USE CASE

Zero Trust Execution

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.

Reach beyond identity and access with zero-trust execution

Challenge:

Zero Trust doesn't go deep enough to stop today's advanced attacks. With vulnerable workloads and applications distributed on-premises and in the cloud and accessed by users from various devices, organizations remain highly exposed to risks they can't address by conventional zero trust enforcement of per-request access and identity decisions in the face of a network viewed as compromised.

Solution:

Unlike traditional Zero-Trust solutions who focus solely on IAM, Virsec Deterministic Protection Platform (DPP) assumes threat actors have arrived on the host server to execute malicious activity using validated requests, data, and components at runtime. DPP applies a 'never trust, always validate' approach to application runtime, delivering the tightest control on software components and solid protection against evasive attacks that weaponize the same. It uniquely maps the entire software stack as applications load to discern how systems should execute, and protections on deviations automatically initiate in milliseconds. Only DPP enables organizations to continuously validate files, processes, process flow, and memory usages automatically as throughout the runtime cycle for zero trust execution that erases risk and simplifies security.

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.

Trust no code during Execution

With applications in a running state, attackers can gain persistent control, and cause arbitrary code to execute in the workload. It's critical that the Zero Trust model be applied to data inputs & activated confirmed processes so that applications do not blindly trust runtime elements that can be corrupted into malicious code.

DPP capabilities are designed to address the trust gap in vulnerable applications and is the only solution that can detect during runtime when an attacker attempts to misuse libraries, files, scripts, executables as it is running in a presumed trusted state. DPP, explicitly verifies all software components across the full application stack and how they are leveraged with each transaction/request, so code is executing only as intended, and any attempt to deviate from legitimately controlled flows is immediately recognized as a breach and stopped.

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

virsec™

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