virsec®

SOLUTION BRIEF

Better Protection for Microsoft SharePoint® Servers

Over 100 high-risk and critical Microsoft SharePoint® vulnerabilities* can put your business at risk when left unpatched. With recent remote code executions attacks targeting SharePoint collaboration servers, experts recommend that organizations patch systems immediately and strengthen existing protections.

Application-Aware Workload Protection

Virsec ensures that vulnerable SharePoint servers are continuously protected, maintaining server integrity against threats like remote code execution, advanced web injections, and more, with minimal operational overhead.

Virsec Security Platform (VSP) delivers app-aware workload protection to identify and stop threats that attempt to breach your SharePoint environment. With host-level runtime protection, VSP prevents manipulation or misuse of trusted commands, processes, scripts, and functions which hackers use to target SharePoint. VSP also defends SharePoint's web services on the ingress, sanitizing requests to prevent privilege escalation, web shell uploads and more, without overhead or false positives.

VSP delivers in-depth application runtime protection that increases the effectiveness of your security program beyond that delivered by traditional anti-malware, document scanning, machine learning, and network traffic monitoring tools - while reducing noise and eliminating attacker dwell time and tuning.

Simple and Effective Server Workload Protection

Frees resources from patching
Automatically addressing high-risk and critical SharePoint CVE's without manual effort

Ensures evolving threat defense
Stops evasive or never-before-seen attacks including those that use a web shell or attempt to introduce malicious code into SharePoint workflows from memory

Assures System Integrity
Guarantees only authorized code, libraries, scripts, and processes can execute

Delivers out-of-the box protection
Scales easily, requiring no ongoing tuning, guess work, or signature updates.

Comprehensive Microsoft SharePoint Protection

With application-aware workload protection, VSP stops hackers from abusing your SharePoint servers, even when vulnerabilities have not been patched or even disclosed. Unlike standard SharePoint security solutions, Virsec does not require sandboxing or cloud-based analytics. VSP deterministically identifies both familiar and unknown file-based or fileless malware, and script-based exploits, no matter how the threat materializes. Our superior detection and protection capabilities stop attacks at the earliest point in the kill chain and ensure no malicious code executes.

Full-Stack Protection

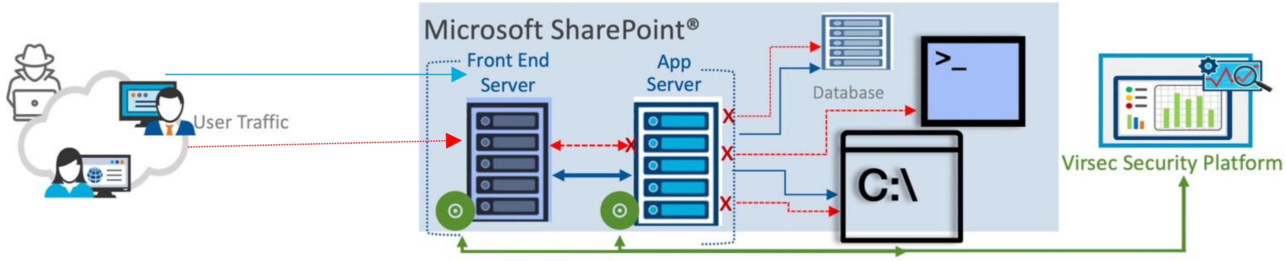
Virsec prevents interpreter abuse and process spawning beyond the web layer

Complete Runtime Visibility

Virsec provides visibility across all application layers and automatically renders malicious shell activity useless

Application Awareness

Virsec understands legitimate SharePoint behavior and stops attempted deviations



Virsec provides the only single-solution that protects host-based applications with visibility from the inside, while combining application control, system integrity, and memory protection to effectively prevent evasive exploits and ensure SharePoint integrity across the web, host, and memory level. For more information visit www.VIrsec.com.

*NIST National Vulnerability Database: https://nvd.nist.gov/vuln/search