Virsec Web Protection

Advanced deterministic protection for Web Applications, Microservices & APIs

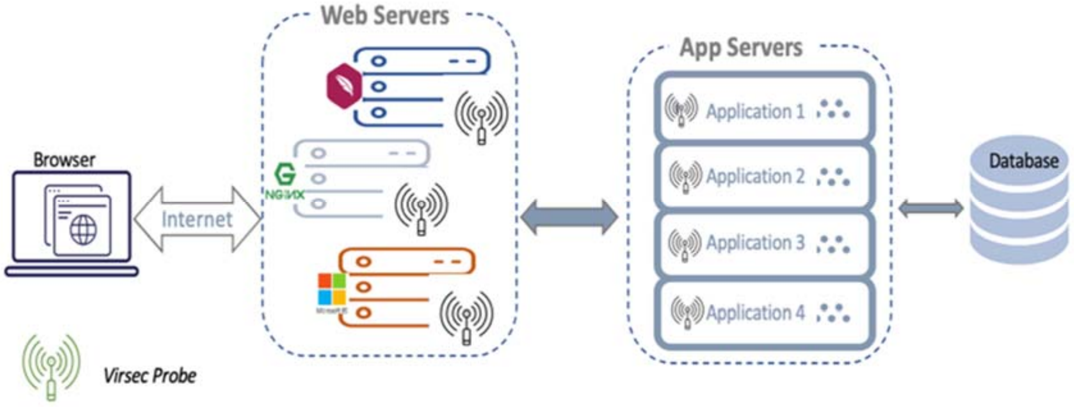
The world runs on software, yet, until now, there was never a way to achieve 100% protection of that software while it is running, wherever it is running. The only way to fully protect software is by fully mapping and understanding what it is supposed to do and immediately stopping what it is not. Virsec's Deterministic Protection Platform (DPP) eradicates software threats in real-time before they can cause any harm, making security response obsolete.

Web Applications are amongst the most common entry points for data breaches and come at a high cost. With the fast pace of software development cycles, the pervasive use of open-source code, and public cloud residence, many Web applications put into production remain ladened with vulnerabilities traditional tools have little means of protecting. Organizations are now seeking host-based, in-app web protection where WAAP tools may not be enough.

Next-generation web protection with Virsec Web Protection increases protection against OWASP Top 10 attacks that have bypassed network-based defenses targeting all types of web application (single page, multi-page, JavaScript, static and dynamic) without the hassle of legacy perimeter technologies like the use of proxies, SDKs, and network changes. You can now easily activate web protection within the webserver and throughout the entire web application infrastructure, automatically shielding known and unknown vulnerabilities at the application layer to stop attacks and erase risk where threats bypass firewalls. Unlike common solutions, our technology uses a deterministic detection approach focused on runtime in real-time and immediate protection without relying upon prior threat knowledge or intelligence, user behavior analysis, or assessing factors external to the application. A single sensor ensures continuous visibility and control that accurately filters HTTP traffic, hardens the host server, and maintains the integrity of trusted processes and kernel functions without a mountain of false alerts, continuous learning, expert tuning, or increased cost.

Modern Web Protection

Because application-layer attacks do evade signatures and reputation-based solutions, modern web security requires a deeper level of web defense that is more precise. Virsec Web Protection is the only web protection solution built on a deterministic protection platform to accurately counter complex web attacks that challenge external rule-based filtering, Data Loss Prevention, anti-malware, and bot defense services. With sensor-based controls inside the running server workloads and deep runtime visibility of data flowing through application business logic, Virsec Web Protection instantly counters unseen attacks. The depth of web application visibility illuminates security blind spots throughout the attackable surface – vulnerable interpreted code, web servers, compiled code, processes, libraries -- delivering protection assurance with out-of-the-box protection without overhead common to WAF technologies. Virsec Web Protection makes Zero-days, evolving threats, high-risk CVEs, and DDoS futile.



Why leverage Virsec Web Protection?

Approaches to web protection rooted in web application firewalls or IPS can’t see attacks that masquerade under trusted context. Apps remain vulnerable, as file-less malware silently trespasses salient web systems and executes activities that make applications non-responsive or even execute malicious code. Other tools often leave teams overwhelmed with alerts and 1,000’s of false positives and thus remain monitoring tools. Virsec Web Protection instruments the application runtime environment to ensure that user inputs never execute as code, stopping evasive web attacks fast, and thwarting attacks that ultimately damage, disable, or disrupt host systems and networks essential to your web application service, without the challenges that burden your IT resources and increase the cost.

Deploy Better Web Protection

- ✓ Protect against OWASP top 10
- ✓ Eliminate False Positive
- ✓ Activate in the datacenter in AWS, Azure, and GCP,
- ✓ Reduce operational workload
- ✓ Whitelist server-side input validation
- ✓ Prevent mass disclosure of records

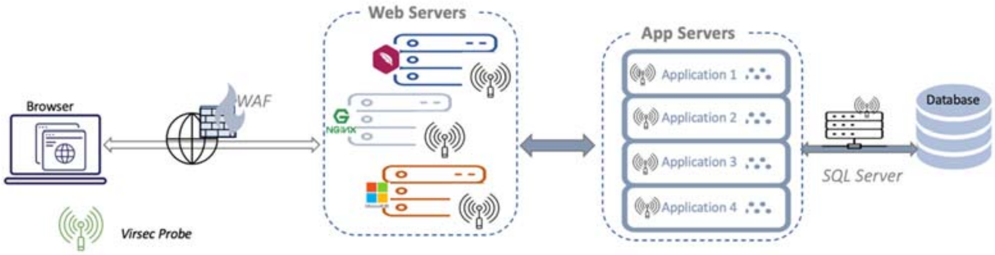
Organizations are leveraging Virsec Web Protection to…

- **Protect where WAF, IPS, and EDR fail** against injections attacks & script exploits with control flow assurance
- **Prevent exfiltration and web abuse,** including tactics that enable lateral movement or change application flow
- **Center security on runtime protection in real-time** and never rendered useless when components are unprotected.
- **New enhancements make deployment easier** and enable flexibility for performance without jeopardizing security
- **Delivered as software and deploys anywhere** windows and Linux based web services are hosted
- **Component of Virsec Security Platform** that addresses vulnerabilities and provides protection beyond OWASP 10

How Virsec Web Protection Works

Virsec Web Protection augments network security with flexible sensor-based web protections focused on the ingress or the entire transaction throughout application infrastructure, unlike WAAP capabilities that converge RASP and WAF technologies to interrogate traffic, browsers, and user devices.

1) **Embedded Webserver Protection** validates requests from the frontend of webservers like Apache, NGINX, and IIS at the protocol level discerning suspicious SQL syntax, providing a simplified approach to application-layer web protection for complex, nuanced runtime environments
2) **In-app Web application Protection** – Deeper instruments in the app-layer that monitors the full transaction pattern through byte code, ensuring that data inputs do not cause nefarious events on runtime elements further downstream.



Unlike advanced WAFs deployed in a hypervisor, Virsec Web Protection loads with the Webserver or the application – no SDKs or code changes needed. Protections are activated with a single click for each attack type. Custom rules and exceptions help further tailor protection to specific needs and ensure trusted requests are never blocked.

Virsec Memory Protection provides depth in visibility and control flow integrity assurance at the memory level to counter evasive threats that hide, affect flaws in software, and change runtime execution. With the broader range of Virsec solutions, organizations are equipped to achieve 100% web protection.

Countering Automated Attacks at Runtime

Today, Assailants are leveraging automation to avoid detection easily and launch large-scale attacks like DDoS attacks, data breaches, and schemes hoarding resources. Compromised systems, command-line scripts, vulnerability scanners, and even headless browsers are tools to bypass security measures and automate attacks. Protecting against such threats had proven to be a daunting task when solely focused on interrogating the user, client browser, and traffic outside of the application – many attacks often go unchecked and unstopped.

With Virsec Web Protection, you can layer in runtime protection to augment network traffic monitoring and eliminate the risk by minimizing the impact and preventing the success of automated attacks. Deployed on the webserver or the within the web application, Virsec Web Protection immediately diffuses aggressive and voluminous attacks from within the host environment so that attacks left unblocked never overwhelm resources or root out and exploit known vulnerabilities. Advanced analytics, contextual awareness, and security controls throughout the application and software execution precisely stop malicious transactions and ensure more evasive process, command, and script techniques aren't misappropriated to breach data or affect web application services.

Benefits Experienced

- Protect without noise and assurance that only malignant traffic is blocked
- Secures the entire application infrastructure allowing you use open-source and other components without risk.
- Provides strong forensic data and actionable governance and regulatory reporting
- Protects Cloud, container and VM based web applications
- Goes beyond OWASP top 10 coverage to reduce risk
- Secures at the edge of the app the web server and throughout business logic on premises or in the cloud

Unique ability to stop automated attacks from the inside.

With full deterministic protection capabilities, DPP analyzes system behavior and events in ways experts and other tools cannot. Complex HTTP filtering, Interpreter syntax mapping, and strict runtime control stop fuzzing attacks used to probe your web app and injection attacks or DDOS that avoid detection and subtly overload the application without continuous learning or client browser interrogation. Moreover, protection telemetry strengthens WAFs against stopping repeat attacks at the perimeter edge in the future.

OWASP Top Ten Protection

Virsec seeks to protect critical web applications from today's biggest security concerns, including OWASP top 10 vulnerabilities. This includes SQL injections, malignant use of Cross-site scripting and XML entities, and fileless memory-based attacks. Unlike other web protection solutions, our technology not only examines, escapes, sanitizes, and filters data inputs, it monitors response and applies strict controls to prevent the outcome of exploits (like privilege escalation, process injections or hallowing, or remote code execution) on known and unknown vulnerabilities no matter how attacks manifest. Virsec Web Protection stands above other solutions delivering a 100% true positive detection rate and a zero percent false positive with OWASP protection in benchmark testing. Competitive solutions score in the range of 30% to 65% of finding True Positive. Apart from the OWASP Top 10, it immediately counters new threat vectors like Server Side Request Forgery (SSRF), Deserialization attacks, and attacks on the exposed API surface. Virsec Web Protection allows development, security, and operations to fully protect web applications, streamlining efforts behind security testing, exposing vulnerabilities, evolving CVE and CWE risks, and protecting production even where security expertise is lacking.

Maximum Runtime Control

Activating the host, memory, and web protection capabilities within our Deterministic Protection Platform helps to ensure vulnerable web services and backend components always execute as intended and software and configuration errors that present risk are addressed continuously without additional expert efforts,

Automatically address concerning vulnerabilities with attention on memory across the entire stack.

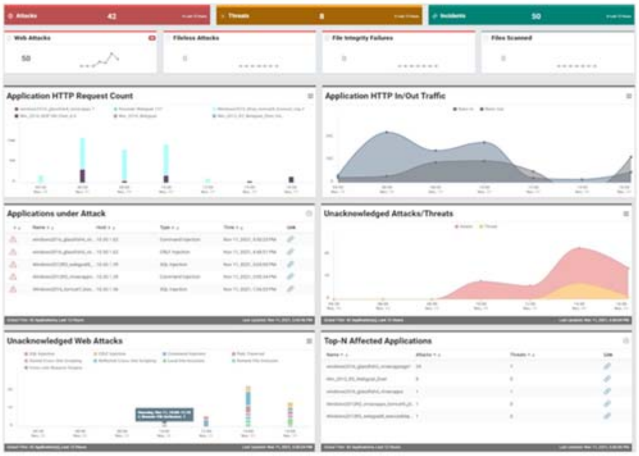
- **Memory Protection**: leverages in-memory instrumentation to detect and protect when an adversary attempts to execute unauthorized or malicious shellcode in memory
- **Web Protection**: leverages application runtime instrumentation to detect and protect when a workload starts executing attacker-provided inputs to a web application.
- **Host Protection**: leverages application control capabilities to prevent even single instructions from any unauthorized executables, libraries, and scripts from executing.

Key Use Cases

- OWASP Top 10
- Blocking WAF bypass attacks
- Protection on custom & 3RD party code
- Compliance
- Anti-breach controls

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.

Real-time Protection Observability


Attacks
42
Threats
8
Incidents
50
Web Attacks
50
Fileless Attacks
0
File Integrity Failures
0
Files Scanned
0
Application HTTP Request Count
Application HTTP In/Out Traffic
Applications under Attack
Unacknowledged Attacks/Threats
Unacknowledged Web Attacks
Top-N Affected Applications

CMS DASHBOARD & REPORTING

- Customize views with drag-and-drop widgets
- Review your security posture at a glance
- Visualize security trends by attack types, geographies, application, and other attributes
- Easily distinguish real threats from attacks, and quickly drill down for deeper insight
- Quickly note the context of the event, effect on application, vulnerability targeted, MITRE tactic used and attribution information
- Ensure alerts are addressed and critical information is communicated to those who need to know

Our Deterministic Protection Platform ensures visualization and alerts, so security teams always know what malicious events have reached the host application environment and the protections executed. Out-of-box reporting further streamlines efforts to assess new attack types and communicate findings to others throughout the organizations for data-driven risk decisions and help leaders understand the value of their investment in security.

Real-time alerts generated are actual and require no further investigation. Operators can readily view insights across the entire application perimeter. At-a-glance dashboard tables, charts, and gauges summarize information over time and provide drill-downs to forensic data captured as events unfold. Security teams benefit significantly from rich attack details that help pinpoint attack source, method, the affected application process, and more while aiding audits and agency investigations, helping ensure attribution, and providing a consolidated view across the entire threat field.

Virsec Web Protection Key Features and Capabilities

	What it means to you
Runtime Application Protection	Intrinsic protection across the entire application runtime environment against the OWASP Top 10 and more.
Zero-Day Web Attack Prevention	Ensures that user-supplied data is never interpreted or executed as code, thus preventing evolving threats and zero-day attacks without signature updates or rules
Programmable Rule Engine	Increases flexibility in how protection is processed to optimize performance - locally on the servers or as a sidecar, remote VM, or POD
Dynamic Exception Handling	Intelligent auto-exception mechanism built into the Incident management console, expanding out-of-box coverage, and ensuring benign requests are never blocked
HTTP Protocol Validation	Enforces strict protocol level restrictions to prevent protocol abuse and exploits, including buffer overflow, malicious encoding, HTTP smuggling, and illegal server operations
Class Load Logging	Maintains detailed class loading activity in the application to aid forensics, incident response, and traceability of unauthorized class loads
SW Exception Logging	Logs details about any exceptions resulting from HTTP transactions, including the source code generating the exception. Aids forensics, incident response as well as application debugging.
Targeted Attacks Protection	Guarantees that APT kill chains are defeated during initial stages (e.g., Infiltration and Initial Access), optimizing Zero-day protection
Visibility Across Web Server, Applications & Container Components	Flexible deployment capabilities across the most common language runtime environments, web servers, container runtimes, and orchestration mechanisms
Integrated Architecture	Seamless integration with other Virsec and third-party products to reduce security gaps and optimize defenses across the entire workload
Forensic Telemetry & Actionable Reporting	Captures actionable forensics with precise insights into real threats and ensures that attackers are not hidden beneath the noise
Event forwarding	Forward incidents to a variety of solutions, including SIEM, SOAR, Syslog, Email, Ticketing, and Webhook endpoints

Key Advantages of Virsec Web Protection

- Enables self-defending security that seamlessly moves with the app in the data center and cloud boundaries
- Meet stringent compliance standards like PCI, FISMA, HIPAA, NIST Cybersecurity Framework
- Rapid Deployment in full protection mode in a few hours without extensive tuning, baselining or learning
- Deterministic Protection Platform offers next-generation threat protection, attack prevention, and flaw remediation by monitoring the entire application software stack as it executes
- Eliminates dependencies on machine-learning, behavior analysis, and auto-learning when detecting changing patterns or zero-days, and the need to optimize rules to identify future attacks
- Protects application runtime in real-time, and not just monitoring network traffic from the outside

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