USE CASE

Remote Code Execution (RCE)

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.

Protection when seconds matter against Remote Code Execution

Challenge:

Conventional security tools can secure some IT infrastructure, but not all. WAFs, firewalls, endpoint detection, and response are essential, but what happens if the attackers are already in the system? Most of our legacy security focuses on the perimeter, and NIST implores us to assume the attackers are already inside the network. Many security teams concentrate on network protection and authorization, but the most dangerous attacks, such as Remote Code Execution (RCE), are executed undetected at the memory layer. Other technologies such as host-based IPS (HIPS), app control, and server endpoint suites have significant limitations against memory-based attacks. They tend to produce large quantities of false positives. File allow-listing is gaining popularity but can miss memory-based attacks that hijack legitimate applications that have been specifically allowed to run in the system.

Furthermore, threat hunting tools and artificial intelligence (AI) require prior knowledge of a given threat fingerprint and overlook an unknown threat hiding in plain sight. As a result, RCE attacks will continue unabated because our existing security tools are ineffective against them. Many conventional security vendors will have you believe that your adversary is repeatedly using the same techniques. This is a dangerous misconception. Organizations must assume that adversaries are well-funded, highly skilled, motivated, and effective. They will continue to create never-before-seen attack techniques, and they will keep hitting systems, whether you're ready or not. The most successful attacks are happening during runtime, and therefore we need complete software protection during runtime.

Solution:

Virsec Deterministic Protection Platform (DPP) approach to security is to protect the application itself, placing guardrails around its code as it executes during runtime. DPP maps all acceptable files, processes, libraries, input, container images, and memory usage associated with all application workloads in any environment. This fully automated process ensures that any deviation from normal is instantly detected, treated as a threat, and blocked. Rather than trying to blacklist everything that is possibly *bad*, DPP enforces *good* through a zero-trust approach – ensuring that applications never get derailed, regardless of threats, vulnerabilities, or patch status. DPP provides unparalleled in-memory and runtime protection and can detect and stop evasive attacks like RCEs within milliseconds, with zero-dwell time.

Ensure Zero Trust where it matters most

Even with existing Zero Trust practices and the best SOC strategy, never assume enough defenses are in place to secure running applications on a protected Host. Exploits now hijack control during runtime with remote code execution (RCE), and open persistent backdoors into critical systems. Concentrating trust and validation inside the workload stops advanced threats that bypass traditional zero-trust controls, turning benign inputs into malicious code, and derail software as it executes, at the memory level.

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.

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

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. Running applications have become the most prominent security battleground. Most security tools protect before or after code execution, but not during execution. These tools have no visibility or control into the application runtime. Therefore, threat actors exploit this lack of protection with remote code execution exploits, advanced fileless attacks, and other evasive memory-based attacks.

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. DPP ensures application integrity at the file level with application-aware control and file integrity monitoring, providing true runtime protection. Patented AppMap® technology maps acceptable files, processes, libraries, web input, memory usage, control flow and more. DPP instantly detects and stops any deviations, preventing attacks at the first step before damage occurs.

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

virsec™