inside the vault is safe, and expect users to manually iterate through the cleanup, hardening, validation, and re-protection work needed before reconnecting users. They ignore the high probability of additional attacks coming to life inside the vault.

CyberVR and Ops Center Protector help 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 and Ops Center Protector automatically create Thin Digital Twins from immutable snapshots of the full data center stack (storage, compute, network, applications) for realistic sandboxing, allowing for accelerated change management, pentesting, security control validations, and recovery into production-grade storage where users can connect. The ability to recover in minutes instead of weeks means organizations can spend time refining processes and preventing new vulnerabilities.

Air gap technology is only the tip of the iceberg in operational resilience.

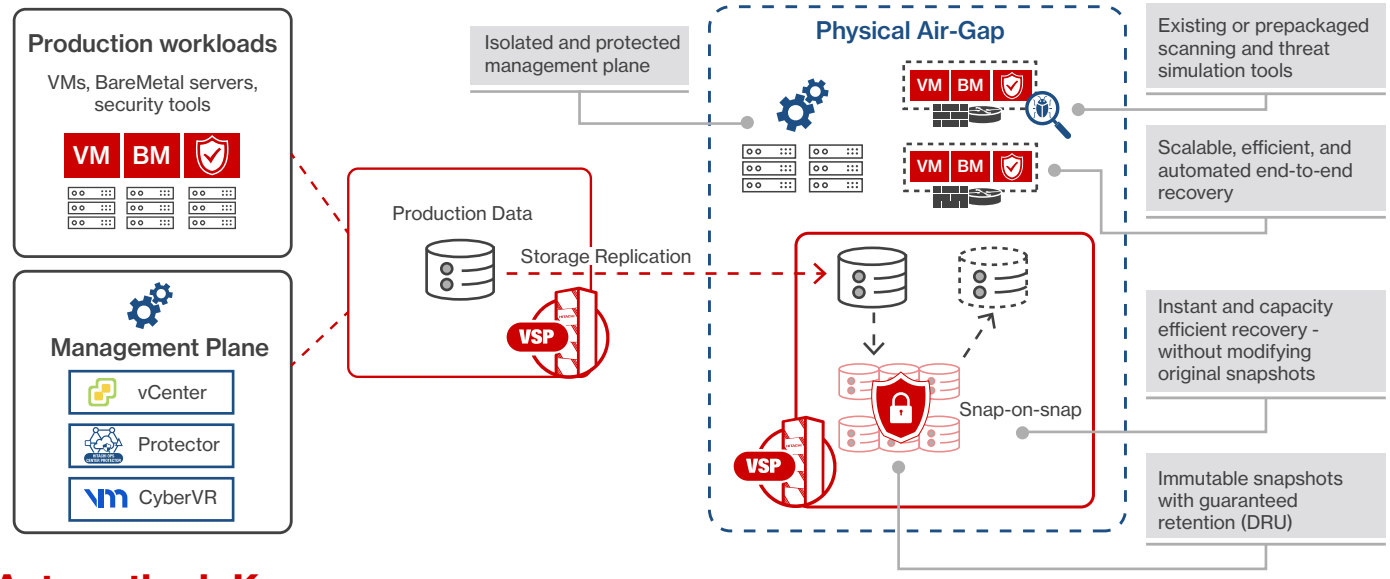
CyberVR and Ops Center Protector have you covered for virtual and physical servers

SOLUTION PROFILE

The World's Fastest and Most Effective Cyber Resilience Vault

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.



Automation is Key

Sustaining Digital Operational Resilience efforts requires advanced automation

Things to look for in a Vault

Low-level Immutability
High performace and storage efficient.
Immune from administrative deletion or NTP tampering

Instant and Automated Recovery
End-to-end automation including capacity efficient data recovery, compute, network, and applications

Scalability for all Required Workloads
Predictable and proven recovery times for thousands of VMs and bare metal servers, that can be easily tested

Automated Workflows with your Choice of Tools
Malware scanning, exploitability, full-force penetration testing, and management plane recovery

Things to avoid

Soft Immutability
Software based immutability is prone to abuse, while password protected repositories are vulnerable.

Manual and Data-Copy Based Recovery
Results in immense recovery delays that require multiple recoveries. Lack of automation makes it hard to test.

Limited Scope and Scalability
Data recovery is not enough, functional services must be recovered, which require storage, compute, and network

Limited and Rigid Workflows
Every environment is different. The workflows in the vault must be adaptable to various tools and workflows

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact

HV-CBE-SP-vm2020-08Aug23