virsec

Healthcare Zero Trust Protection

Healthcare Organizations Face Unprecedented Ransomware, Zero-Day, and Remote Code Execution Attacks

Healthcare Providers are being targeted at an alarming rate by ransomware attacks—and the numbers are rising. Due to the critical nature of health systems, attackers know they are more vulnerable to ransom demands. Recent studies found that attacks targeting healthcare delivery organizations doubled from 2016 to 2021.

Zero-day attacks have become a cause for great concern as unpatched and legacy systems are increasingly targeted due to their high level of vulnerability.

Remote Code Execution (RCE) is another common attack vector used as traditional detect and respond tools cannot guard against it adequately.

226 Airport Parkway Suite 350, San Jose, CA 95110 VIRSEC.COM

Protect Mission-Critical Workloads

Backstop protection against zero-day, RCE, ransomware and software supply chain vulnerability exploits to ensure business contunity and avoid the cost of a breach.

Legacy Workload Protection

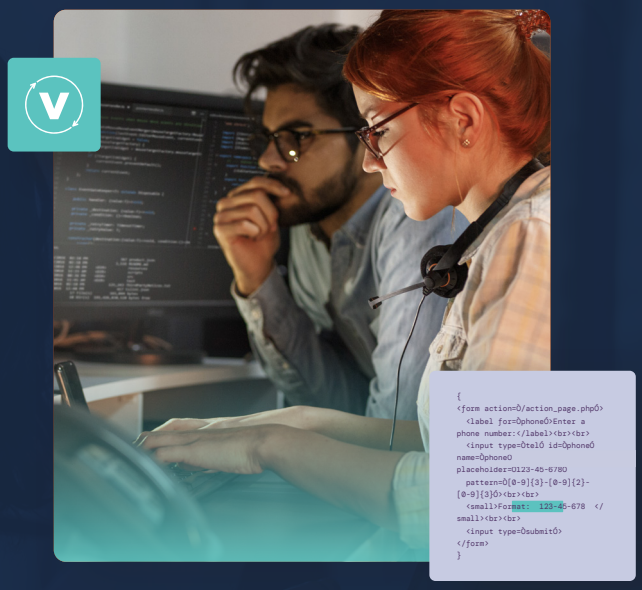
Protect vulnerable, out-of-support workloads that no longer receive regular security patches against modern attacks.

Patch on Your Terms

Mitigate patch pressure that comes with more software and more vulnerabilities with backstop vulnerability protection.

Virsec offers the industry's first Zero-Trust Platform for Server Workload Protection

Virsec leverages security controls that embrace a modern automated "allow listing" approach – permitting only known good code (executables, libraries, and scripts) to run. All other code is explicitly denied execution.

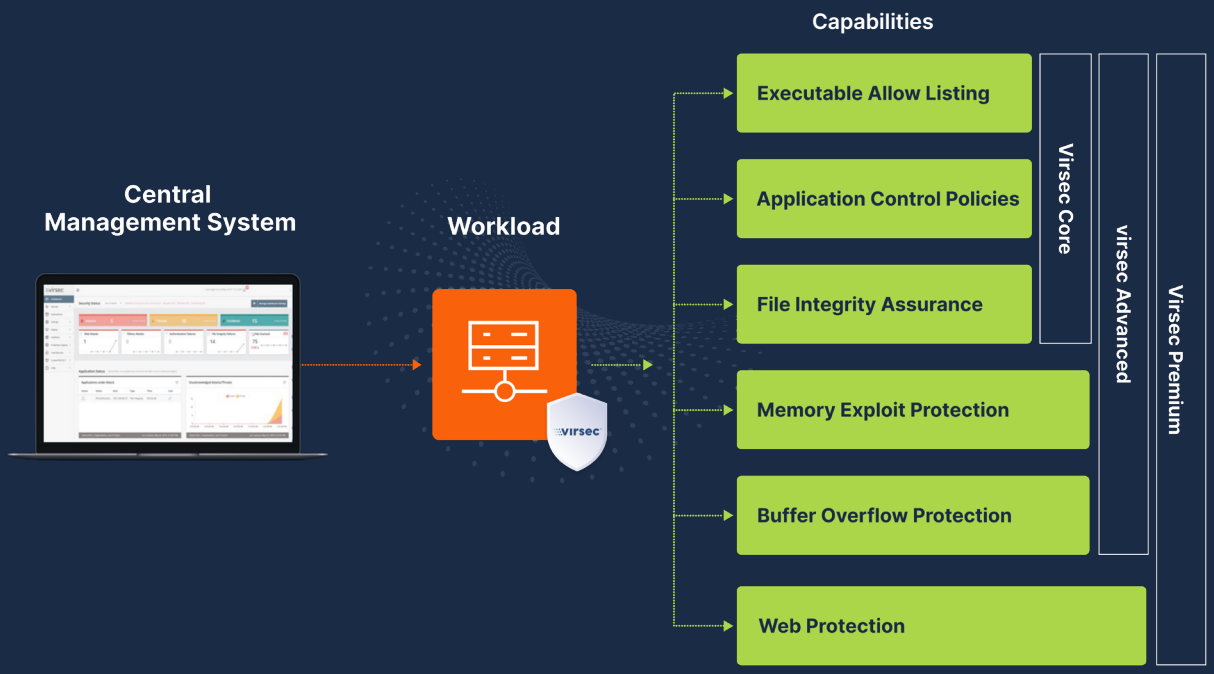


With our groundbreaking approach, Virsec delivers the highest levels of protection, with zero dwell time and low false positives to:

- Stop known and unknown attacks
- Protect servers, even unpatched and legacy systems
- Reduce dwell time to zero
- Lower false positives
- Minimize disruption to patient care
- Improve safety record
- Meet regulatory requirements
- Protect revenue and reputation
- Alleviate patch management
- Keep legacy applications running securely
- Stop ransomware and malware in milliseconds and avoid millions of dollars in data breach costs

226 Airport Parkway Suite 350, San Jose, CA 95110 VIRSEC.COM

Virsec **Zero Trust Protection Stack**



About Virsec

Virsec offers continuous protection for application workloads, stopping known and unknown attacks—including zero days. With our patented technology, we take a defense-in-depth approach with a Zero-Trust model that allows only authorized code and executables to run, and nothing else. Battle-tested against 200+ of the top government red-teamers and trusted by Fortune100 companies, Virsec has repeatedly proven a protection-first model works. Virsec is headquartered in San Jose, CA with offices worldwide.

For more information, please visit **virsec.com** and reach out to Anthony Binge, VP Healthcare at **abinge@virsec.com** or call/text **(407) 314-3859**

Red Hat

Virsec has partnered with Red Hat® to automate server protection at scale – both RHEL and Windows. We can deploy our patented security solution using pre-configured Red Hat Ansible® Automation Platform playbooks, and once your workloads are protected, Red Hat will consult with your teams to configure your incident response automation playbooks, including ticket automation, firewall rules, and file and VM quarantine.