USE CASE

APPLICATION CONTROL

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.

Ensure your applications always executes as intended

With global organizations facing ever-increasing evasive cyberattacks in the form of more sophisticated ransomware and vulnerability exploitation comes a stronger focus on application controls. These controls must ensure that only good software can run and only the intended way. Cyber actors evolved their exploits and malicious tactics to disguise their activities within trusted system attributes. So, to truly protect host-centric applications, application control systems must evolve to not only control what executes in a given system but also how it executes. This requires much deeper visibility over the application runtime that was not available in the market until Virsec's Deterministic Protection Platform (DPP).

Key Features

- Application control
- File integrity monitoring
- Process Monitoring
- Script control
- Advanced Memory protection
- Reputation services

Today, enterprises and government agencies are looking for next-generation application controls that can protect their environment against the most evasive types of file-based and fileless attacks, ensuring trusted software processes data as intended even when vulnerabilities are unknown or remain unpatched.

Strengthen Application Controls Protecting Vital Software

- Ensure trusted applications run as intended
- Block unwanted and undesirable software
- Defend against invisible exploits weaponizing trusted code
- Remove ill-suited passive monitoring tools like anti-virus
- Simplify the complexity of generating and maintaining allow lists
- Eliminate requirements for expert services
- Enable robust protection for evolving attacks & zero-days

Activate Strict Application Controls

With Vireces's ***Deterministic Protection Platform (DPP)***, application control becomes a strong and precise line of defense for core enterprise systems, mission-critical software, and single-purpose workloads. DPP's rich capabilities combine dynamic application controls (allow-listing), memory protection, script controls, and library and filesystem monitoring to lock down server workloads and impose advanced exploit mitigation that confines running applications to good behavior. Utilizing granular security policies, only verified executable files, processes, and scripts can run on protected systems. Any other file or process cannot execute, even if a file is known-good. As a result, no zero-day malware can even start to execute when application controls are in effect. Virsec delivers unbeatable protection, with a low-touch deployment and management, and the lowest system overhead in the market.

Prevent host system abuse

Our deterministic approach delivers strict controls that block file system changes and prevent execution abuse. It uniquely ensures that processes only load safe and trusted libraries essential to the process' intended operation and prevent any loading of other unintended libraries into a running 'good' process. With added behavior sequencing controls focused on runtime memory, advanced process injection attempts are unveiled and instantly stopped before new threads in existing processes can be created, or processes execution can be redirected to malicious code. Only Virsec Host Protection application control can effectively defuse the most dangerous exploit techniques and stop runtime malicious behavior in real-time.

Ensure Continuous Compliance

DPP with Virsec Host Protection rich capabilities enables risk teams to continually ensure compliance with standards like NIST, GDPR, which recommend application controls to reduce the attack surface and ensure systems integrity of business functional areas. During an attack, admins maintain a complete picture of application usage patterns, with the added protection that secures software on the host system using low touch, high performing application controls with respect to the nature of the application, and maintain compliance even as these applications are updated, change, or new software is installed.

Maintain Control Flow Assurance

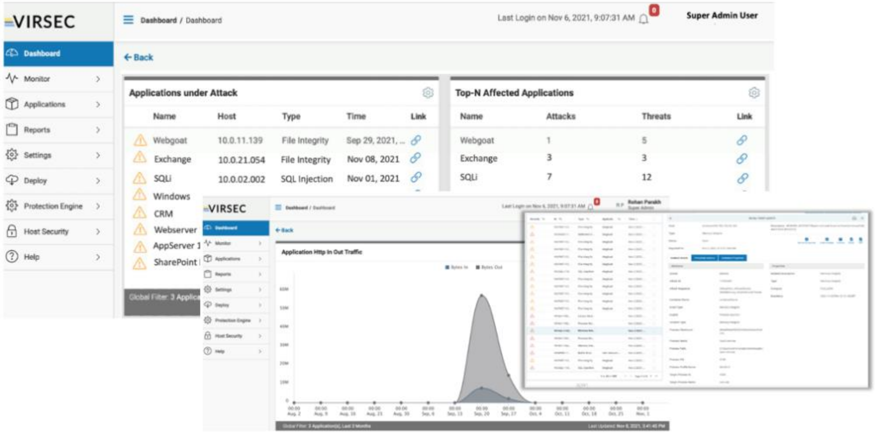
Activating Virsec Host Protection ensures efficient control flow integrity by uniquely mapping and securing the application memory runtime without dependencies on access to source code. Malicious in-memory events are revealed at run-time, distinguishing trusted execution flow, control data, and user data from malicious events - precisely stopping any attack attempts in real-time before they can inflict any damage.

Deploy and activate protection with ease.

Once you download and install the software, login to Host Guardian, deploy probes wherever your apps reside, and turn on protection – then begin to experience stronger security.

Until now, generating and maintaining allow-lists has been a tolling task for IT and security operations teams. With Virsec Host Protection, administrators can automatically scan servers and auto-generate allow-lists for each workload, including executable files, processes, scripts, interpreters, and related libraries, regardless of file extensions. This data can then be easily scaled to the enterprise, site, or group level. Virsec Host Protection also provides out-of-the-box templates that lower management overhead by automating and streamlining software deployment workflows by IT, DevOps, or Security Operations.

Report and respond to critical activity in real-time



Applications under Attack

Name	Host	Type	Time	Link
Webgoat	10.0.11.139	File Integrity	Sep 29, 2021, ...	🔗
Exchange	10.0.21.054	File Integrity	Nov 08, 2021	🔗
SQLi	10.0.02.002	SQL Injection	Nov 01, 2021	🔗
Windows				
CRM				
Webserver				
AppServer 1				
SharePoint				

Top-N Affected Applications

Name	Attacks	Threats	Link
Webgoat	1	5	🔗
Exchange	3	3	🔗
SQLi	7	12	🔗

Maintain visibility over all files on a workload, their execution behavior, and where they came from. Watch and track as DPP Virsec Host Protection stops threats and attacks in real-time across all of your software, with deep insight into the tactics and techniques employed by the malicious actors.

Learn more

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

or contact us for a [personalized demonstration]()