Protect Legacy Out-of-Support Applications and Workloads

Secure outdated Windows and Linux Servers™

Legacy systems that are no longer supported by the vendor present a security risk. However, a runtime protection solution like Virsec Security Platform (VSP) provides continuous protection for the application infrastructure on operating systems such as Microsoft Windows 2008 or CentOs 6.x. It instruments the runtime environment so only authorized processes, files, libraries and their verified dependencies are able to run. It monitors deviations in runtime and mitigates any instance of executing executables that have been added or modified, blocking malicious activities from the otherwise trusted operating system-related process. Many organizations aim to strengthen security by adhering to common best practices *(i.e., monitoring logs, network activity, and permissions)* and wrapping older applications inside a protective bubble secured by hardware-enforced isolation to minimize risk. However, this approach is not enough to prevent more sophisticated attacks. Even if your organization is making progress in patching legacy systems still supported by vendors, there often remains thousands of applications and varying workloads posing an imminent security risk that remains unresolved, especially within expansive infrastructures with thousands of known vulnerabilities.

Where patching is not viable or too difficult to accomplish, organizations accept the risk without immediate remediation as they look to upgrade the business system sometime in the future. With VSP, organizations can do just that with the assurance that protection is in place for legacy application workloads that expose the business to risk and even for the replacement technology they are upgrading to in the future.

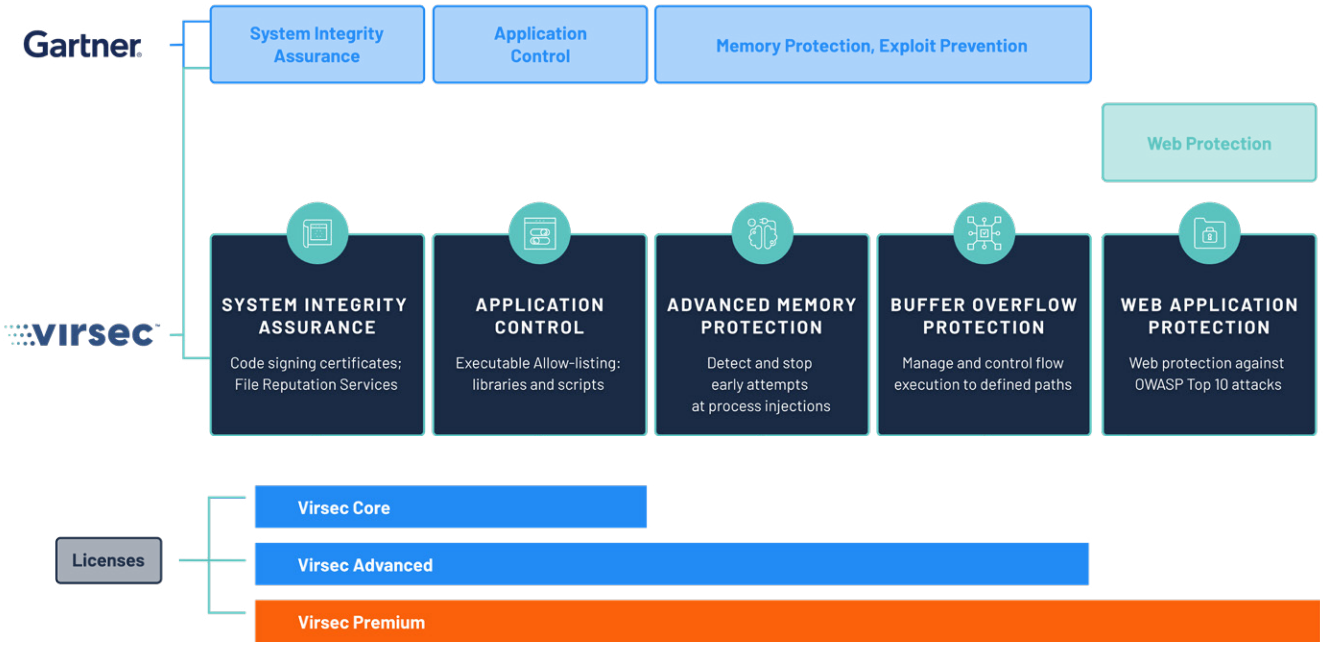
226 Airport Parkway, San Jose, CA 95110 VIRSEC.COM

Easily Overcome Workload Security Challenges:

- Legacy applications were written when application security was simple or non-existent
- New vulnerabilities and the sophistication of attack method continuously evolves, reaching voluminous levels
- Vendors have gone out of business, support has slowed or ceased with obsolescence
- Expertise to develop software patches or address software errors has become specialized and costly to maintain
- Digital transformation is an arduous process taking months or years to complete as risk remains

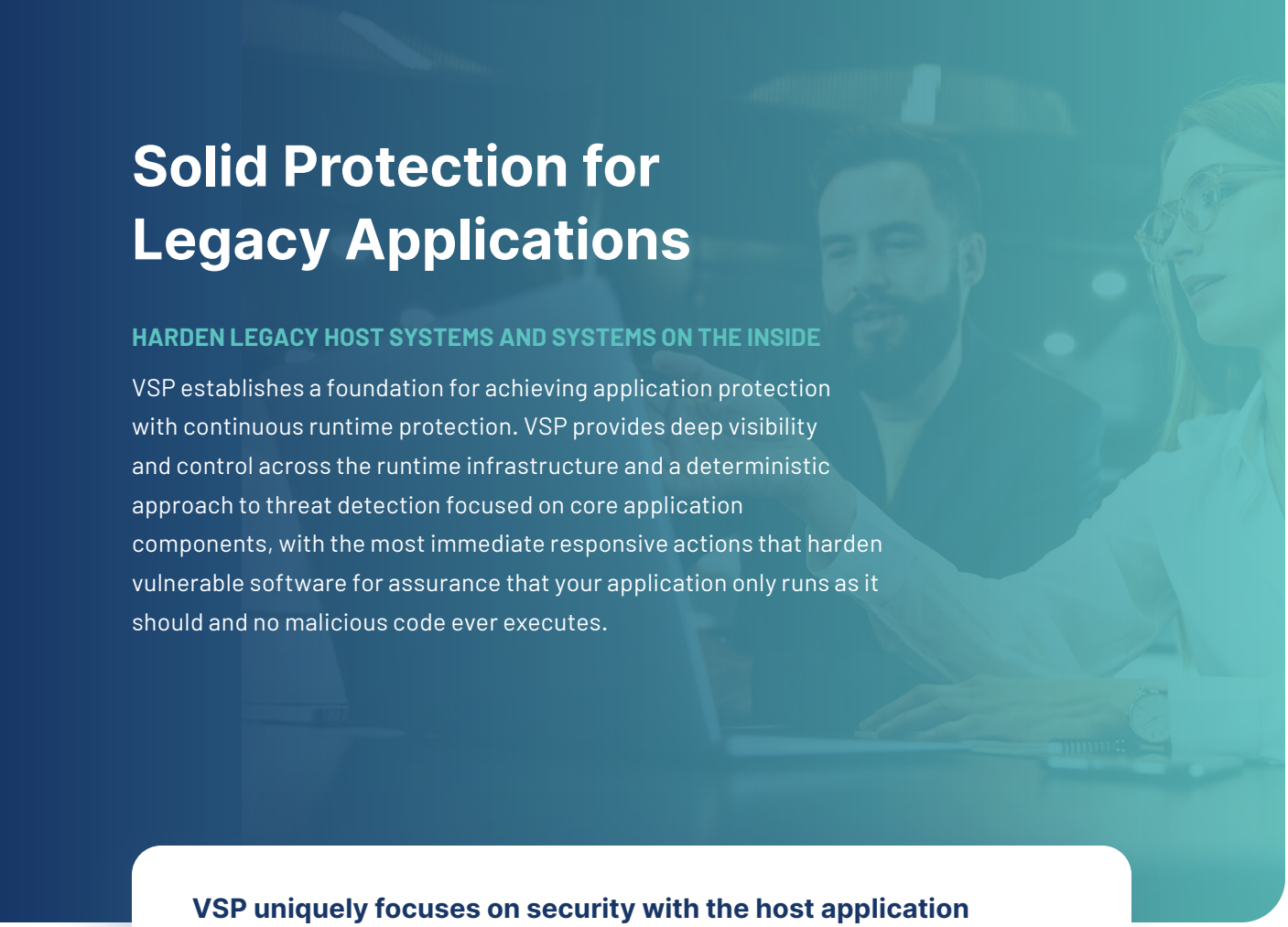
Virsec Security Platform

Virsec Security Platform (VSP) automatically maps what your workloads are supposed to do, then stops any deviations in milliseconds, preventing attackers from leveraging vulnerabilities to take control and run malicious code. VSP is a proven technology that enables leading government and commercial organizations worldwide to protect the legacy and proprietary software essential to business at runtime against ransomware and other known and unknown threats before there is business impact. It further reduces overall security costs and ensures continual compliance even where applications have outlived the intended life span.



Note: Protection for legacy applications is currently provided only via Virsec Core capabilities.

Solid Protection for Legacy Applications



HARDEN LEGACY HOST SYSTEMS AND SYSTEMS ON THE INSIDE

VSP establishes a foundation for achieving application protection with continuous runtime protection. VSP provides deep visibility and control across the runtime infrastructure and a deterministic approach to threat detection focused on core application components, with the most immediate responsive actions that harden vulnerable software for assurance that your application only runs as it should and no malicious code ever executes.

VSP uniquely focuses on security with the host application delivering zero-touch protection against attacks that bypass traditional tools and efforts without code changes

CONTINUOUS RUNTIME PROTECTION

Virsec Security Platform allows you to protect applications running in **Windows Server 2003, 2008 R2 SP1, 2012, Red Hat Enterprise Linux or CentOS 6.5, 6.7, 6.10, and SUSE 12 with strict application controls and runtime analysis**. It covers vulnerabilities exposed due to the time between patching and will **act as a patch-bridge for Windows Server between upgrades**. The implementation will continuously protect the entire software stack across all runtime components, including files, executables, processes, and libraries that allow attacks to build in memory as systems execute. The deep visibility activates deterministic runtime protection capabilities to counter dangerous attempts to misuse or exploit trusted authorized components in real-time as events happen. Thus, it blocks attacks like PrintNightmare or those that affect supply chains.

226 Airport Parkway, San Jose, CA 95110 **VIRSEC.COM**

FREE IT RESOURCES OF REMEDIAL TASKS

All businesses using legacy systems are commonly advised to invest in different layers of security, including endpoint solutions, network-based IPS, proxy solutions, and a solution for email security. These solutions in themselves are not foolproof. Eternal Blue, WannaCry, Ransomware, and other malicious tactics have compromised workloads protected by these other solutions. Virsec adds a layer of protection on the server to enforce defense where common solutions fail and reduce the need or resources to perform common actions taken to maintain your security framework across an array of systems.

VSP minimizes risk even when you:

- **Are unable to conduct vulnerability assessments to identify weaknesses & what needs fixing.**
- **Are unable remove any unused applications and services.**
- **Cannot create rules and policies to help securely govern your systems.**
- **Cannot update your operating systems.**
- **Are unable to ensure your antivirus solution is up to date where support is still offered.**
- **Cannot maintain layer 5 and 7 network-level attack defenses, including host-based intrusion prevention software policies and application firewall.**

Upgrading infrastructure devices is a big undertaking and, in some cases, requires downtime. However, the costs of ignoring the problem of aging infrastructure and running legacy workloads can run much higher. With VSP, organizations have successfully mitigated the attacks without downtime, zero-touch automation, and no false positives to reduce costs of protection assurance for critical legacy workloads.

226 Airport Parkway, San Jose, CA 95110 **VIRSEC.COM**

Optimize Workload Protection Strategy

Take the complexity out of workload protection with a single solution that provides complete runtime visibility at depth and consolidate existing application controls that drive workload protection across all vulnerable applications. Identify known and unknown attacks and evasive threats like process or DLL injections under a single integrated solution that provides additional advanced web application protection capabilities and precise zero-day defense. Optimizes your line of sight and control while reducing the impact of threats throughout your workload environment.

Improved Security

- Virsec provides modern application security by controlling legacy applications to only execute as intended and blocking any unknown or known bad functions.
- Reduce risk with protection against OWASP top 10 and MITRE top 25 most dangerous attacks.

Maintenance

- Allows for continued use of implemented known maintenance and troubleshooting processes and utilization of IT staff's established knowledge.

Business agility

- Business functions can focus on execution and scaling rather than spending time learning and establishing new processes and methodologies.

Cost Reduction

- Reduction or no interruptions to business services and applications due to security breaches - allows for continued ROI on existing applications and their supporting infrastructure.
- Eliminates the immediate need to replace with new modern applications that might not provide equivalent functions.
- No need to retrain staff on how to use and maintain new applications.
- Reduction in investigating false positives.

User Experience

- Maintain consistent user experience within established processes and methodologies.

virsec™

To learn more about the Virsec Security Platform and to find out how to start protecting your mission-critical server workloads, visit us at www.virsec.com

At Virsec we know a protection-first cybersecurity model is possible. By making server workloads self-protecting, we offer continuous protection, stopping known and unknown attacks—including zero days. With our revolutionary, patented technology, we secure software from the inside at runtime, precisely mapping what the app can do and stopping malicious code before it can run. Battle-tested against 200+ of the top government red-teamers and trusted by several Fortune100 companies, Virsec has repeatedly proven a protection-first model works. Virsec is headquartered in San Jose, California, with offices worldwide. For more information, please visit virsec.com.

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