ESX Hardening vs. Behavioral Enforcement
What Compliance Frameworks Check, and What They Leave Behind

The left column is what **DISA STIG**, **CIS Benchmarks**, **VMware's hardening repository**, and **VCF Advanced Cyber Compliance** tell you to verify on every ESX host. The right column is what attackers do once they are inside, drawn from recent Mandiant and Huntress reporting. Hardening cannot reach those actions. **ZeroLock can.**

Disable SSH and ESX Shell Under the Host Services view, confirm TSM and TSM-SSH are stopped unless actively in use for administration. CIS / DISA STIG / VMware hardening repo	**Attackers re-enable SSH using stolen credentials** Mandiant documents UNC3944 logging into vCenter with credentials harvested through help desk social engineering, then enabling SSH on ESX from the VCSA. The compliance state is restored afterward. The window in between is where damage happens.
Enforce Secure Boot and execInstalledOnly Run `esxcli system settings encryption get`. Both values should read TRUE. Blocks unsigned executables from running on the host. DISA STIG ESXI-80-000148 / CIS Benchmark	**Native binaries are not blocked** openssl, esxcli, vim-cmd, dd, and python are all signed platform components. Huntress documented attackers using openssl to AES-encrypt VMDKs directly—no custom binary to detect. execInstalledOnly is silent on tools the system trusts by design.
Default-deny firewall, disable unused services Keep DHCP, DNS, NTP, vMotion, and vSphere Web. Disable Active Directory, FTP, SLP, CIM, and any service not in active use. DISA STIG ESXI-80-000214 / CIS firewall section	**Authenticated management traffic is expected** Once an attacker holds valid vSphere credentials, their actions flow over the same management interfaces administrators use. Firewalls and segmentation see legitimate vCenter API calls. The network has no basis to block them.
Avoid Active Directory integration Open the Host Authentication view. "Active Directory enabled" should read No. The default 'ESX Admins' group has been actively abused per Broadcom and Microsoft advisories. Broadcom advisory / VMware hardening guidance	**Hypervisor access is reached through identity, not the network** Mandiant's 2025 reporting describes attackers adding compromised AD accounts to vSphere Admins groups via WinRM, then pivoting to vCenter. The hypervisor itself is hardened. The path in goes around it through the identity plane.
Patch known-exploited CVEs Compare your build against current advisories. CISA tracks active exploitation of CVE-2025-22224, -22225, and -22226—all added to KEV the same day they were disclosed in March 2025. CISA KEV / VMware Lifecycle Manager	**The window before a patch ships is unprotected** Those three CVEs were already being exploited as zero-days at disclosure. CVE-2025-41236 had a two-month gap between Pwn2Own and a shipping patch. Configuration baselines cannot defend against unpatched vulnerabilities.

The Pattern

Every check on the left confirms the host is configured correctly. Every item on the right is something an authenticated identity can do once they are already inside. DISA STIG, CIS, the VMware hardening repo, and VCF Advanced Cyber Compliance all measure configuration state. None of them constrain runtime behavior. **ZeroLock evaluates each action inside an authenticated session and blocks destructive workflows in real time—even when the user is root.**

valicyber®