

Virtual Patching

Eliminate Vulnerability Risk During Patching Cycles

Patching software is a fact of life, but the avalanche of vulnerabilities and today's complex software stacks makes it difficult to keep up. Many organizations fall behind in patching software because the process is too labor intensive, disruptive and causes unintended consequences, or simply because patches are not available. Meanwhile, attackers have the upper hand during the weeks, months, or years it takes to close the window on vulnerabilities.

Virsec eliminates the risk posed by disclosed or undisclosed vulnerabilities being exploited during lengthy patching cycles. By mapping and monitoring actual code execution, Virsec Security Platform (VSP) instantly identifies when an application is about to be targeted and stops attacks in their tracks. VSP delivers precise **Compensating Security Controls** that eliminate the risks of vulnerabilities being used to abuse web applications, third-party code, and legacy systems.

Virsec Ensures

- *Automated protection from disclosed or undisclosed vulnerabilities*
- *Compensating Security Controls eliminating vulnerability risks during patching cycles*
- *Inline protection for vulnerabilities discovered during testing*
- *Runtime protection for undisclosed vulnerabilities and zero-day threats preventing exploits from executing*

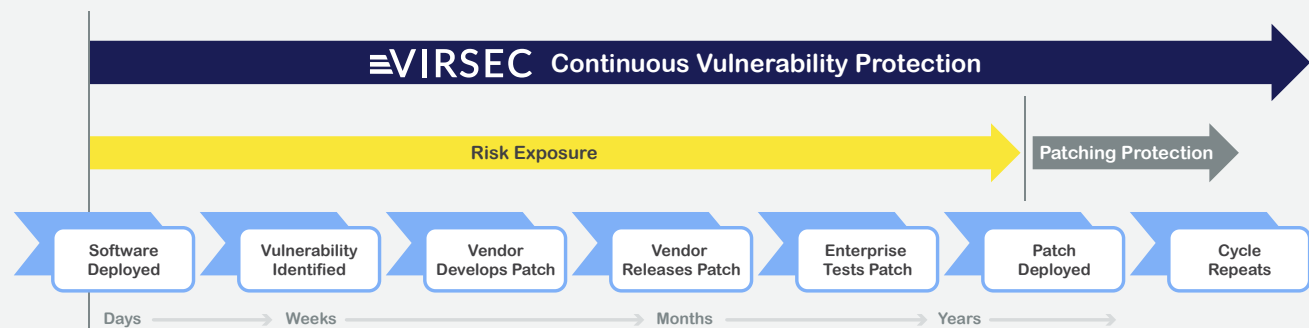
Reduce Cost and Risk

While patching is always challenging, the numbers of vulnerabilities that must be address has grown dramatically. The NIST National Vulnerability Database (NVD) tracks more than 20,000 vulnerabilities per year – a threefold increase in just three years. Meanwhile, according to the Verizon Data Breach Investigation Report, the average time for enterprises to remediate serious vulnerabilities is 4-6 months, while the cost to find and remediate a serious flaw can be over \$50K per incident. Faced with these challenges, businesses either have to hire huge teams of expensive experts, or ignore many vulnerabilities and keep their fingers crossed.

Continuous Vulnerability Protection

Virsec technology secures code from the inside based on specific mapping of proper application execution. Delivering compensating security controls during runtime, VSP ensures that unpatched or undisclosed vulnerabilities cannot be exploited. Virsec delivers both stronger defense and greater simplicity than solutions based on rules and policies.

Unlike signature-based solutions, VSP requires no prior insight into attack patterns or methods. Attacks on existing vulnerabilities, using familiar, uncommon or unknown exploits, are detected without ongoing expert monitoring and tuning. Security is provisioned once, at the code and memory level, so no matter what method or entry point an attacker uses, applications run only as intended. Virsec helps organizations reduce costs and minimize risk to high-value applications and industrial control systems by ensuring an effective defense against increasingly advanced application attacks – today and tomorrow.



Typical patching cycles and risk – with Virsec and without

Application-Aware Workload Protection

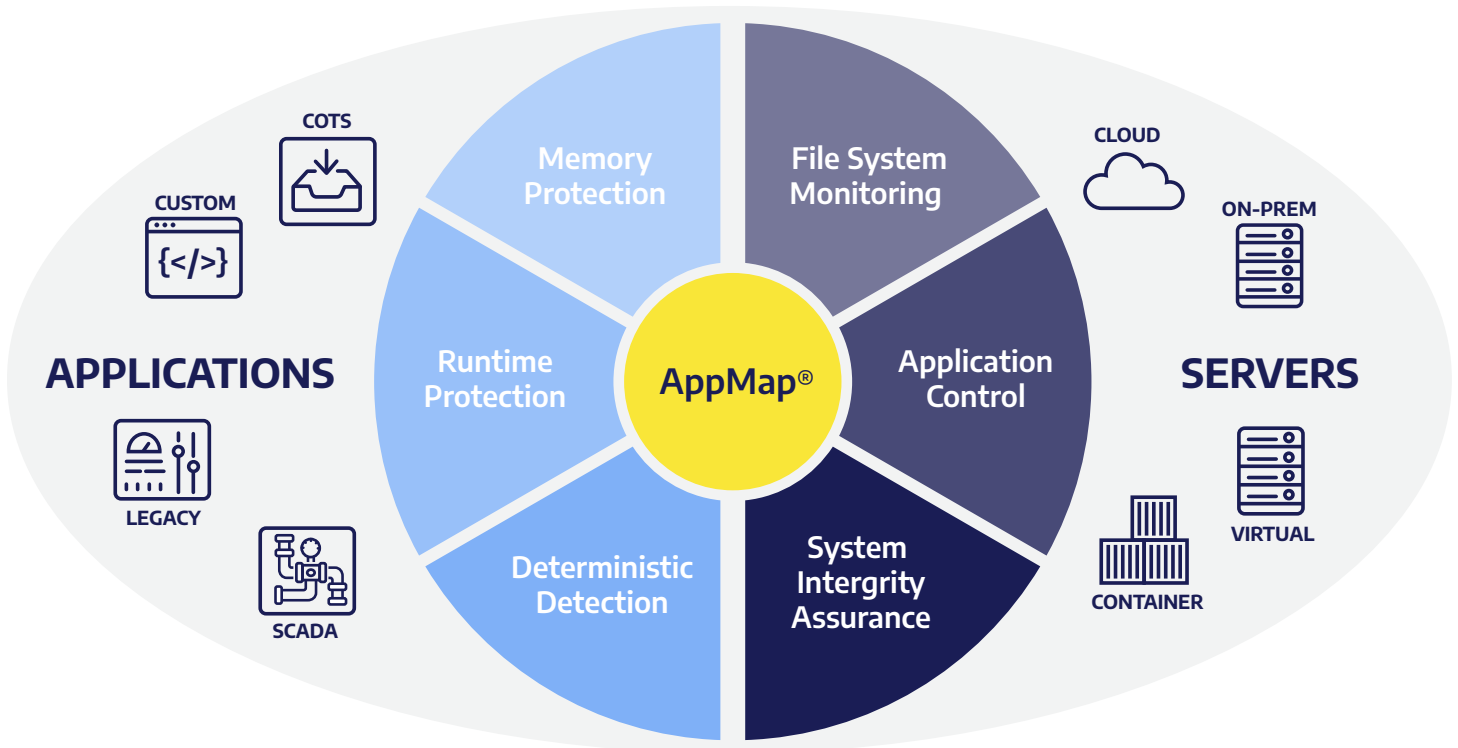
Virsec provides application-aware workload protection against the widest range of evasive cyberattacks – known and unknown – and secures applications from the inside. Virsec protects all your applications, including custom, COTS, third-party, legacy, SCADA and more. And the Virsec solution protects across any platform, including on-prem servers, virtual, cloud, hybrid, container, and edge.

ANYWHERE
On-prem, public/private cloud, hybrid, container

ANYTHING
Custom, legacy, COTS and air gapped applications

ANYTIME
Deploys in minutes, protects continuously in real-time

“Do not use an offering designed to protect end-user endpoints and expect it to provide adequate protection for server workloads.” Gartner





**Server &
Application
Workload
Protection**



**Application-
Aware Mapping
Technology**



**No Signatures,
No Tuning,
No Noise**



**Zero
Dwell Time**



**Full-Stack
Runtime
Protection**

Securing the World's Most Critical Applications

Virsec is deployed globally protecting mission-critical applications and infrastructure in industries including financial services, healthcare, government, defense, power, oil & gas, transportation, telco, technology, and more.

"Virsec virtually patches vulnerabilities in runtime, so nobody can exploit them."

Chief Security Architect, Schneider Electric

Recognition

