Virsec Host Protection

Lock down your server-based software & experience deterministic runtime 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.

Todays cyberattacks are highly sophisticated with a level of complexity that allows bad actors to exploit low-level vulnerabilities in host systems and obtain control of software, applications, & workloads - bypassing preeminent security solutions for their own gain. Large and small organizations are demanding a deeper layer of protection with a direct line of sight into all software code, composite workloads, and components executing during runtime.

Virsec Host Protection is purpose-built to ensure the integrity of application software using a deterministic runtime protection approach that erases risks, reduces the attack surface, and minimizes the impact of attacks targeting mission-critical applications, and container workloads on-premises or in the cloud. The rich capabilities and continuous automation address significant cyber security challenges -- lack of accurate runtime visibility, ineffective application controls, limited process protection, and no means to prevent misuse of components and attacks that masquerade as trusted processes. Without Virsec Host Protection, vulnerable systems remain at increased risk with little means to prevent attacks from exploiting software and propagating and advancing malware, ransomware, data breaches, service disruption, and more.

Harden Applications from Inside

Unlike common workload protection solutions, Virsec Host Protection establishes a foundation for achieving 100% application protection. It 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.

HOW IT WORKS: As a host-based security solution, Virsec Host Protection employs a lightweight probe on the application. When your protected application is activated, it automatically generates an AppMap™ depicting the entire software stack including data flows, processes, libraries, interpreters, and the relationship between elements. This is applied to default protections and 'allow-list' that maintain strict control on executables, libraries, processes, tools, scripts, and more securing integrity across runtime as malicious attempts happen in real-time. AppMap™ is the basis for continuous monitoring of runtime elements through the lenses of the application business logic for a deterministic approach to detection that yields precision protection. Any anomalous process and malicious file load, data input, command use, or system call, will trigger an alert instantly and initiate protective action to stop threats and trigger other network defenses before attacks fully evolve – without human intervention.

STANDARD CAPABILITIES

Application Control and Integrity Monitoring

- Automated Dynamic Allow-listing
- Process, Library & Script monitoring
- Cloud Reputation Service
- Publisher Control
- User & Group Access Control
- Command Line Control
- Change management control

Exploit Protection

- Code Injection
- Library injection
- Library hijack

Container Protection

- Drift Prevention
- CICD Integration
- Dynamic Scaling
- Flexible Deployment

Prevent Unauthorized Execution (Zero-trust Execution)

Virsec Host Protection applies the concept of zero-trust to execution, for assurance that untrusted code cannot execute a single line of instructions. Malware, targeted exploits, LOLBins, and malicious scripts, are automatically terminated with precision and without prior threat knowledge, validation, and efforts of mature security operations with trained specialists.

No longer is such advanced protection tied to the latent response actions of behavior algorithms, network solutions, MSSP and MDR services, and other tools geared towards investigation and hunting. Hardening your system with Virsec Host Protection enables you to maintain resilience in the face of attacks with our integrated Deterministic Protection Platform (DPP) designed to stop, block, kill, and revert malicious server-side events with precision as they happen early in the threat cycle. Unlike other solutions that allow attacks to progress, our technology prevents dangerous and pervasive attack schemes used to build and execute attacks quickly on systems within memory, processes, and files without notice until long after cyber actors recede.

> "I picked CrowdStrike to protect my endpoints and Virsec to protect my servers. Virsec proved to be more accurate, more agile and gave us faster time to value, with lower admin costs than conventional tools."
>
> CTO, integrated supply chain leader

Prevent the Effects of Ransomware Attacks

The risk of Ransomware attacks becomes futile with solid defenses that help prevent attack escalation from inside the host where cyber actors employing ransomware have already gained initial system access. Our strict application controls and runtime visibility stop attackers from infiltration, defense evasion, and persistence techniques & halts attempts at malicious payload execution using files or file-less means, misuse of PowerShell and illegal file access like unauthorized reads and modifications.

Ensure Strict Application Control Continuously

Virsec Host Protection uniquely combines runtime memory protection, script control and file system monitoring, for strict application control capabilities that maintain the integrity of your workloads and stop file-based and fileless attacks for assured resilience where others fail.

By employing a layered defense strategy that combines dynamic application controls to lock down server workloads and advanced exploit mitigation, it also guardrails running applications to good behavior. Our approach significantly reduces the attack surface and prevents the success of malware and sophisticated stealthy nation-state attacks with minimal operator overhead.

Automated Allow Listing & Process Monitoring

From a single click, Virsec Host Protection users can generate an allow list for a specific workload including executable files, processes, scripts, interpreters, and related libraries, regardless of file extension, and applied at a global, site, or group level.

Automations streamlines allow listing exclusion activation easily assuring only trusted components run, while greatly reducing complex arduous workflows commonly needed to build and maintain complex allow lists. When application components are updated, changes to allow lists are addressed automatically.

Library Monitoring

To avoid detection and elevate privileges, attackers commonly abuse vulnerabilities in libraries that load into trusted system processes like explorer or svchost. Virsec Host Protection prevents library abuses and ensures that processes only load safe, trusted libraries essential to the process. Any other library is prevented from loading into a running process, effectively defeating some of the most dangerous malware exploit techniques.

Files System Scanning and Monitoring

To boost anti-malware practices and readily understand exposure to threats, Virsec Host Protection allows you to scan application inventory before implementing protection, alerting you of vulnerable, high risk, and malicious executables and packages on the host. With suspicious or vulnerable files, it provides a reputation score and context of the rating. Furthermore, repositories are continuously monitored for access or change violations, alerting you in real-time, leaving no window for attackers, and automatically triggers responsive actions to maintain the original state of the filesystem.

Dynamic Trust Validation

With the integration of cloud-sourced reputation intelligence, Virsec enables continuous validation of file reputation and publishers and software packages, along with file path and against file reputation databases automatically. The dynamic services map to Microsoft recommendations and MITRE ATT&CK techniques to mitigate LOTL attacks and uncover malware that uses trusted system process to execute attacker-controlled data.

Memory Exploit Protection*

Detecting early attempts at process injections like reflective DLL injection, hollowing, and doppleganging is often unachievable when relying on analytics and behavior analysis. 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 redirected. A single click within the host profile activates protections instantly and binds workload elements in this way, organizations harness applications. Protections automatically expose execution violations in real-time, capturing the source and target process and function call details and updating the affected process's reputation score. Protective actions immediately safeguard execution, especially within Windows environments, preventing critical defense evasion tactics that bypass other workload protection solutions for zero-trust performance.

*Requires additional licensing of Virsec Memory Protection

Deploy and activate protection with ease

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

Virsec tools simplify probe placement and automate activation of protection on workloads

1) Execute script for probe placement and automation will drive the rest
    - Probe auto registers
    - Scans to identify and provision apps or container images
    - Initiates AppMap generation
    - Enables Protection

Protect Legacy & Modern Applications

Embracing digital transformation while retaining legacy systems doesn't have to come at a cost or pose a significant risk to the organization. Virsec Host Protection is designed to continuously address critical vulnerabilities in outdated, unpatched windows and Linux-based software (and off-the-shelf technologies) no longer supported. Easily maintain strict change management, prevent malware from building on the system, stop zero-day attacks targeting binaries or infecting processes in runtime without prior knowledge, learning, or access to source code. Only Virsec Host Protection enables you to enforce full-coverage protection on modern applications and secure legacy systems needed to drive the business forward.

Secure Cloud-Based Software

Although public cloud providers guarantee a secure infrastructure, Virsec Host Protection helps software owners confidently ensure the same for software workloads and data deployed there. Combined with the full capabilities of the DPP solution in infrastructures like AWS, Google Cloud, Azure, you can easily enforce protection from the guest operating systems up and throughout the composite structure of the applications running, even to the web. Centralized management and monitoring simplifying activation throughout the scaling multi-cloud environment and ensures runtime visibility across protected applications and the events countered that put your organization at risk. Furthermore, Virsec Host Protection maintains the same automated assurance of vulnerability protection in the cloud as in the data center to help you ensure compliance wherever you maintain your business infrastructure.

Implement Deeper Container Protection

Virsec Host Protection can be extended within running container images, protecting throughout the duration of runtime. By runtime, we mean as data input and calls drive processes to launch and code to execute so that deterministic security actions instantly reduce the attack plane that may compromise a Kubernetes-based container (in public or private cloud environment). Whether deployed in AWS, GWC, AZURE or private datacenter attacks are stopped instantly with precision regardless of granularity, duration or locality.

Furthermore, seamless integration with the container orchestrator means that your protections automatically scale with the workloads. Orchestrator support includes native Kubernetes, AWS EKS, AWS ECS, Azure AKS, and including Helm chart support for easy deployment at scale. Virsec Host Protection for containers is flexibly deployed either as sidecars or embedded directly inside the containerized application.

With Virsec Host Protection your DevSecOps team can effectively optimize CICD cycles to close the door on container risk -- automatically scanning container images and injecting security, thus ensuring the containers are “born secure” from the get-go. Unauthorized binaries, and malignant command lines and shellcode are automatically denied execution. It enforces strict immutability and provides drift prevention for containerized workloads during their entire lifecycle.

Optimize Your Cyber Security Strategy

A single pane of glass to monitor, deploy, and manage endpoints is often not enough to streamline the workflows and efforts required to ensure rapid response to attacks, especially if the goal is to immediately stop malicious events targeting servers. Take the complexity out of application protection with a single solution that provides complete runtime visibility at depth and consolidates tools that drive workload protection across all vulnerable applications. Virsec Host Protection allows you to fuse existing application controls, anti-virus capabilities, and tools to 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 from a single pane of glass. It truly optimizes line of sight and control that reduces the impact of threats throughout your data center and multi-cloud workload environments.

Benefits

- **Provides deterministic protection** against high-risk CVE’s, zero-day, and poly morphic exploits that often go unnoticed with EDR, EPP and XDR solutions without prior insights or false positives.
- **Focuses protection inside the application stack** based on how software should execute without tuning.
- **Secures with precision out-of-the-box,** protecting workloads & everything interacting with it
- **Auto-generates an AppMap and allow lists** to guardrail the application workload without learning or ongoing tuning
- **Ensures continuous visibility into runtime execution** with strict controls inside running containers, and applications deployed in VMs
- **Continually address**:
  - MITRE ATT&CK Framework
  - MITRE Top 25 Most Dangerous Attacks
  - Supply chains attacks

Enrich Existing Security Tools

Integrate with **SIEM**, **SOAR** and **Network Perimeter** solutions, and XDR/EDR tools that analyze compiled security data –bring awareness to unseen threats and vulnerabilities protected at runtime.

zendesk

servicenow

paloalto NETWORKS

splunk>

…and other vendor solutions

Maintain Continuous Compliance

Cyber security compliance is an ongoing process that challenges many IT team efforts to stay on top without interruption as new requirements arise, code or applications change, and vulnerabilities increase. Deterministic Protection Platform, which comprises of Virsec Host Protection offers capabilities and automation designed to take IT teams away from responding reactively to audit requests and attacks to being proactively prepared for future threats and data reporting requirements. It automates many aspects of people, processes, expertise and tools required for compliance with key regulatory security standard benchmark, including **NERC CIP, NIST 800-53, SOX, ACSC, PCI** and **HIPPA**. Furthermore, Virsec Host Protection helps spot developing threats at the web, memory and host layers and responds with protective actions in the event of a security breach and impact on services to exceed many regulations and assists in compliance that ensure effective risk management even when vulnerable software has yet to be patched.

Drive Efficiencies and Unburdens IT

"With Virsec, there is nothing to do, no issues to resolve, and when there is an alert, it is real". **Former CISO, Inspirage**

Virsec solutions are designed to take complex operations out of security and instill automated defensive actions driving efficiency, so security can deliver secure business systems without risk.

Gain assured runtime protection with the continuity to defend against evolving threats and known and unknown attacks automatically.

Zero Touch

Eliminates need for expert tuning, investigation and audit practices.

No False Positive

Detects with precision generating alerts only where there is a true threat or attack.

Simplifies updates

Protection is easily maintained even when deploying new SW versions or variations in threats evolves.

Reduces Tools

Consolidate web, allow-listing, AV and evasive exploit protection

CASE STUDY | Leading Oracle Systems Integrator

Harden Legacy Application	**Strengthen security defense** for aging, legacy client-server application software at the heart of your enterprise, while migrating to newer, more efficient code or infrastructure that makes use of current technology and programming languages
Modern Application Protection	**Maintain solid protection** where complex and highly composite applications and web services being developed at rapid pace comprised of vulnerable components (like opensource packages), and deployed across numerous virtual machines, containers, and serverless functions.
Cloud Security	**Harden cloud workloads** from the inside and maintain unified protection for all applications deployed in public, private and multi-cloud environments
Secure Air Gapped Systems	**Ensure the resilience** of software running in isolated environments that cannot connect with cloud-based intelligence services or external manages services
Maintain Zero Trust	**Extend zero trust** to runtime execution to ensure that no malicious code ever executes, and systems always run as intended

Challenges

- Migrating customer apps from AWS to OCI with stronger security requirements for custom developed applications and middle-ware
- Application integrity and data privacy concerns increased with increased development activity
- Increased concerns for effective risk management throughout the threat plane and real-time response
- Sparse resources make policy updates, tuning, analysis and hunting difficult to accomplish 7/24

Virsec Host Protection delivers protection that has unmatched by leading EDR/XDR providers. It uniquely **ensures continuous detection** & response without expert management or threat hunting. Requirements for system integrity monitoring and application control are also easily met.

Learn more

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

or contact us for a personalized demonstration