

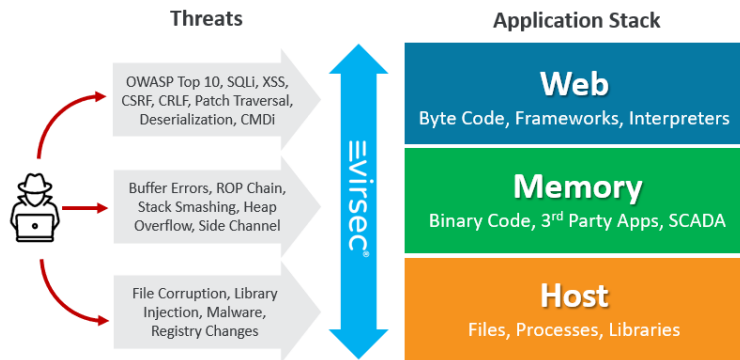
## Protecting Applications from the Inside

Virsec delivers a radically new approach to security, protecting enterprise applications from the inside against today's most dangerous cyberthreats. The Virsec Security Platform (VSP) definitively stops fileless and in-memory exploits that bypass conventional security, delivering unprecedented speed and accuracy, while eliminating false positives.

## Complete App-Stack Protection

Attackers are adept at finding vulnerabilities and they can easily bypass point solutions such as WAF, EPP and EDR that don't see the bigger picture.

**Virsec is the only vendor** to protect the entire attackable surface of the application including Web, Memory, and Host. VSP detects and stops the widest spectrum of attacks including OWASP Top 10, memory errors, library injections, process corruption, malware and much more.



## Memory Protection is “Mandatory”

Analyst firm Gartner\* states that memory protection is “mandatory” for workloads and recognizes Virsec for providing advanced capabilities. In fact, **Virsec is the only vendor** to integrate three core areas recommended by Gartner:

- **Application Control:** making sure only the right files, libraries and processes are allowed to run
- **System Integrity Assurance:** preventing critical processes from being corrupted or hijacked
- **Memory Protection:** stopping the most advanced attacks that derail applications during runtime

## Real Visibility Requires and Inside View

Almost all conventional security tries to protect from outside the application, guessing at the perimeter what might be bad, or looking for clues after attacks when damage has already been done. **Virsec is the first solution** that runs inside the memory perimeter protecting applications during runtime. This delivers unprecedented visibility, accuracy, and speed to stop attacks in their tracks.

## Patented AppMap™ Technology

In order to protect workloads, you need full knowledge and context into how applications will execute during runtime. Virsec's patented process automatically maps extensive details about acceptable files, processes, libraries, web input, memory usage, control flow and more. This comprehensive AppMap enables VSP to instantly detect deviations and guardrail applications – stopping attacks at the first step before damage occurs.

## Automated Protection Without Learning or Tuning

Virsec is ideally suited for security teams that need out-of-the-box protection, without learning, tuning, policy updates, heuristics, or signatures. VSP never requires source code, access to developers, or extensive application-specific expertise. The solution deploys easily in on-premises, hybrid, or cloud-based workloads and seamlessly integrates with existing network infrastructure and SIEMs.

## Protecting Critical Applications Across Industries

Because of Virsec's its unique technology and unprecedented results, VSP is being deployed globally to protect mission-critical applications and infrastructure in industries including financial services, healthcare, government, defense, power, oil & gas, transportation, technology and more. In all cases, Virsec provides front-line protection and definitive results across all stages of the attack kill chain.

\* Market Guide for Cloud Workload Protection Platforms, Gartner 2019