Datasheet

Virsec® Security Platform

Application Protection from Memory to Web

Advanced application attacks that weaponize at runtime (WRT) are increasingly putting businesses at risk. These attacks challenge application security by leveraging fileless malware, memory corruption and uncommon vulnerabilities to evade traditional security solutions. WRTs manipulate legitimate processes and enable stealthy execution of malicious code, resulting in data breaches, damaged infrastructure, and financial losses.

Low-level WRT exploits that manipulate code in memory allow attackers to control the process flow of critical business applications without immediate detection. These threats can persist within a network for months (or years) before discovery.

Virsec introduces a breakthrough deterministic approach to detecting advanced threats and memory-based attacks within milliseconds. It enables fast detection of threats during application runtime, effectively closing down the window of exposure for enterprise applications.

Advanced Attack Protection

Virsec® Security Platform is the first solution that deterministically blocks advanced memory-based attacks, unknown threats, stealthy fileless malware, and more with complete accuracy and no impact on applications.

Using patented Trusted Execution™ technology, the platform delivers the most advanced application protection against sophisticated attacks, discovering and preventing exploits of critical composite application functions, process memory and the CPU—stopping threats that bypass traditional security solutions. The solution discretely analyzes compiled and interpreted code, and acts as a memory firewall to prevent misuse of memory and unauthorized deviations in process flows in real time.

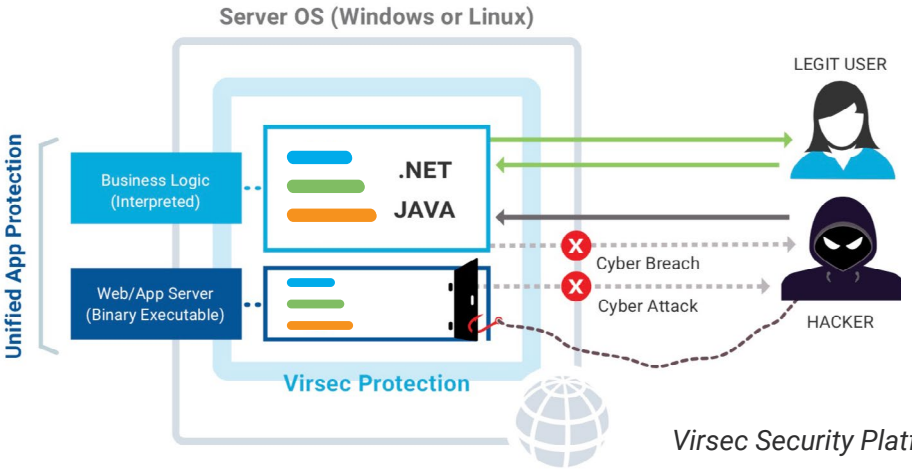
With Virsec enterprises can effectively harden applications from the inside, while ensuring application integrity, API enforcement and continuous authorization in the face of a threat.

Why VIRSEC

- **Hardens applications from the inside out,** across all workloads without re-compiling code
- **First memory corruption firewall** preventing spectre/meltdown, and application hijacking through process memory
- **Most advanced defense** that stops sophisticated attacks bypassing traditional security
- **Broadest range of attack coverage** without rules, monitoring and requirements for expert tuning
- **Delivers deterministic attack detection** using precise forensics and unsurpassed accuracy
- **Ensures application integrity in the face of an attack** with TRUSTED EXECUTION™ technology

Key Benefits

- **Defends against the most advanced attacks** unknown, zero-day threats, fileless memory exploits and WRTs
- **Protects internal, legacy and web applications** from OWASP 10 and attacks invisible to traditional security
- **Prevents lateral movement** and advanced persistent threats
- **Eliminates false positives** with accurate threat detection, even on first attempt
- **Compliments existing web application firewalls** to prevent attackers from ever reaching servers
- **Enforces pre-emptive vulnerability patching** of hardware and software flaws without signatures



Virsec Security Platform

Features and Capabilities	
OWASP top 10 prevention	Zero-day attack protection
Unknown threat discovery	Database transaction protection
Injection protection | SQL, DLL, XSS, CSRF, HTTP Header, OS command, Path traversal and process injections	Advanced threat defense | Memory-based attacks, data leakage, fileless malware, buffer overflows, Meltdown, Triton
Brute force attack detection	Response checking
Java de-serialization attacks | CRLF and HTTP Response Splitting	Automatic attack mitigation | Alert, block, log, URL override or redirect URLs
File system protection	REST API Support
PCI-DSS, FFIEC Compliance	Continuous policy-based authentication
Email and SMS alerts	External ticketing system support
Visualization | Reporting | Monitoring	
Real-time Dashboard reporting	Customizable charts and reports
Granular reporting by threat type	Violation classification and risk scoring
Attack attribution reporting	Real-time logging | Multi-lingual syslog/CEF formats per transaction URL -SQL activity
Centralized management and reporting	Customized alerts
Platforms Supported	
Operating Systems	Microsoft Windows Server 2012 R2 (64-bit) Linux Kernel RHEL 6.7 (64-bit)
JRE	JRE version 1.8 and Oracle Hotspot JVM
.NET	4.x or higher
Protocols/Data Transport:	HTTP/HTTPS/REST/SOAP/XML/JSON
Web Application Server environments	WebLogic, Apache Tomcat, JBOSS, WildFly
Technology frameworks	Spring, Apache, Hibernate, STRUTS
Databases	Oracle, MySQL, PostgreSQL, H-SQL etc
System Requirements	
Flexible deployment VM or bare metal	VMware ESXi Hypervisor, x86

Use Cases

In-depth Application Protection

Always-on defense against unknown and advanced attacks

Critical Infrastructure Defense

Securing critical infrastructure and control systems

Pre-emptive Patching

Patching design flaws before vulnerabilities are discovered

Risk Reduction

Minimizing the attack surface, lifecycle and overall business impact

226 Airport Parkway, Suite 350 • San Jose, CA 95110
Email: info@virsec.com • Phone: (877) 213-3558 • Web: www.virsec.com • Twitter: virsecsystems