Deterministic Protection Platform

A COMPLETE DETERMINISTIC SECURITY APPROACH FOR THE ENTERPRISE

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.

Why do you need Deterministic Protection?

Cyber-attacks have become increasingly complex where actors exploit systems at the core to obtain control of software, applications, & workloads - bypassing traditional security solutions for their own gain. Organizations are demanding a deeper layer of protection with a direct line of sight into all software code, composite workloads, and components during runtime to defend and protect against any known and unknown vulnerability with precision, deterministically, as events unfold without guessing.

Deterministic Protection Platform by Virsec

Deterministic Protection Platform (DPP) by Virsec is the only security product that ensures better protection against zero-days, evolving attacks and known and unknown threats to workloads deployed in production. No matter the type of application, environment, or attack method employed, DPP ensures full-stack software protection continuously while it is running, wherever it is running. It instantly reduces threat actor dwell-time from minutes to milliseconds, with true runtime observability and precise protection that ensures application integrity and reliability. Unlike other solutions, DPP precisely determines what your software is supposed to do and stops it from doing what it is not. The app-aware focus delivers deterministic protection that stops threats earlier and prevents the rise of the most dangerous events. With DPP, organizations quickly achieve 100% protection before an attack can cause any damage, erasing risk from the applications and workloads most vital to the business.

Deterministic Protection Platform

DPP Packages three key elements that harden the software stack and continually ensure integrity and reliability

Host Protection

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

Memory Protection

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

Web Protection

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

virsec™

Principles of Deterministic Protection

Secure Your Workloads

Redefines cybersecurity with breakthrough technology that protects software application workloads from within by ensuring the correct execution of all software components. DPP prevents dangerous attacks

Full-Stack Protection

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

No Patching, No problem

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

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.

Key Benefits

- Complete software workload protection across the entire stack
- Guardrails applications during runtime at the memory level to stop the most fatal attacks
- Protects workloads residing in public and private clouds whether in VM's or containers
- Full visibility on all software components and processes from inside the application stack.
- Enables scalability through advanced automation for continuous compliance

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. Using a deterministic detection approach, combined with pre-defined protective actions, threats that bypass existing security controls can be countered with precision at any stage in the attack sequence, so assailants do not benefit from delayed security efforts.

Strict controls deliver precise attack detection that allows 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 the system operation.

Continual protection against the most dangerous attacks

- Ransomware
- Zero days
- Injection Attacks
- Remote Code Execution

virsec

Promise of Deterministic Protection

Precise Protection

DPP focuses on application protection that counters attacks that have reached the server as applications run and 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. With application-aware workload protection in runtime, achieve zero attack dwell time, eliminate risk, and close the door to cyberattacks that threaten legacy and modern applications. DPP is the only solution to ensure full integrity across all runtime elements of the workload, preventing remote code execution and providing applications execute as intended and can never be altered by malicious code.

Operational Savings

Security teams deploying DPP have experienced tremendous OPEX savings by as much as 70%[1] and increased time to focus on business innovation versus managing the rigors of monitoring suspicious events, hunting out threats, investigating results, tuning protections, and reacting to 1000's alerts daily. DPP consolidates several security tools (WAF, AV, Allowlisting) and unifies protection for workloads deployed in containers, the cloud and VMs, 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. Furthermore, the zero-touch instrumentation and continuous protection minimize daily operational expenditures in ways that reduce end-user expenses and while lowering the spend on MDR/MSSP and eliminating downtime due to threats by proactively addressing malicious events before they cause damage.

Continual Compliance

Complying with standards and requirements on a continuum to face off changing attack patterns challenges many organizations. Implementing recommended and necessary security controls is often a slow and arduous task, causing critical systems to remain highly vulnerable for extended periods.

DPP delivers audit-ready protection that continually addresses specific NIST regulatory requirements to ensure cyber resilience and compliance without interruption. The rich compensating controls easily minimize risk to complex systems, un-patchable legacy technologies vulnerable to threats, and where no remediation method previously existed. The continuous security controls identify and remediate unseen software risks by shielding known and unknown vulnerabilities to protect against evolving threats during runtime without human effort. Controls remain in place even as new vulnerabilities emerge.

Only DPP maintains a clear line of sight into the entire application stack, including interpreted code, compiled applications, libraries, interpreter responses, and database interactions to sustain the effectiveness of compensating controls and maintain compliance with NIST requirements on a continuum.

[1] 70% based on application infrastructure and scale.

Meeting Your Business Needs

Full Stack Workload Protection

Full-stack 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 continually observes runtime components comprising the software package on the host, in memory, and throughout the data flow for the duration of the running software processes execution, for full-stack coverage with contextual understanding. 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 known and unknown vulnerabilities in Windows and Linux-based software, even that which is no longer supported and left unpatched. Now, IT is no longer left to find individuals with enough expertise to develop custom fixes to address troublesome vulnerabilities in technologies that have been replaced or put to rest by vendors. DPP provides protection that makes age inconsequential 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 zero-day attacks targeting binaries or infecting processes in runtime without prior knowledge, learning, or access to source code. 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 remain reliant upon time-consuming and costly manual human intervention. DPP delivers continuous hands-off protection with increased effectiveness and coverage without human intervention. DPP simplifies operations and drastically reduces overhead costs. Its patented technology automatically maintains visibility throughout the execution of the software workload detecting threats deterministically without learning, tuning, or signatures. 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

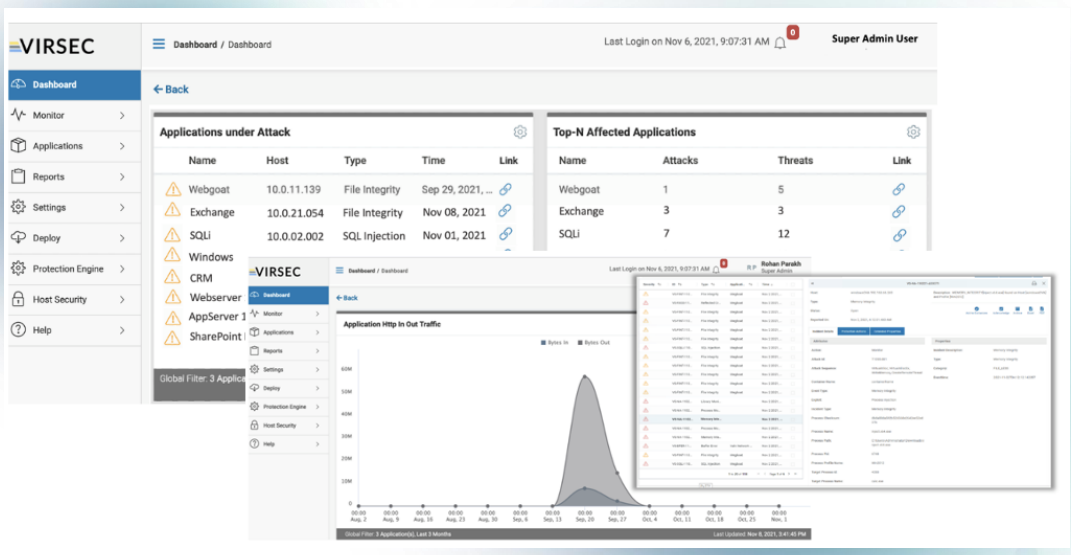
DPP makes it easy to embrace a cloud-first strategy without concerns for heightened risk and security complexities. It integrates seamlessly with DevOps, DevSecOps, and CI/CD pipelines for secure code development, drift prevention, and assurance that applications are deployed to the cloud protected.

DPP applies a deterministic approach to threat detection that 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, and 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 allows organizations to unify security capabilities central to cloud runtime protection within one 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 attacks discovery and protection that stops attacks without human involvement.
- Protects the entire application stack across the web tier, the host, and memory.
- Continuously monitors execution workflows and stops threats and attacks at the earliest point in the attack chain.
- Automates security and eliminates manual tuning, ensuring best-practice implementation continuously.

Increased Risk Visibility

DPP provides continuous deep visibility into core workings of running workloads, container images, and serverless environments by capturing security data points runtime execution for a frontline view inside running applications under attack. Once DPP is deployed it protects your workloads & provides SecOps with a dashboard that accurately depicts nefarious attempts and 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 seen below. 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 range, potential business impact, and the code involved. And all without complex human analysis.



With DPP, applications, services, and data are less in jeopardy because it precisely pinpoints the threat and stops it within milliseconds. DPP is the only security solution that has complete visibility across all runtime components that make up an application workload an DPP provides continuous deep visibility into core workings of running workloads, container images, and serverless environments by capturing security data points runtime execution for a frontline view inside running applications under attack. Once DPP is deployed it protects your workloads & provides SecOps with a dashboard that accurately depicts nefarious attempts and 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 seen below. 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 range, potential business impact, and the code involved. And all without complex human analysis.

With DPP, applications, services, and data are less in jeopardy because it precisely pinpoints the threat and stops it within milliseconds. 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 efforts, 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 advert risk.

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

- Eliminates a multitude of efforts involved in creating and maintaining operational policies and rules that are common with other solutions.
- Eliminates time spent on incident investigation and remediation of affected systems.
- Purpose-built to protect complex systems and scale your current security operations.

Continual protection against the most dangerous attacks

EDR | Intelligence | Investigation | User Behavior Monitoring | Log Analysis | Hunting

Learn more

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