VIRSEC SECURITY PLATFORM

DATASHEET

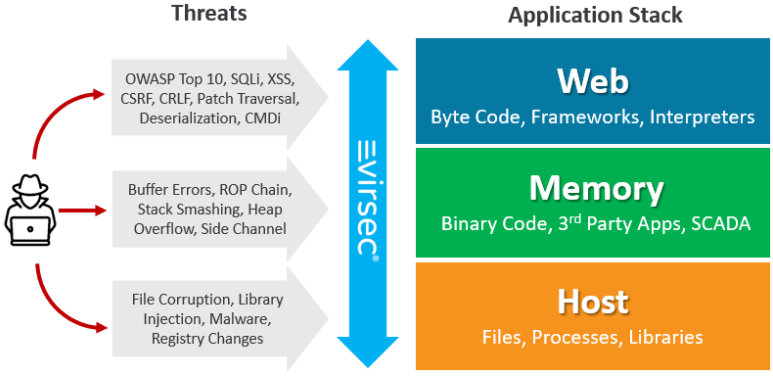
Eliminating Security Blind Spots

Advanced application attacks threaten critical systems and vulnerable data, as attackers increasingly target vulnerabilities deep within the application stack.

These attacks are challenging because they outpace conventional security by leveraging fileless malware, memory corruption, and the exponential growth in vulnerabilities. By causing applications to misinterpret input as code, attackers can hijack servers, execute ransom attacks, inject fraudulent transactions, steal data, or detonate malware without detection.

Full-Stack Application Protection

Virsec Security Platform is the only solution that unifies memory protection, application control, and system integrity assurance to secure workloads without false positives or performance impact.



Virsec uniquely maps intended application execution to ensure applications cannot be derailed. It analyzes interpreted and binary code, prevents misuse of memory, file systems, and libraries to prevent unauthorized deviations of process flows.

Key Benefits

- **Definitively stops advanced attacks** including zero-day, Remote Code Execution & supply-chain threats
- **Protects internal, legacy and web applications** out-of-the-box without requiring source code
- **Eliminates dwell time** to prevent lateral movement & payload detonation
- **Reduces operational complexity** without training, tuning or updates
- **Effectively hardens applications** against known and unknown vulnerabilities without patching

Only Virsec Delivers

- **Most advanced application security**
  Hardens applications from the inside
- **Complete app-stack protection**
  Integrates web, memory and host protection
- **Deterministic attack detection**
  No guessing, learning or security tuning
- **Unprecedented accuracy**
  Precise results reduce analyst costs

With patented AppMap™ technology, VSP monitors memory where the application stores user data input and application code. No matter the attack technique utilized, Virsec safeguards all workloads against efforts to process input as code, ensuring that applications never execute malicious input.

While attacks can cause damage within minutes, discovery and containment with conventional security tools can take months. Virsec, by comparison deterministically identifies attacks as they happen and stops malicious events in milliseconds. With industry leading capabilities VSP delivers the fastest detection and mitigation while reducing SecOps workloads – dramatically improving security while reducing costs.

Features and Capabilities	
OWASP Top 10 prevention	Zero-day attack protection
Remote Code Execution (RCE) prevention	Database transaction protection
Injection protection SQL, DLL, XSS, CSRF, HTTP Header, OS command, XML/XPath, Path traversal and process injections	Advanced threat defense Memory-based attacks, data leakage, fileless malware, buffer overflows
Brute force attack detection	Response checking
De-serialization attack detection CRLF and HTTP response splitting	Workflow Integration REST API support, logging, ticketing, SIM/SOAR
File system protection	Automated process monitoring
PCI-DSS, FFIEC, GDPR compliance	Automatic attack mitigation
Visualization | Reporting |Monitoring	
Real-time dashboard reporting	Customizable charts, reports and alerts
Unmatched forensic data captures by threat type	Violation classification and risk scoring
Attack attribution reporting	Real-time logging Multi-lingual syslog/CEF formats per transaction URL – SQL activity
Application Environments Supports	
Operating Systems	Microsoft Windows Server 2008, 2012 R2, 2016 (64-bit) RHEL 6.7, 7.x (64-bit) Ubuntu 14.04, 16.04 LTS
Web Application Server environments	WebLogic, Apache Tomcat, JBOSS, WildFly, Websphere, SharePoint, Unicorn,
Technology frameworks	Spring, Apache, Hibernate, Zend, .NET, Rails
Databases	Oracle, MySQL, MS SQL, PostgreSQL, H-SQL, Maria DB, etc.
Software Languages & Code Types *(minimum version and higher)*	JRE *(1.8)* and Oracle Hotspot JVM, .Net *(3.x/4.x),* PHP *(7.x),* Ruby, C#, and all compiled languages

virsec®

ProtectedIT
Elevating & Unifying Security Technologies

226 Airport Parkway, San Jose, CA 95110 www.virsec.com (877) 213-3558