USE CASE

Legacy 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.

Secure outdated Windows and Linux Servers™

Updating security for legacy systems that host applications controlling vital business processes is often complex, slow, can be very costly, disruptive, & impossible in some cases. But it does not have to be with a runtime protection solution, like Deterministic Protection Platform (DPP) by Virsec. DPP removes the complexity of securing legacy applications and erases the associated risk of utilizing old technology by ensuring continuous protection. Minimizing risk and averting attacks targeting legacy systems in a world of increasing cyber threats raises concerns where vital data may be in jeopardy. Many organizations attempt to strengthen security by adhering to common best practices *(i.e., monitoring logs, network activity, and permissions)* and wrapping older applications inside a protective bubble secured by hardware-enforced isolation to minimize risk. However, this approach is not enough to prevent more sophisticated attacks. Even if your organization is making progress in patching legacy systems still supported by vendors, there often remains thousands of applications and varying workloads posing an imminent security risk that remains unresolved, especially within expansive infrastructures with thousands of known vulnerabilities.

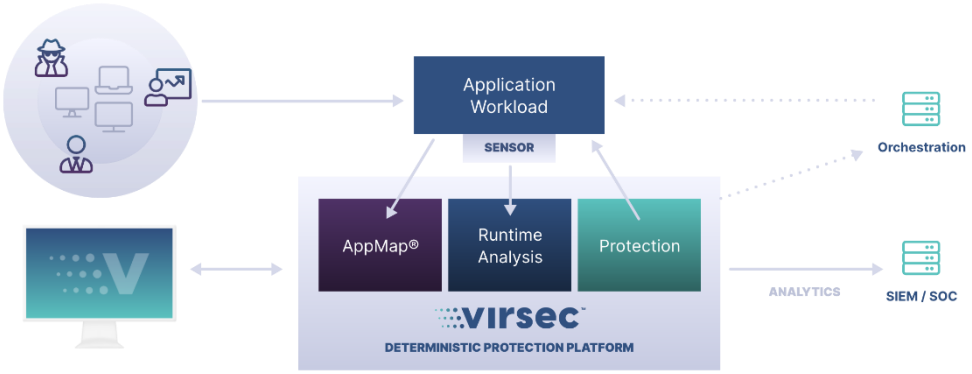
Where patching is not viable or too difficult to accomplish, organizations accept the risk without immediate remediation as they look to upgrade the business system sometime in the future. With DPP, organizations can do just that with the assurance that protection is in place for legacy application workloads that expose the business to risk and even for the replacement technology they are upgrading to in the future.

Virsec Allows you to Easily Overcome Concerning Security Challenges:

- Legacy applications were written when application security was simple or non-existent
- New vulnerabilities and the sophistication of attack method continuously evolves, reaching voluminous levels
- Vendors have gone out of business, support has slowed or ceased with obsolescence
- Expertise to develop software patches or address software errors has become specialized and costly to maintain
- Digital transformation is an arduous process taking months or years to complete as risk remains.

Deterministic Protection Platform by Virsec

With a first-principles approach to protection, the Deterministic Protection Platform (DPP) by Virsec automatically maps what your applications are supposed to do, then stops any deviations in milliseconds, preventing attackers from leveraging vulnerabilities to take control and run malicious code. DPP is a proven technology that enables leading government and commercial organizations worldwide to protect the legacy and proprietary software essential to business at runtime against ransomware and other known and unknown threats before there is business impact. It further reduces overall security costs and ensures continual compliance even where applications have outlived the intended life span.



Solid Protection for Legacy Applications

Harden Legacy Host Systems and Services on The Inside

Unlike common workload protection solutions, DPP establishes a foundation for achieving 100% application protection with continuous runtime protection. DPP provides deep visibility and control across the runtime infrastructure and 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.

DPP uniquely focuses security with the host application delivering zero-touch protection against attacks that bypass traditional tools and efforts without code changes

Implement Evasive Memory Exploit Protection

With DPP, organizations can continuously address the most devastating and difficult-to-detect adversary tactics built entirely in memory out of view of most security tools. Advanced runtime memory protection automatically identifies evasive injections driving memory access, malicious inputs, and unauthorized code execution so that attacks cannot be concealed inside benign processes. Furthermore, there is assurance that no data or information loaded will harm the application process flow. These advanced capabilities activate from a single click on the Host profile. It is not dependent on software development tooling, reputation, probabilistic heuristics, or signature updates, allowing you to activate frictionless defenses in minutes and without ongoing tuning or policy updates.

Protect the Full Software Stack in True Runtime

Deterministic Protection Platform allows you to protect applications running in **Windows Server 2008, 2019, and 2012 with strict application controls and runtime behavioral sequence analysis.** It covers vulnerabilities exposed due to the time between patching and will **act as a patch-bridge for Windows Server between upgrades.** The implementation will continuously protect the entire software stack across all runtime components, including files, executables, processes, libraries, kernel commands that allow attacks to build in memory as systems execute. 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 that affect supply chains.

Free IT Resources of Remedial Tasks

Additionally, all businesses using legacy systems are commonly advised to invest in different layers of security, including endpoint solutions, network-based IPS, proxy solutions, and a solution for email security. These solutions in themselves are not foolproof. Eternal Blue, WannaCry, Ransomware, and other malicious tactics have been compromised. Virsec adds a layer of protection on the server to enforce defense where common solutions fail and reduce the need or resources to perform common actions taken to maintain your security framework across an array of systems.

DPP minimizes risk even when the following tasks are not maintained or ineffective.

- Conduct a vulnerability assessment to identify weaknesses & what needs fixing
- Remove any unused applications and services.
- Create rules and policies to help securely govern your system.
- Configure and update your operating system securely.
- Ensure your antivirus solution is up to date where support is still offered.
- Maintain layer 5 and 7 network-level attack defenses, including host-based intrusion prevention software policies and application firewall

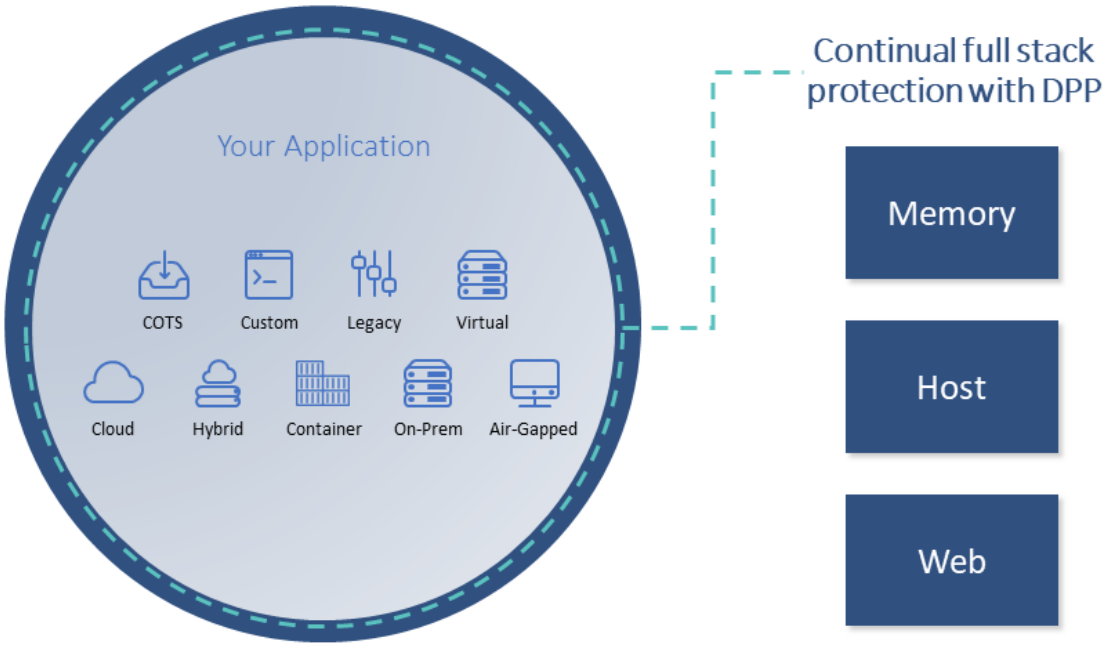
We know that upgrading infrastructure devices is a big undertaking and, in some cases, requires network downtime. However, the costs of ignoring the problem of aging infrastructure and running legacy protocols can run much higher. With DPP, organizations have successfully mitigated the attacks without downtime, zero-touch automation, and no false positives to reduce costs of protection assurance for vital systems and data.

virsec

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 advanced web application protection capabilities 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 legacy workload protection