Deterministic Protection Platform

Fully Automated Protection Across Your Server Workloads

The world runs on software, yet, until now, there was never a way to achieve precise protection for software while it is running, wherever it is running. Virsec's Deterministic Protection Platform (DPP) precisely maps what software is intended to do and stops attacks instantly in real-time before they can cause any harm, making security response obsolete. Take the guesswork out of server protection, stop reacting to alerts, and start preventing breaches.

Why do you need Deterministic Protection?

Cyber-attacks have become increasingly complex where actors exploit systems at the core to obtain control of server workloads - bypassing traditional security solutions for their own gain. Conventional security solutions are probabilistic in their approach as they rely on heuristics or AI to “guess” if an attack has occurred, typically by analyzing logs days after an incident. As a result, breaches keep happening, with attacker dwell times averaging almost seven days. Additionally, these tools generate hundreds of false positive alerts - overwhelming precious security resources with having to investigate and respond to each one.

Organizations are demanding a deeper and more effective layer of protection with a direct line of sight into all software code, composite workloads, and components during runtime. Enterprises need to defend and protect against any known and unknown vulnerability with precision as events unfold (without guessing).

Deterministic Protection Platform by Virsec

Deterministic Protection Platform (DPP) by Virsec is the only security solution that ensures precise protection against zero-day and evolving attacks to workloads deployed in production. DPP automatically maps what each software component is supposed to do and instantly stops any deviations instantly. DPP reduces threat actor dwell-time from minutes to milliseconds, protects unpatched systems both known and unknown attacks with true runtime observability, generates zero false positives, and enables massive operational costs savings. DPP uniquely protects the full software stack across the host, memory, and web layers.

Deterministic Protection Platform (DPP)

DPP packages three key elements that harden the software stack and continuously ensure integrity and reliability

Host Protection

Hardens applications from the inside with AppMap™ technology, monitoring runtime elements and leveraging strict application controls to prevent even a single instruction from any unauthorized executables, libraries, and scripts from executing

Memory Protection

Automatically maps and secures process memory to ensure that apps only run as intended and malicious code can’t execute

Web Protection

Protects from the inside for a truly self-defending platform that counters events bypassing firewalls

Principles of Deterministic Protection

Secure Your Workloads

Re-defines cybersecurity with breakthrough technology that protects server workloads from within by ensuring the correct execution of all software components. DPP prevents dangerous attacks.

No Patching, No Problem

Provides coverage where conventional solutions fail. Unique DPP technology detects advanced attacks at the web, host, and memory levels that bypass X/EDR, WAF, IDPS, EDR, EPP, AV known patched/unpatched vulnerabilities and those yet to be discovered.

Full-Stack Server Protection

Uniquely secures the entire application surface during runtime across Windows and Linux operating systems to automatically protect vulnerable workloads, application components, filesystems, processes, and memory that present a risk

True Runtime Defense

With its read-only approach to mapping the software workload, DPP detects and stops attacks during execution, providing true protection without affecting performance or causing harm to your applications. No access to code or prior knowledge required.

Key Benefits

- Protect against advanced threats – Detect and defend against Zero-Day attacks in milliseconds
- Maximize ROI up to 70% OPEX Savings
- Automate runtime protection on any server workload and in any workload environment
- Gain insights into all software components from inside the application stack for true runtime visibility
- Achieve full-stack server protection with little to no impact on performance

DPP is uniquely designed to prevent cybercriminals' efforts to set up attacks, execute scripts/code, and gain free reign over server environments by exploiting hosted applications. Threats that bypass existing security controls can be countered with trusted precision at any stage in the attack sequence, so attackers do not benefit from delayed security efforts.

Strict controls deliver precise attack detection that enables you to tailor protective action, like un-injecting an illicit library, quarantining suspicious files, and restoring originals. Unlike typical solutions that enable threats to progress as various incidents are evaluated or precedence is established, DPP ensures early attack eradication for zero attacker dwell-time without affecting system operations.

Continuous protection against the most dangerous attacks

Ransomware

Zero days

Injection Attacks

Remote Code Execution

Promise of Deterministic Protection

Precise Protection

DPP focuses on true server workload protection that detects and stops attacks in real-time with complete visibility and contextual awareness. It distinguishes system exploits from benign system events and stops attacks during execution to prevent data theft, service disruption, and financial losses. DPP is the only solution to ensure full integrity across all runtime elements of the workload preventing remote code execution (RCE), supply chain and web attacks, by ensuring applications execute as intended and can never be altered by malicious code.

Operational Savings

Security teams deploying DPP have experienced tremendous OPEX savings by up to 70%[1] and increased time to focus on business innovation versus the hassle of monitoring suspicious events, hunting out threats, investigating results, and reacting to thousands of false alerts daily. DPP consolidates several security tools (WAF, AV, allow-listing) and unifies protection for workloads deployed in containers, clouds, and VMs (virtual machines), shrinking the security footprint within a single installation while delivering accuracy in protection and no false positives. The intuitive UI maximizes usability and accelerates deployment and protection at scale.

Continuous Compliance

DPP relieves stress from compliance-mandated patching fire-drills and employee turnover. It’s a well-known fact that unprotected workloads that are accessible on the Internet will be attacked in less than seven minutes. In 2021, over 5,800 remotely exploitable vulnerabilities in applications were disclosed. It is safe to say that most organizations cannot patch these vulnerabilities in sub-seven minutes after disclosure.

Like a GPS protects a driver from going off course, Virsec’s DPP solution automatically ensures that an application riddled with vulnerabilities cannot be exploited. This means enterprises utilizing DPP can easily meet (the otherwise very burdensome) “flaw remediation” compliance requirements. DPP meets the requirements of a broad set of Cyber Security Framework control requirements such as FISMA, NIST 800-53, NIST 800-171, HIPAA, and others.

[1] 70% based on application infrastructure and scale

Meeting Your Business Needs

Full Stack Workload Protection

Full-stack workload protection with DPP uniquely centers on the software stack, not the infrastructure where the application resides, interfaces, systems on the network, traffic, client devices, and external intelligence factors outside the application runtime. DPP precisely detects attacks (without false alerts) that are difficult to identify with legacy security, regardless of threat granularity, duration, or locality.

Legacy Application Security

Embracing digital transformation while retaining legacy systems doesn't have to come at a cost or pose a significant risk to the organization. Deterministic protection capabilities continuously address vulnerabilities in Windows and Linux-based software, even those which are no longer supported and left unpatched. DPP provides protection without tuning, prior knowledge, or access to code.

Organizations can now easily maintain strict change management for legacy systems, prevent malware from building on the system, and stop attacks targeting binaries or infecting processes in runtime. Furthermore, the automated runtime protection capabilities enforce full-coverage protection to secure legacy systems even through migration to newer modern technology needed to drive the business forward.

Real Security Automation

The essence of security automation stems from the notion that resolving complexities in application security requires the power of programmatic detection, investigation, and remediation of cyber threats. However, much of today's automation remains reliant upon time-consuming and costly manual human intervention. DPP delivers continuous hands-off protection with increased effectiveness and coverage without human intervention. With its read-only approach to mapping the software workload, DPP does not harm your applications while providing true protection without slowing them down.

Protection in the Cloud for Containers and VMs

DPP embraces a cloud-first strategy without concerns for heightened risks and security complexities. It integrates seamlessly with DevOps, DevSecOps, and CI/CD pipelines for secure code development, drift prevention, and assurance that applications are deployed to the cloud are protected. DPP instantly reduces the attack surface and protects against the most evasive attacks that may compromise Kubernetes environments, containers, or VMs. Whether deploying in cloud environments like Amazon Web Services, Google Cloud Platform, or Microsoft Azure, you can experience the same depth of visibility and full-stack protection afforded on-premises without additional skill requirements or shifting expertise to an MDR/MSSP. Furthermore, DPP enables organizations to unify security capabilities central to cloud runtime protection within a single platform instead of relying on solutions that add more complexity to protecting cloud deployments regardless of infrastructure demands.

- Unifies visibility across all private, public, and hybrid cloud environments
- Defends against cloud breaches and unifies security for multi-cloud deployments
- Provides a runtime-focused approach that automates attack discovery and protection that stops attacks without human involvement

- Protects the entire application stack across the web tier, host, and memory
- Continuously monitors execution workflows and stops threats and attacks at the earliest point in the attack chain
- Automates security and ensures best-practice implementation continuously

Increased Risk Visibility

DPP provides continuous deep visibility into the core workings of running workloads, container images, and serverless environments by capturing security data points during runtime execution for a frontline view. Once DPP is deployed it protects your workloads and provides SecOps with a dashboard that accurately depicts suspicious behavior within software systems (from the inside) at the time of an attack. DPP focuses visibility across intrinsic software elements to magnify observation beyond external factors like connections, assailants, and network infrastructure provided with other solutions. As DPP stops attacks, it also captures detailed forensics that can be used to precisely pinpoint the nature of the threat event such as its origin, potential blast radius, potential business impact, and the code involved. DPP is the only security solution that has complete visibility across all runtime components that make up an application workload and, in parallel, counterattacks as they happen – eliminating the attack surface.

Reduced Operation Workflows

DPP simplifies the operational reality of IT security and the tools essential to the effort, automating key aspects of workflows to reduce overhead, and integrating with technologies to maximize the value of SOC components while maintaining protection in real-time to prevent dangerous events and avert risk.

Upon initial use, teams are freed from the complexities of security operations with protection automation that allows your team to focus more on achieving overall enterprise goals.

- Eliminates efforts involved in creating and maintaining operational policies and rules that are common to other solutions
- Eliminates time spent on alert triage, incident investigation, and remediation of affected systems
- Purpose-built to protect complex systems and scales to your current security operations

Continuous protection against the most dangerous attacks

Learn more

To learn more about Deterministic Protection Platform by Virsec, visit us: www.Virsec.-com

virsec™