SOLUTION BRIEF

VIRSEC SECURITY PLATFORM

Application-Aware Workload Protection

Virsec changes the status quo in cybersecurity with breakthrough technology that protects critical application workloads from the inside against dangerous attacks that bypass conventional security. By combining deep application-awareness with automated runtime protection, Virsec instantly stops advanced attacks without prior knowledge across the entire attackable surface.

Extending Zero Trust to Workloads

Recent software supply chain attacks have exposed gaps in conventional security tools that require prior knowledge or look for clues after-the-fact. Virsec is the first solution to extend and automate zero trust security across the entire workload, ensuring that applications only execute as intended and are never derailed by malicious code.

Simply Better Security

Virsec delivers security that is far more effective, easier to manage, and simplifies compliance. Virsec's patented technology automatically maps acceptable execution across the entire workload, without learning, tuning, or signatures. Runtime detection instantly spots any deviations down to the memory level, and precisely stops attacks without the noise of false alerts.

VIRSEC

- *Stop advanced attacks without prior knowledge*
- *Guardrail applications during runtime at the memory level*
- *Protect the entire attackable surface in any environment*
- *Stop attacks at the first step and eliminate dwell time*
- *Precise results eliminate noise and lowers costs*
- *Automate protection without learning or tuning*

"Virsec understands what's happening to applications at runtime, making them self-defending against any vulnerabilities."

Enterprise Architect
Cisco

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

Application Awareness: Complete, Precise and Automated

Virsec protects precisely during runtime, because it understands the context of applications across multiple dimensions, at the host, web, and memory layers. Patented AppMap™ technology automatically extracts detailed knowledge and context across the entire application workload, providing unprecedented defense in-depth against advanced attacks and complex kill chains. This in-depth mapping includes detailed information on:

Packages: Decomposes application packages (RPM, MSI, SEAs) and extracts checksums to detect supply chain compromise at the earliest stage.

Libraries: Decomposes executables to find library dependencies, preventing memory injection attacks.

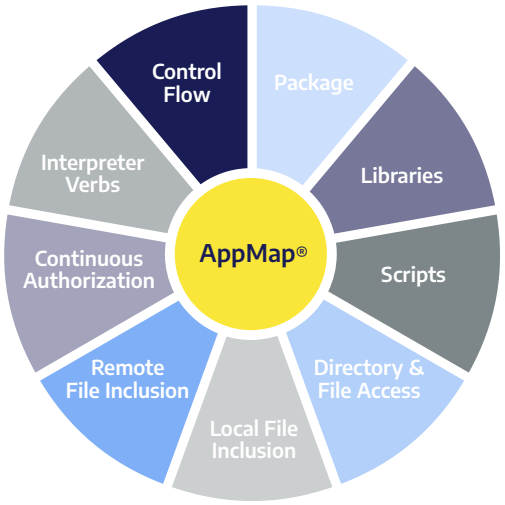
Scripts: Enumerates developer and Ops allowed/disallowed interpreter and script combinations preventing fileless malware attacks.

Directory & File Access: Enumerates files and directories that processes will access during runtime. This hardens the app and captures malicious access to critical code early.

Local File Inclusion: Captures directory paths and web roots for web apps. This prevents attacks from breaking out of jail and corrupting the environment of the app.

Remote File Inclusion: Captures permitted remote redirects. This prevents malicious code from being downloaded by end users.

Continuous Authorization: Assigns stronger authentication and authorization requirements for highly sensitive web application functionality.



Interpreter Verbs: Captures allowed syntax from a range of interpreters (SQL, JavaScript, OS Commands, and many more). This prevents OWASP Top 10 attacks that can lead into planting of backdoors and remote code execution exploits.

Control Flow: Extracts valid branches from binary code and enforces only developer provided branch transitions at runtime. This prevents attacks such as ROP gadgets, that lead to remote code execution attacks.

"When we deployed Virsec, we got immediate ROI. We instantly stopped new threats and got a clear view into our entire application surface." **Principal, Cybersecurity,** Broadcom

Automated Protection & Detailed Analytics

Armed with this deep application-awareness and runtime visibility, Virsec can instantly detect and stop deviations caused by attacks that are invisible to conventional security tools. Through an intuitive management console, admins can choose from a range of context-specific protection actions. Because the results are precise, and immediate, security teams can have the confidence to automatically stop attacks, without disrupting business from false alarms.

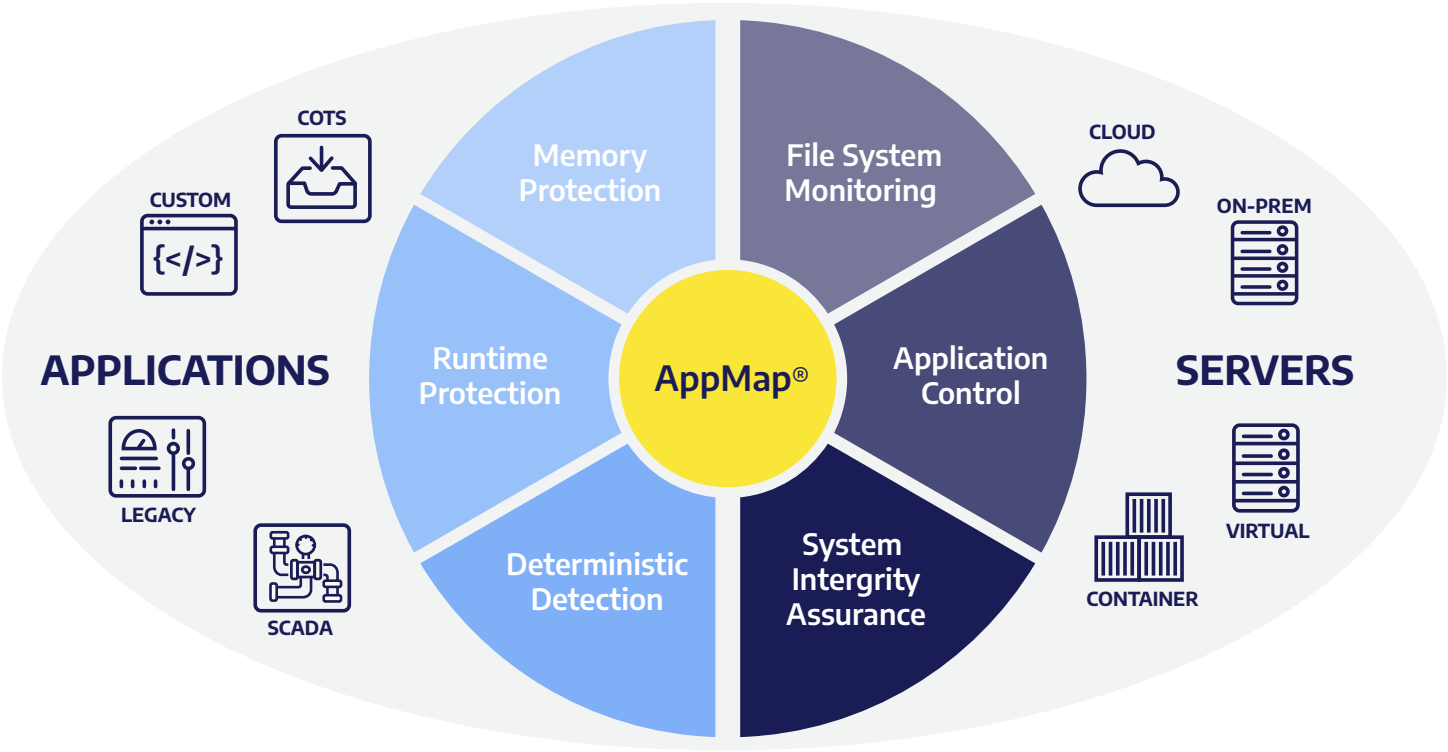
The solution also delivers detailed forensics on every incident, (including IP addresses, session ID, and details on the malicious HTTP requests and more) which can be integrated with SIEM systems.

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	ANYTHING	ANYTIME
On-prem, public/private cloud, hybrid, container	*Custom, legacy, COTS and air gapped applications*	*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.

Recognition

Partners & Customers