Why Hypervisor Security, Why Now?
Protecting Your Most Vulnerable Assets from Ransomware

As organizations increasingly adopt virtualization and private cloud infrastructure to improve scalability and cost-efficiency, the hypervisor has become a core asset. However, this central role also makes it a high-value 'Keys to the Kingdom' target for cyberattacks. Traditional endpoint defenses fail to secure hypervisors, leaving a critical gap in the organization's security posture. With a 3-fold YoY rise in hypervisor attacks costing hundreds of millions of dollars, investing in virtualization security is no longer optional—it's mission critical.

What would happen if half of your annual profits were lost in an attack?

Marks and Spencer reported a potential profits impact of $402M as a result of a recent Scattered Spider attack which leveraged their VMware ESXi hypervisors.

bleepingcomputer.com/news/security/marks-and-spencer-faces-402-million-profit-hit-after-cyberattack/

4 Impacts of Not Securing Your Hypervisors

Failing to protect your hypervisor from ransomware can lead to prolonged downtime, loss of critical data, significant operational disruption, and serious legal and financial consequences.

1. **Risk:** Hypervisor attacks are driving massive losses and lawsuits, putting virtualization security on the board's agenda. Securing this layer mitigates those risks and reinforces the success of key priorities, such as deploying AI on private cloud infrastructure.
2. **ROI:** Reports from Scattered Spider attacks show organizations have experienced between 2 weeks and 2 months of disruption; having a multi-layer defense strategy for your private cloud helps ensure operations runs moothly.
3. **Compliance**: With the addition of ESXi to the MITRE ATT&CK framework, auditors will be paying close attention to hypervisor security. Organizations should act proactively now to ensure they pass future audits.
4. **Competitive advantage:** Particularly for service and hosting organizations, building out a secure private cloud solution is a high priority. Next generation security provides differentiation and speaks to customer demands.

Solution & Benefits Provided by ZeroLock®

Vali Cyber's Hypervisor Ransomware Protection takes a multilayered approach to virtualization defense by providing a comprehensive security solution that allows you to:

1. **Reduce risk by preventing attacks** with SSH-MFA, application filtering, tamper protection, and more, allowing you to protect revenue and key priorities.
2. **Deliver ROI through operational continuity** provided by an easy-to-deploy security solution for VMware ESXi and Linux-based hypervisors with minimal overhead, one-line deployment, and a signed VIB with Broadcom.
3. **Secure the competitive advantage** by being able to provide and market a holistic security approach to your hypervisor-based products.
4. **Help meet regulatory compliance with virtual patching and runtime security**. Virtual patches that can be employed quickly without taking systems offline, AI detection, and automated remediation keep systems safe in real-time.

Schedule your demo today! info@valicyber.com

valicyber®