Virsec®

Datasheet

Memory-Based Attack Cyber Defense

Full-Stack Application Protection from Memory to Web

With years of investment in failed security strategies at the endpoint and network level, applications have become the weak point in cyber security. Applications are at the center of the majority of today's data breaches and hackers view public facing web apps and unpatched internal binaries as rich targets.

These attacks have become significantly more sophisticated using advanced tools, often developed by nation-state actors. Today's hackers are well-funded, patient, and employ a wide range of zero-day exploits, including memory-based techniques that evade traditional network and endpoint security. Many of these exploits, such as return-oriented programming (ROP) chain attacks, have been considered "indefensible" until now.

Virsec introduces a unique deterministic approach for detecting memory corruption attacks in microseconds. Working during application runtime, real-time detection effectively closes down the zero-day windows of exposure on enterprise applications.

Breaking the Sophisticated Attack Life Cycle

While cyber-attacks popularized in the media focus on social engineering and phishing, today's hackers work in more sophisticated ways with advanced tools now widely available. Infiltration, network re-entry and lateral pivots to higher value targets often make use of zero-day vulnerabilities and fileless memory-based attacks. Data exfiltration is more ingenious and clean-up more comprehensive, making attribution difficult. Most importantly, these malicious actors have capabilities to subvert traditional security products that rely on signatures, log analysis or network packet identification.

A new approach is needed for dealing with these targeted and advanced persistent threats.

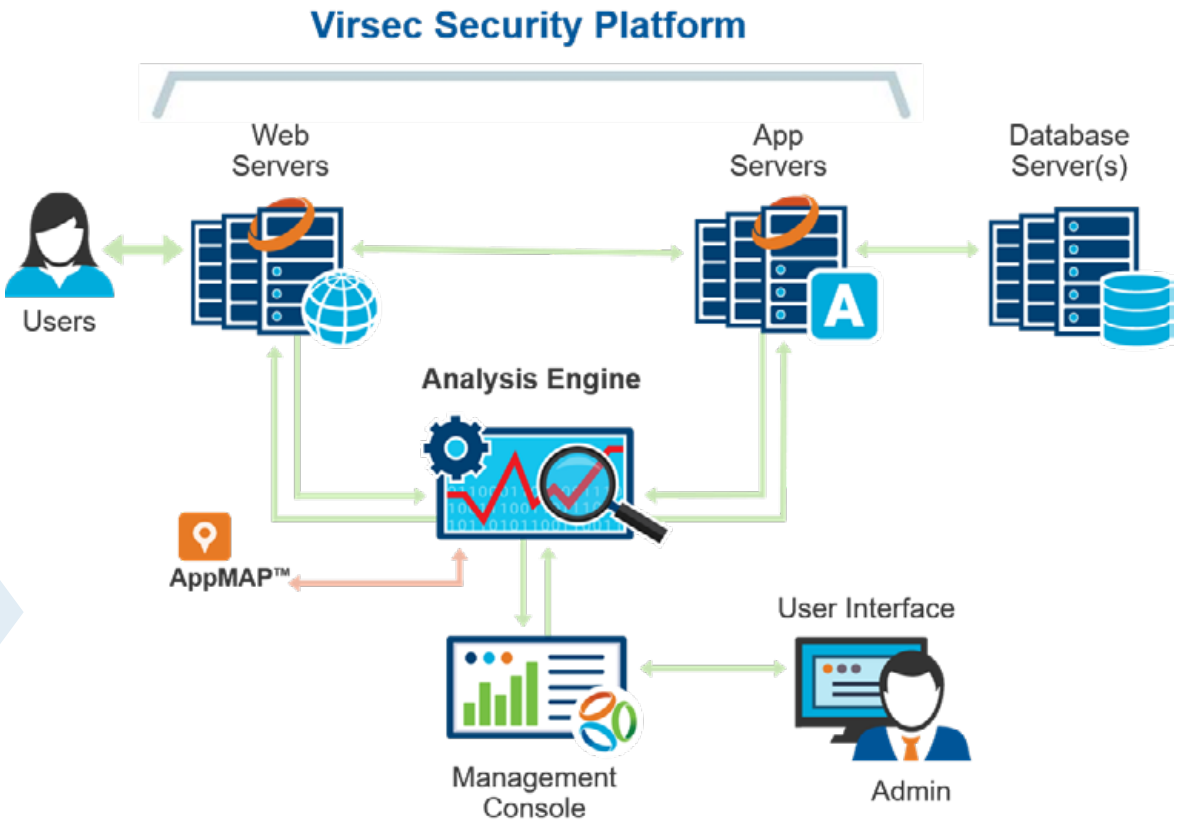
Key Feature Summary

- **Fileless, Memory Attack Protection**
  Detects sophisticated memory attacks delivering true zero-day protection
- **No False Positive Approach**
  Trusted Execution™ is a deterministic, signature-less approach that achieves near perfect accuracy
- **Web Application Protection**
  Precisely detects web app attacks in Java, .NET and most server-side languages
- **Third-Party Component Protection**
  Extends protection to any app without requiring source code, including legacy, public-facing, internal, commercial and open source
- **Easy to Deploy**
  Apps are instrumented easily and make use of virtual or cloud analysis engines, with no impact on developers

Trusted Execution™

Trusted Execution delivers granular protection at the memory and CPU levels to ensure that critical systems are not compromised. Any application binary, whether legacy or actively being developed, can be protected in memory instantly and without requiring access to source code. Rather than relying on signatures of past malware, Trusted Execution precisely maps the known and predictable activity of an application, creating an AppMap™. When the application runs, Virsec monitors all system, file, and memory activity and proactively takes action if the application goes off the rails.

This provides Virsec's unique ability to detect and block memory corruption attacks such as buffer overruns, return-to-libc exploits, and ROP or JOP chain attacks. The solution also detects fileless web exploits such as SQL injection and DLL hijacking. Trusted Execution delivers near 100% accuracy at detecting memory-based attacks on your applications. Because there are virtually no false positives, and precise attack information, alerts can be acted on with confidence.

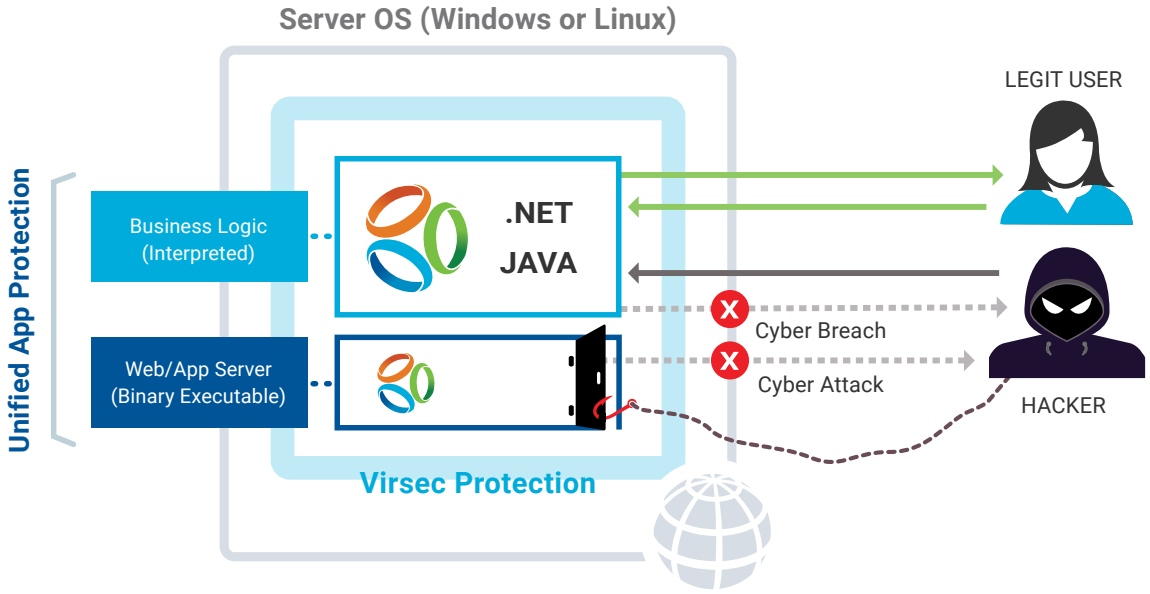


Full Stack Application Protection

Virsec extends runtime protection to the full application stack, from the memory layer up to the web and business logic layer. As organizations increase the surface area of their business-critical data through public facing web applications, it is critical that these applications be secured from top to bottom. The platform provides complete protection from web application attacks such as SQLi and cross-site scripting (XSS), which are often used for data exfiltration.

Despite years of investment in security technologies, web application vulnerabilities are increasing. The wide-spread use of third-party components, in many cases without access to underlying source code, exacerbates the problem. Secure SDLC practices never yield perfect results, leaving inevitable vulnerabilities in enterprise applications.

Virsec enables organizations to protect applications at runtime in a way that eliminates these problems. The solution works on key server-side programming languages, including those where source code is not available, whether or not a vulnerability has been previously identified. This provides effective zero-day virtual patching on web applications so organizations don't have to hope for a perfect SDLC process.



Comparison of Cyber Security Approaches

FEATURES	VIRSEC	ENDPOINT SECURITY	APPLICATION SECURITY
Server Endpoint File System Protection	✓	✓	
File-Less, Memory-Based Attack Protection (on Binaries)	✓		
Web Application Attack Protection	✓		✓
Continuous Protection of Changing Web Applications	✓		
Non-Signature-Based Approach	✓		
Definitive, No False Positive Technology	✓		

About Virsec Systems, Inc.

Virsec definitively prevents zero-day cyberattacks from sophisticated memory corruption hacking attacks such as ROP chain exploits and buffer overruns. Virsec utilizes a patented, innovative approach known as Trusted Execution™ to deterministically stop these advanced security attacks without false positives and delivering near 100% accuracy. Virsec extends this precision to the protection of web applications from important web app attacks such as SQL injection (SQLi) and cross-site scripting (XSS).

More information can be found at www.virsec.com.

Virsec®

Headquarters:

226 Airport Parkway, Suite 350 • San Jose, CA 95110

Email: info@virsec.com • Phone: (877) 213-3558 • Web: www.virsec.com • Twitter: virsecsystems