ZeroLock® Enhancing VCF with Preemptive Security

	VCF Security: vDefend, Advanced Cyber Compliance (ACC), Live Patching	ZeroLock: Preemptive and Runtime Security for the Hypervisor
Coverage	• vDefend operates at the network level and provides network traffic control. • ACC is focused on compliance rather than protection.	• Operates at the host and hypervisor runtime level. • Provides preemptive and runtime security for the hypervisor itself.
Patching	• vDefend's Distributed IDPS virtually patches guest workloads at the VM's virtual NIC. It does not inspect the hypervisor, leaving a visibility gap. • Live Patching is reactive; it requires a known CVE and a vendor patch and excludes DPUs and some VM types. • A VM escape that targets the hypervisor through device emulation or hypercalls is not inspectable network traffic, so vDefend cannot not see it from the network layer.	• A live ESXi exploit was demonstrated at Pwn2Own Berlin on May 17, 2025. Broadcom's patch shipped July 15. ZeroLock customers were protected the entire two months. • Preemptive zero-day protection on the hypervisor itself. Behavioral lockdown rules detect CVE exploitation at runtime. • Runs on the hypervisor and watches the host's own execution. A VM escape produces anomalous hypervisor behavior at runtime, and behavioral lockdown rules stop it without a known CVE or signature.
Ransomware Prevention	• vDefend catches ransomware on the workload network. Fileless detection is limited to Windows guest workloads. • ACC provides recovery to isolated clean rooms after an incident. Clean rooms are expensive; they require additional hardware & VCF licenses as well as a segmented network.	• Stops ransomware on the hypervisor in real time, including fileless and Living off the Land (LotL) attacks using native ESXi tools (openssl, rm, sh, Python). • Blocks the ESXi attack chain Google Mandiant documented in July 2025 against Scattered Spider in "From Help Desk to Hypervisor."
Hardening	• vDefend's Distributed Firewall provides microsegmentation between workloads. • execInstalledOnly blocks unsigned binaries. It does not stop LotL attacks using signed native tools such as python, sh, nc, and openssl. VCF has no native MFA for SSH to ESXi.	• MFA for SSH, dCUI, and CLI on the hypervisor, closing a significant gap VCF leaves open. • Behavioral detection of LotL execution on ESXi and runtime lockdown rules that block unauthorized config changes at the moment of execution.
Compliance	• ACC and DISA STIG enforce ESXi configuration. They cannot see what a logged-in attacker actually does. • Drift is detected and remediated with periodic scans. These scans do not provide real-time prevention of active attacks.	• Blocks malicious config changes at the moment of execution, eliminating the window ACC's remediation cycle leaves open. • Forensic-grade alerts with process, parent, and user context provide PCI DSS, HIPAA, and DORA audit evidence that configuration baselines cannot produce. • Satisfies runtime monitoring controls required by PCI DSS 4.0 (Req 10, 11.5), HIPAA §164.312(b), DORA Article 9, and NIST 800-53 SI-4 that configuration baselines alone cannot meet.

valicyber®