virsec

Solution Brief

PROTECTION AGAINST ADVANCED WEB ATTACKS

Defending against attacks that bypass conventional security

Sophisticated attacks on applications are increasingly challenging security and IT teams and posing grave threats to businesses and their customers. Attacks on power grids, malware strikes on plants, data breaches like Equifax, attacks on banking systems and global ransomware are just the latest examples of cyberthreats that are increasing in scope and frequency. These attacks should worry enterprises of all types and drive teams to evaluate areas of weakness in their existing security systems where attackers can bypass existing defenses.

Targeted attacks by highly-skilled and persistent cyber criminals are a business reality and threaten enterprises daily. Attackers are using a variety of complex schemes and new techniques to infiltrate networks and manipulate applications to steal data or damage critical systems. Conventional security tools, such as WAFs, are ineffective at stopping advanced evasive attacks on composite web-applications, especially when criminals use stolen credentials to access applications on the network and target memory, process flow and application data in memory.

VIRSEC APPLICATION DEFENSE

Virsec® Security Platform delivers ground-breaking application defense that protects enterprise applications from web to memory. With a unique deterministic approach, Virsec provides real-time protection from inside application server environments, stopping evasive malware, memory corruption attacks, attempts to change binaries and malicious injections. It effectively prevents advanced attacks that move laterally across the network and could otherwise persist for months or years.

Enterprise Security Teams Require:

- Application-Centric Security
- Full-Stack Application Protection
- Rapid Disruption of the Attack Lifecycle
- Actionable Attack Visibility & Attribution

Virsec Security Platform defends applications at the code level by analyzing request transactions and compiled code during execution and in memory, ensuring application integrity. It closes windows of exposure and stops exploits at the onset of an attack. Security teams gain visibility into events typically not seen, enabling rapid response, recovery and effective risk management. With Virsec, organization are more confident that they have the right security controls in place to prevent attacks that threaten business, customer data and critical web services.

APPLICATION-CENTRIC SECURITY

Virsec enables true application-centric security that ensures the most effective defense against attacks on datacenter and cloud applications.

IT and SOC teams can configure protection based on the application, its underlying business logic and supporting resources. Using Virsec's patented Trusted Execution™, the platform examines user inputs and the full transaction pipeline. It also analyzes processes within core processor-memory functions and validates libraries and file systems, all in real time. The combined capabilities and deep visibility into the full application structure enables instant identification of compiled-code tampering, complex SQL injections, DLL attacks, memory corruption and unauthorized branching within instruction sets. All of this is done without extensive provisioning steps, machine learning, or sandboxing. App-centric security from Virsec provides deep visibility into application functions, with the means to uncover and audit the most evasive threats continuously and with zero false positives.

Trusted Execution™

Virsec Security Platform is built on Trusted Execution technology, which performs deep analysis of requests and responses with additional defenses at the memory and CPU levels to ensure business-critical applications are not compromised. Compiled code, 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™ of process flow in memory. Virsec monitors all system files and memory activity against the AppMap, and proactively takes action if the application goes off the rails.

Virsec has the unique ability to detect and block memory corruption attacks, such as buffer overruns, return-to-libc exploits, and ROP or JOP chain attacks. It also detects fileless exploits including SQL injection, XSS and DLL hijacking. Trusted Execution delivers near 100% accuracy in threat detection, which translates into virtually no false positives and greater confidence in attack alerts.

FULL-STACK APPLICATION PROTECTION

Virsec extends runtime protection throughout the full application stack. Whether a suite of closely related applications supporting specific services or composite infrastructure software, Virsec ensures security for most applications that drive business. Virsec protects programs developed in various languages, including those where source code is not available and whether or not a vulnerability has been previously identified. It also protects data delivered between processes, services and resources to stop breaches and malware execution. Full stack defenses provide effective security across each app component at runtime and in a way that patches vulnerabilities that weren't addressed with software development, yielding an uncompromising defense from all OWASP 10 and dangerous exploits like WannaCry, Triton and those posed by Spectre and Meltdown.

RAPID DISRUPTION OF THE ATTACK LIFE CYCLE

Breaking the attack lifecycle remains a challenge as advanced attacks continue to evade detection, facilitating deeper reconnaissance and giving way to attack progress. Adversaries are thinking outside the box and employing multiple fileless techniques and code injections to exploit application flaws, escalate privileges, manipulate legitimate processes and corrupt memory, in order to extract valuable information or damage systems. These advanced attacks fly under the radar of conventional security tools like AV, WAFs, IPS and other solutions that rely on signatures and pattern matching.

Attack Life Cycle

1. Attackers scan for human and system vulnerabilities
2. Determine method for delivering attack
3. Exploit vulnerability and gain initial entry point
4. Escalate privileges & insure persistence
5. Establish command channels, take control of system and instruct attack
6. Execute and manage attack with continued command channel use, ensured persistence, system control and instructions

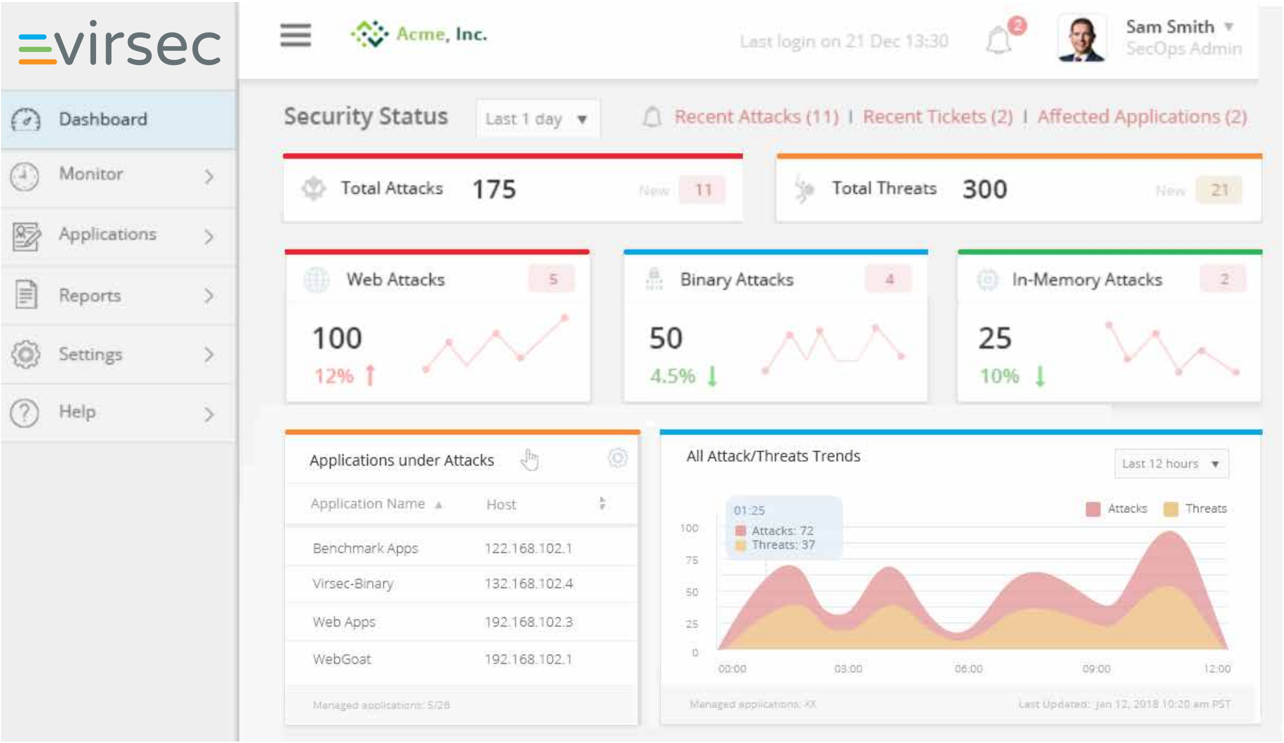
Virsec Security Platform focuses less on chasing threats and more on ensuring the integrity of application code and execution. By ensuring normal application process flow, Virsec provides the most effective means of interrupting the attack in real time.

Our unique approach prevents efforts at exploiting code vulnerabilities and manipulating existing programs even with privileged access and commonly acceptable tools. By monitoring both interpreted and binary code execution, Virsec identifies corrupt data, memory usage and illegitimate process execution upon the onset of attack exploits. It effectively brings a halt to malicious activity—stopping efforts to hide, inject and execute malicious code, exfiltrate data, affect application behavior and move between systems in a compromised environment.

ACTIONABLE ATTACK VISIBILITY & ATTRIBUTION

Virsec delivers a powerful, real-time visibility tool that allows enterprises to focus on what matters most. Operators can receive notifications and alerts of attacks in real time, readily view security trends and easily distinguish attacks from threats and incidents using a web-based dashboard that provides insight across the entire application perimeter. At-a-glance dashboard tables, charts and gauges summarize information over time and provide drill downs to forensic data for all events.

Security teams benefit greatly from rich attack details that help pinpoint attack source, method, affected application process and more, while aiding audits and investigations, helping ensure attribution and providing a consolidated view across the entire threat field.



Security Status Last 1 day ▼ Recent Attacks (11) | Recent Tickets (2) | Affected Applications (2)

Total Attacks 175 New 11

Total Threats 300 New 21

Web Attacks 5
100
12% ↑

Binary Attacks 4
50
4.5% ↓

In-Memory Attacks 2
25
10% ↓

Applications under Attacks

Application Name ▲	Host
Benchmark Apps	122.168.102.1
Virsec-Binary	132.168.102.4
Web Apps	192.168.102.3
WebGoat	192.168.102.1

Managed applications: 5/26

All Attack/Threats Trends Last 12 hours ▼

Managed applications: XX Last Updated: Jan 12, 2018 10:20 am PST

VIRSEC MANAGEMENT CONSOLE

- Real-time information
- Dashboard summaries—attacks, threats and incidents
- Quick trends—attack or app types
- File integrity failures
- Custom and canned reports
- Detailed forensic data logging

Virsec Security Platform

Virsec Security Platform secures the entire application from memory to the web as attacks happen, identifying OWASP Top 10, advanced targeted attacks, unknown threats without signatures, DAST/SAST integration, additional emulators and intelligence services. With Virsec, enterprises can effectively harden applications from the inside to prevent malicious activities, while ensuring application integrity, API enforcement and continuous authorization in the face of a threat.

Virsec Security Platform complements existing security solutions and increases the value of your entire security investment. It provides additional defense against advanced attacks that aren't commonly detected by traditional security solutions. With each attack or threat detected, the platform ensures precise attack attribution with detailed forensic data captured during execution. Attack information can be leveraged by existing firewalls, access control solutions, application delivery controllers and cloud-based security services to prevent subsequent attacks from ever reaching the server. Virsec Security Platforms provides enterprises with increased confidence that business services, applications and high valued information are protected from the most advanced targeted attacks today and tomorrow.

Key Capabilities	Virsec Security Platform	RASP	WAF
Web Application Protection	X	X	X
Fileless, Memory-based Attack Protection (on binaries)	X		
Server-side File System Protection	X	X	
Automatic Defense Against Evolving Attacks	X		X
Advanced Non-Signature-Based Protection	X		
Definitive, No-False-Positive Technology	X		

> "Virsec stands out when compared to the most common solutions"
>
> *Paul Forney,*
> *Schneider Electric*

About Virsec Systems, Inc.

Virsec offers security solutions that definitively prevent sophisticated, unknown and zero-day cyberattacks. Our advanced technology uses a revolutionary deterministic approach to threat detection that stops complex and sophisticated attacks on critical applications in real time with near 100% accuracy. Virsec uniquely provides the only single solution that protects against common vulnerability exploits and the most sophisticated threats like Spectre and Meltdown. Contact us to learn more about our technology.

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

virsec®

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