

USE CASE

FULL-STACK WORKLOAD PROTECTION

The world runs on software, yet, until now, there was never a way to achieve 100% protection of that software while it is running, wherever it is running. The only way to fully protect software is by fully mapping and understanding what it is supposed to do and immediately stopping what it is not. Virsec's Deterministic Protection Platform (DPP) eradicates software threats in real-time before they can cause any harm, making security response obsolete.

Runtime protection for workload makes cyberattacks irrelevant




Enterprise application workloads are becoming more granular, distributed, and complex. With thousands of workloads deployed across VMs, bare metal, containers, and serverless environments, security and risk management teams struggle to maintain consistent, accurate, and in-depth workload visibility and protection.

How equipped are you to protect your most vital workloads?

Many organizations find that implementing dynamic workload protection for ever-changing applications remains difficult. Existing security tools such as EDR/XDR/EPP/WAF are based around probabilistic methodologies that are founded on the principles of detection & response which cannot prevent attacks as they occur. They require manual human intervention which causes lengthy delays allowing for dwell-time & lack full protection capabilities. These legacy solutions responsive actions require analytics to establish application behavior baselines that are impossible to garner even with strong DevOps practices, AI capabilities, and real-time visibility across the infrastructure.

Although considered necessary for good hygiene and automation, controls rooted in indicators of compromise, that examine data outside of runtime leaves vital workloads at high risk.

CHALLENGES WITH COMMON WORKLOAD PROTECTION SOLUTIONS

 Visibility <i>Host</i> Legacy applications are often deployed in hybrid-cloud environments or ported to containers without keeping the same level of protection during runtime, regardless of the platform <i>Memory</i> Lack of in-depth visibility into the instruction execution cycle and control flow data <i>Web</i> Lack of visibility across the entire webserver leaves applications vulnerable, as file-less malware silently trespasses salient web systems and executes activities	 Detection <i>Host</i> Traditional EDR/XDR solutions discern deviations based on known threats/intelligence, but lack visibility into software during runtime <i>Memory</i> Lack of detection against advanced memory attacks with catastrophic consequences <i>Web</i> Common Web Application Firewalls (WAF) solutions have a lot of overhead & can often miss vulnerabilities from blind spots in the attack surface	 Response <i>Host</i> Resources must be allocated to comb through the numerous false positives and then analyzed for appropriate action <i>Memory</i> Lack of memory protections that automatically identifies invalid code jumps in memory and unauthorized actions <i>Web</i> Users experience supplied data interruptions that may result in the need for additional patches or dwell time
--	--	--

Comprehensive protection from inside the workload

Virsec provides a new means of protecting workloads with zero tolerance for risk, exposure, and resource overload. Our Deterministic Protection Platform™ ensures comprehensive protection across the entire software stack (web, host, and memory) at runtime as code executes. And it does so continuously throughout the production lifetime, without the need to establish behavior baselines from an ever-evolving application and stops attacks in real-time.

DPP uniquely delivers primary server workload protection controls including strict application allow-listing supplemented with advanced memory protection and breach prevention capabilities that harden software wherever it's deployed. Our proven technology is the only solution to protect against exploits targeting vulnerabilities in application or trusted processes and threats built entirely in memory. Modern web security requires a deeper level of web defense that is more precise. DPP is the only solution with built-in web protection to accurately counter complex web attacks that challenge external rule-based filtering, Data Loss Prevention, anti-malware, and bot defense services. DPP offers rich capabilities to defend against the broadest range of attacks at the web, host and memory layers, with unprecedented precision as exploits unfold early in the attack sequence, so dangerous attacks never execute.

Deterministic Protection Platform (DPP)



Virsec Host Protection



Virsec Web Protection






Virsec Memory Protection

DPP delivers solid protection

wherever your applications live

Deterministic protection capabilities delivered by Virsec cover web, host, and memory with a contextual understanding of the underlying business logic and the expected application execution flow, stopping in real-time and with precision even the most advanced attacks across the entire application attack surface.

 <p>Complete visibility</p> <p>Maps application and expected runtime behavior in minutes then monitors execution as code executes</p>	 <p>Reliability and integrity</p> <p>Guards process memory and process flow to ensure no malicious code executes and services run as intended</p>	 <p>Continuous Protection</p> <p>Automated defensive action that stops known and never-before-seen attacks in milliseconds automatically without human effort</p>
--	--	--

Protect in True Runtime

With our platform runtime protection is more than information characterizing the workload or container's runtime information and all events logged. Runtime is the essence of deep visibility and control across the software stack as it executes delivering 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, as delivered in our Virsec Host Protection solution. With activation of Virsec Host Protection capabilities, you gain the foundation for achieving 100% application protection.

Prevent dangerous exploits from escalating

Deterministic Protection Platform delivers the most effective controls capable of shielding unpatched vulnerabilities and safeguarding files, executables, processes, libraries, kernel commands that allow attacks to build evasively in the core of the system as code executes. 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 renders attacks like PrintNightmare, or those which affect supply chains, target known and yet-to-be discovered CVE's or give way to remote code executions obsolete, so applications only execute as intended and never give up data and execute malicious transactions.

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 capabilities for advanced web application protection and precise zero-day defense. Optimizes your line of sight and control while reducing the impact of threats throughout your workload environment.

- Reduce SecOps cost with Virsec's Deterministic Protection Platform
- Eliminate alert exhaustion with zero false positives and real-time threat analytics
- Compliment Zero Trust identity protection that covers endpoint devices and user access by guard-railing applications during runtime
- Protect where WAF, IPS XDR, & EDR fail to protect against injection attacks & script exploits
- Reduce risk with protection against OWASP top 10 and MITRE top 25 most dangerous attacks
- Meet stringent compliance standards like, PCI, FISMA, HIPAA, NIST Cybersecurity Framework
- Utilize extensive forensic data and actionable insights for regulatory reporting
- Secure the entire software stack deployed on-premises, in the Cloud, containers, and VMs allowing you to use open-source, legacy applications and other components without risk

Learn more| [Click here](#) for more information about workload protection with Virsec Host Protection by Virsec