Virsec Memory Protection

Counter invisible attacks and prevent zero-days from affecting systems through memory

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.

Advanced attackers rely heavily on memory-based file-less techniques to avoid touching the filesystem and remain extremely stealthy. Without a means to observe and stop threats born in memory, organizations remain at high risk from unknown attacks with little to no defense from detection-centric solutions that rely on signatures, threat hunting, or broken AI algorithms that drown you in false alerts while the attackers keep advancing. Advanced memory protection proactively ensures that only fully trusted code is allowed to execute anywhere in your systems.

Virsec Memory Protection provides industry-leading evasive exploit protection addressing the most devastating and difficult-to-detect adversary tactics built entirely in memory to evade detection. Advanced memory protections automatically identify invalid code jumps in memory and unauthorized code execution, so malicious code cannot be concealed and executed inside benign processes. Furthermore, there is assurance that no data or information loaded will harm the application control flow or overrun memory bounds. Virsec Memory Protection activates from a lightweight probe on the host server. It is not dependent on software development tooling, reputation, probabilistic heuristics, or signature updates, allowing you to activate frictionless defenses in minutes.

Zero Trust Execution

With our technology, you gain the most advanced level of memory protection for hosted software applications. Our patented approach ensures efficient control flow integrity by uniquely mapping then securing memory at the core without conflict, kernel dependencies, or access to source code.

Detection of malicious in-memory events is uniquely centered on code and data inputs loaded into memory at runtime to distinguish trusted execution flow, control data, and user data from that is malicious and in various segments of process memory quickly, precisely, in real-time. Unlike other technologies, our solution effectively protects compiled and 3rd-party software targeted with buffer overflows, return-oriented programming (ROP), and other methods that allow attackers to seize control of compiled applications and systems when deployed in containers or VMs. Combined with host protection, organizations gain solid protection assurance against Ransomware, sophisticated supply chain, and nation-state attacks on modern and legacy systems.

Why leverage Virsec Memory Protection?

Today's widespread nation-state attacks execute more evasively to leave victim organizations with hundreds of millions in losses ultimately. Regulatory agencies and industry standards like NIST[1] suggest organizations implement memory protection with the intent of protecting hosted systems from tactics that enable code execution in specific regions of memory, even memory locations that are prohibited – accomplishing attacks invisibly without ever affecting the disk.

Deploy Better Memory Protection

- ✓ Protect against ROP & BROP attacks
- ✓ Buffer overflow
- ✓ Corruption of non-control configuration data
- ✓ Fileless attacks
- ✓ Stack smashing
- ✓ Remote DLL loading & execution

[1] National Institute of Standards and Technology SI 16 - NIST SP 800-53 database Revision 5, Security and Privacy Controls for Information Systems and Organizations.

Virsec Memory Protection:

- **Extends existing runtime memory protection** against code injections and PowerShell script exploits that Virsec Host Protection provides with full control flow assurance
- **Adds granularity to memory protection** against buffer overflows, return-oriented programming, and other blind attack schemes on program flow, memory stack, and return addresses. tactics that enable lateral movement or change application flow
- **Overcomes challenges faced when leveraging ASLR, CET, DEP,** and other operating system-based controls that require compile-time flags yet can be bypassed by ROP/BROP kind of attacks or even disabled by attackers
- **Delivers continuous protection against evolving attack variants** and is never rendered useless when other components are unprotected

Continual Defense for Evasive Attack Tactics

Memory-based attacks comprise the most insidious threats to critical applications, exploit the most common vulnerability in applications (buffer overflows), and represent the most frequently used advanced exploit over the last several years. Remote code execution exploits – once an outlier – have now become the go-to evasive attack technique, and many IT professionals regard memory attacks as "indefensible" by today's security products.
Virsec Memory Protection is essential for achieving 100% application protection. It provides depth in visibility and protects memory allocated across the application runtime infrastructure to ensure effective memory protections and defenses against fileless attacks that affect flaws in applications and change runtime execution without notice.
With deep visibility into the instruction execution cycle and control flow data, Virsec Memory Protection compliments Virsec Host Protection application control capabilities when activated with host monitoring profiles. Protection is implemented on a per-app basis without code changes, additional hardware, software dependencies, off-to-the-cloud analysis, or ongoing security expertise. It increases protection for most common complied software and applications deployed in production without constant tuning of policies, threat validation, and false positives for effortless defense.

Effective Remediation

Virsec Memory Protection easily defends against memory-based attacks that evade HW & SW data execution prevention (DEP), host-based IPS, and endpoint suites, overcoming limitations of these solutions without policies and while tracking remediation for every vulnerability and incident detected. Critical flaws and unknown software errors can be remediated continuously, preventing exploits via memory that compromise system operation, information, and data. Threats and attacks against process flows and corrupt memory are discovered and remediated in milliseconds with protections given below.

- Stop attempt to inject malicious code with zero dwell time
- Terminate/Restart affected process(es)/thread(s)thread(s)

Automatically address concerning vulnerabilities with attention on memory across the full stack to detect and protect when a workload starts executing attacker-provided shell code.

Advanced Memory Protection for Mission Critical Software

- Application Servers
- Web servers
- containers,
- APIs
- COTs
- GOTs
- Frameworks

Enables true runtime protection in real time, thwarting attacks early to minimize dwell time without tuning, analysis or hunting well before things get out of hand.

SOFTWARE AGNOSTIC

Protects compiled applications and workload components developed using languages like J**ava, Python, C++, C**#, and **Ruby** and running in **Windows**, **Linux** and other operating systems, and within OpenShift, Docker®, **Kubernetes** environments.

Benefits Customers Experience

- Real-time exposure of evasive malicious events with protection that prevents ransomware, breaches, and exfiltration.
- Erases risk and concerns where vulnerable software is deployed.
- Activates easily and deploys at

Maximum Runtime Control

Almost every application has vulnerable components developed by 3rd-parties that aren't quickly or easily resolved. For example, Apache and NGINX web servers front-end many custom web applications, which have been vulnerable to attacks. Legacy applications are also fraught with an increasing number of vulnerabilities that remain unpatched. Activating memory protection within our Deterministic Protection Platform helps to ensure vulnerable code always executes as intended and software and configuration errors that present risk is addressed continuously without additional expert efforts.

Memory Exploit Protection

Detecting and stopping early attempts at process injections like reflective DLL injection, hollowing, and doppleganging is often unachievable when relying on analytics and behavior analysis. With 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 memory exploit protections immediately and binds workload elements; in this way, organizations harness applications within memory. 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 environments, preventing critical defense evasion tactics that bypass other workload protection solutions for zero-trust performance.

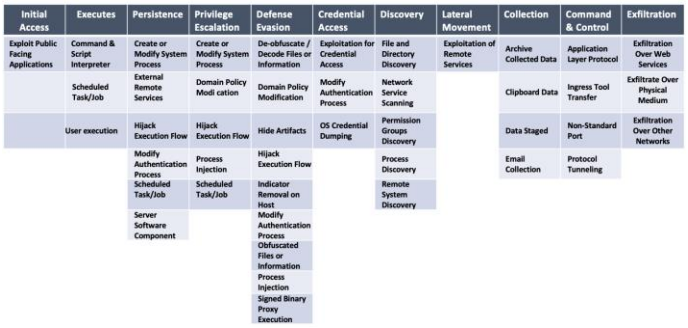
Experience Protection in Milliseconds

No longer is advanced protection tied to the latent response actions of behavior algorithms, MSSP and MDR services, and other tools geared towards investigation and hunting. Activating memory protection with Virsec Memory Protection and hardening system with Virsec Host Protection enables you to maintain resilience in the face of attacks with our integrated Deterministic Protection Platform 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.

Comprehensive MITRE ATT&CK Coverage

Virsec Memory Protection elevates your security with protection that aligns to the MITRE ATT&CK matrix, efficiently and effectively addressing adversary techniques used in the most critical stages of the server's attack kill chain (i.e., execution, defense evasion, privilege escalation, and persistence).

Advanced memory protection capabilities are essential aspects of our Virsec Security Platform intended to stop the progression of various malicious tactics, thus prohibiting discovery, lateral movement, and data exfiltration events. MITRE coverage leverages host-based runtime memory protections that prevent process injections and stop misuse of trusted components and adds comprehensive visibility across application memory enabling control flow awareness with optimized protection inside the memory. Our deterministic solution operates from the best vantage point for identifying unexpected, untrusted anomalous events targeting critical systems and exposing adversaries that may evolve at any urgent point in the malicious sequence. And protective actions execute a lot sooner and with greater accuracy than XDR-based solutions that analyze relevant indicators of compromise and use third-party telemetry to pull together signals indicative of an attack.



Initial Access	Executes	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
Exploit Public Facing Applications	Command & Script Interpreter	Create or Modify System Process	Create or Modify System Process	De-obfuscate / Decode Files or Information	Exploitation for Credential Access	File and Directory Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Exfiltration Over Web Services
	Scheduled Task/Job	External Remote Services	Domain Policy Modi cation	Domain Policy Modification	Modify Authentication Process	Network Service Scanning		Clipboard Data	Ingress Tool Transfer	Exfiltrate Over Physical Medium
	User execution	Hijack Execution Flow	Hijack Execution Flow	Hide Artifacts	OS Credential Dumping	Permission Groups Discovery		Data Staged	Non-Standard Port	Exfiltration Over Other Networks
		Modify Authentication Process	Process Injection	Hijack Execution Flow		Process Discovery		Email Collection	Protocol Tunneling	
		Scheduled Task/Job	Scheduled Task/Job	Indicator Removal on Host		Remote System Discovery				
		Server Software Component		Modify Authentication Process						
				Obfuscated Files or Information						
				Process Injection						
				Signed Binary Proxy Execution						

Virsec Memory Protection is an element of Deterministic Protection Platform by Virsec which uniquely delivers runtime defense against tactics named in MITRE ATT&CK Framework

- Hardens hosted applications and systems
- Ensures zero dwell-time for no persistence
- Uncovers and blocks defense evasion attempts
- Prevents hijacking of DLL's, processes, execution
- Stops lateral movement and C&C practices
- No data source requirements

Deterministic Security for Linux & Container Workloads

Linux powers over 95% of the top domains and is increasingly subjected to sophisticated 0-days from advanced adversaries. Once considered a relatively low-risk environment, implementing security measures on Linux systems may now lag behind Windows environments. Virsec Memory Protection offers a powerful yet lightweight agent for security observability and proactive threat protection for your Linux-powered infrastructure – including VMs, containers, and Kubernetes clusters – either in the cloud or datacenter. Advanced memory and control flow assurance ensures that evasive emulations on Linux hosts are thwarted, preventing bad actors from assessing critical systems, information, and other targets.

Virsec Memory Protection Key Features and Capabilities

	What it means to you
Automated Memory Mapping	Builds an *AppMap* of the application, including the allocation of memory to deterministically detect attacks in real-time
Control Flow Integrity Assurance	Automatically ensures that only trusted data flow and execution progresses in alignment with *AppMap*
Memory and Process Monitoring	Continuously monitors and tracks the spawning of processes and data from memory, discerning anomalies that are indicative of attacks
Targeted Attacks Protection	Addresses all untrusted events immediately before any malicious code executes
Centralized Monitoring and Activation	Provides a single pane from which to instrument protection and observe protected workloads and the threats and attacks faced
Open Integrated Architecture	Seamless integration with other Virsec and third-party products reduces protection gaps, eliminate reduces and optimize defenses at the perimeter
Forensic Data Collection & Security Reporting	Provides intelligence that reveals what threat actors are doing and how the threat may have manifested, provide insights on the severity of the event, and the context of the compromise on the victims' software

Key Advantages of Virsec Memory Protection

- Detect real threats with precision based on contextual understanding of memory use and the data within it & not based on any specific industry, region, or external indicators of compromise.
- Offers complete runtime protection against evasive threats, not mere guidance for you to assess and improve security upon.
- A component of Virsec's **Deterministic Protection Platform** offers next-generation threat protection, attack prevention, and flaw remediation by monitoring the application software stack as it executes.
- Precision protection eliminates dependencies on manual efforts and expertise, including support from MDR and MSSPs, focused on hunting and investigating concerning events.
- Uncovers attacks in the earliest phase of threat sequences within milliseconds and not seconds, minutes, hours, or days as with common solutions.
- Eliminates dependencies on machine-learning, user behavior analysis, and auto-learning when detecting changing patterns or zero-days, and the need to optimize rules to identify future attacks.
- Protects runtime in real-time and not 'near real time' as others claim.

Learn more| To learn more about Virsec Memory Protection, visit us here