Virsec® Overview

Full Stack Application Protection from Advanced Cyberattacks

Virsec is an innovative cyber security leader protecting organizations from today’s most sophisticated and dangerous cyberattacks. Through its unique technology Virsec protects business-critical applications from zero-day threats, fileless attacks and memory corruption exploits that fly under the radar of most security solutions.

Today’s Security Challenge
The latest wave of fileless, memory-based attacks are effectively invisible to conventional security controls. They manipulate legitimate application processes, corrupt memory, and hijack control of applications to steal or ransom data. Recent attacks including WannaCry, Petya, Industroyer, and others have all exploited fileless techniques which are indefensible by technologies that depend on pattern matching of known threats.

Trusted Execution™
The Virsec platform is unique in securing any type of mission-critical application in real time, as close to the application and processor as possible. Through its patented Trusted Execution technology, Virsec maps exactly what an applications is allowed to do and uses a deterministic process instantaneously detect if a process has been compromised.

Key Benefits
Virsec provides peace of mind to businesses struggling to keep up with today’s threats with a platform that delivers:

- **Unrivaled accuracy**: scored 100% accuracy with zero false positives, in identifying attacks cataloged by the OWASP Benchmark Project
- **Lower TCO**: helps you consolidate redundant security layers and reduce managed costs by eliminating false positives
- **Full stack protection**: real-time security with deep application integration covers web apps, interpreted apps, files, processes, and binaries
- **Reduced risk levels**: delivers precise protection with actionable forensics for any applications including internal, legacy or public web apps
- **Support for unpatched servers**: completed security for legacy apps regardless of whether patches or operating systems are up-to-date

Why Virsec

- **Security Innovation**: Patented deterministic protection stops threats to applications during run-time
- **Advanced Threat Defense**: Uniquely protects against sophisticated fileless and memory-based attacks
- **Real-Time Protection**: Deep application integration detects and prevents all anomalous behavior before damage occurs
- **Enterprise Scalability**: Secures critical applications for leading organizations in finance, healthcare, critical infrastructure, defense and government
- **Experienced Management**: Seasoned Silicon Valley team from leading companies such as AMD, Cisco, Palo Alto Networks, Juniper, Dell, NexGen, Forcepoint and BMC
Virsec® Security Platform
For Industrial Control Systems (ICS)

Industrial environments and critical infrastructure are increasingly at risk of attacks from advanced malware like Industroyer, Stuxnet, BlackEnergy, Triton and NotPetya that are designed to cripple operations, cause outages and affect populations.

Nation-states and cybercriminals have turned their focus towards unpatched vulnerable ICS/IT/OT/SCADA systems that control critical operations and processes essential to services that drive the economy and ensure energy, health, safety and national security systems.

Using attacks that weaponize at runtime in application memory (i.e. registry attacks, ROP, DLL injections, fileless exploits), attackers evade traditional security to get a foothold on vital systems, then exploit communication links between corporate, IoT and control system networks. Attacks persist for months (or years) before discovery—inflicting substantial damage and causing great losses.

Virsec provides a breakthrough deterministic approach to protecting critical infrastructure against memory-based attacks with real-time detection that alerts within milliseconds. Virsec optimizes threat detection for hard-to-patch Windows and Linux based OT/IT/ICS systems during runtime, effectively closing down the window of exposure for industrial applications and critical infrastructure operations.

ICS Attack Protection

Virsec ICS protection with patented Trusted Execution™ technology monitors compiled binary code in memory during execution to prevent crippling attacks. It uniquely detects exploits of critical functions, process memory, and the CPU with accuracy. It also generates alerts of all detected attacks, notifying security specialists and enabling rapid remediation without further analysis. Virsec monitors compiled ICS applications (modern and legacy) and acts as a memory firewall, preventing misuse of memory that gives way to unauthorized deviations in code processing and malware execution.

Why VIRSEC

- Hardens applications from the inside, increasing operational integrity without re-compiling code
- Only technology that protects against Spectre/Meltdown without upgrades and minimal performance impact
- Most advanced application defense protecting against known, unknown and evasive memory-based attacks
- Precise forensics from unique deterministic threat detection delivering unsurpassed accuracy
- Ensures application integrity in the face of an attack with Trusted Execution™ technology

Key Benefits

- Defends against crippling attacks aimed at ICS, SCADA, MES, PLC, HMI, Historian, EW services
- Protects internal, legacy and modern applications from attacks invisible to traditional security
- Prevents APTs & lateral movement throughout the industrial environment
- Eliminates false positives with accurate threat detection, even on first attempt
- Complements existing network security solutions to prevent attackers from ever reaching servers
- Enforces pre-emptive vulnerability patching of hardware and software flaws without signatures
Deployed without recompiling or accessing source code, Virsec ICS solution provides an immediate defense to the most crippling attacks on ICS services while ensuring application integrity and continuity of services in the face of a threat. Virsec effectively hardens critical infrastructure and control systems from the inside and helps organizations avert substantial damage and mounting losses.

**Virsec ICS Offering**

- **Features and Capabilities**
  - Memory-based attack defense
  - Compiled code attack detection
  - Unknown threat discovery (Basic)
  - Code integrity defense (Basic)
  - Buffer overflow
  - Fileless malware
  - Full request & response examination
  - Industroyer, Meltdown, TRITON defense
  - File system protection
  - Automatic attack mitigation

**Visualization | Reporting | Monitoring**

- Real-time Dashboard reporting
- Detailed event logging
- External ticketing system support
- SMS & email alerting

**Product Specifications**

- Flexible deployment VM or bare metal: VMware ESXi Hypervisor, x86
- 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: HTTP/HTTPS/REST/AJAX/SOAP/XML/JSON
- Web Application Server environments: WebLogic, Apache Tomcat, JBOSS, WildFly
- Technology frameworks: Spring, Apache, Hibernate
- Databases: Oracle, MySQL, PostgreSQL, H-SQL etc
- Email and SMS alert: Yes
- External ticketing system: Yes

---

**Use Cases**

**Critical Infrastructure Defense**

- Securing critical infrastructure and control systems

**In-depth Application Protection**

- Always-on defense against unknown and advanced attacks

**Pre-emptive Patching**

- Patching design flaws before vulnerabilities are discovered

**Risk Reduction**

- Ensure rapid response and full visibility into attacks early in the attack lifecycle
Raytheon and Virsec Partner to Guard the Grid

With energy grids under constant threat of cyberattack, Raytheon is getting the technology of small, innovative software firms into the hands of big international customers.

The malware that blacked out parts of Kiev, Ukraine, was a ticking time bomb.

It slipped inside the networks of electrical substations through a flaw in an obscure device. It built back doors to other parts of those networks and waited. Then, at a time chosen by its programmers and written into its code, it destroyed. It commandeered circuit breakers, shut down relays and hobbled the control software.

The malware, known as both CrashOverride and Industroyer, showed how hackers not only understand the arcane networks of the energy industry, but are using that knowledge to carry out devastating cyber offensives. It also showed how urgently the keepers of critical infrastructure need to shore up their defenses.

To speed that along, Raytheon is working with smaller companies like Silicon Valley cybersecurity firm Virsec to license network-saving technology to government agencies and large enterprises including healthcare companies, financial institutions and utility providers. That partnership answers a call in the U.S. National Defense Strategy for the defense industry to deliver new technologies faster. For Virsec, it also accelerates the long, difficult acquisition process smaller companies often encounter when breaking into the federal and international markets.

"Raytheon is clearly adept at changing that paradigm and bringing newer technologies and solution sets more quickly to its customer base," said Ray Demeo, co-founder and chief operating officer of Virsec. "Without partners like Raytheon, the U.S. government would not be able to access essential and immediately needed technology. And this is important to all of us and its allies as citizens, the ability to change our defense posture. It really is a day-to-day battle."

At the heart of the Raytheon-Virsec agreement is a defense against "memory-based" cyberattacks, or those that exploit weaknesses in legitimate applications, rather than installing malware. Well-known examples include the WannaCry and NotPetya ransomware attacks, which exploited a PC feature called Server Message Block that allows computers on a network to access shared resources such as printers.

Virsec calls its defense against memory-based attacks "Trusted Execution," and it basically works like this: It learns what applications should and shouldn’t do, and when it sees an application executing an abnormal script, for example, it flags the activity and sends an alert that enables security to shut down the rogue function immediately.
The technology could fill a critical need, said John DeSimone, vice president of cybersecurity and special missions at Raytheon.

"Commercial tools from companies like Virsec can help bridge the gap for our global government and commercial customers and provide effective protection against the growing cyber threat," he said.

About Virsec

Virsec is an innovative cyber security leader protecting organizations from today's most sophisticated and damaging cyberattacks. Through its unique technology, Virsec definitively prevents zero-day threats, fileless attacks and memory corruption exploits that are invisible to conventional security tools. Virsec's patented Trusted Execution™ system deterministically stops advanced security attacks in real-time, delivering unprecedented accuracy, without false positives. Virsec is headquartered in San Jose, California with a global presence in Europe, Asia, and Australia.

Author: John Zaremba, Raytheon
Winning Against the “Indefensible Attack”

Introduction

The next ‘Pearl Harbor attack’ will include attacks on private sector functions, including those supporting our daily lives. Attacks on industrial systems are adversely effecting production processes in critical infrastructure environments at an increasing rate. And a vast majority of industries still lack adequate cyber security controls.

Against this backdrop, providers of Industrial Control Systems (ICS) software recognize the need to increase security measures on solutions that power much of the country’s critical infrastructure. In an environment where nation-states are investing heavily in building out cyber warfare capabilities, the pressure continues to mount.

Background of Customer Application

Virsec has been working with a leading global provider of ICS Supervisory Control & Data Acquisition (SCADA) software and solutions to protect control system software from memory-based, binary attacks. The legacy solution for protecting ICS applications has been Application Control (file whitelisting), but this leaves these critical systems exposed to a significant class of “indefensible” attacks—fileless, memory-based.

The following constraints and concerns were paramount for this organization and its global customers:

1. Increasing operational technology (OT) and IT convergence over the past decade for operational efficiency of industrial control systems has increased the risk of malware infections and malicious activity at OT systems are no longer “air-gapped” from the internet.

2. Safety and reliability are paramount for critical SCADA systems like the power grid, with which often require 100% uptime. This makes patching software and updating signatures in security products difficult and expensive.

3. Much of the SCADA world is run on legacy Windows platforms that are end-of-life at this point. These systems are often compiled for 32-bit operation as opposed to newer 64-bit architecture. Given the relentless focus on uptime, availability and costs, getting more life out of existing and legacy solutions is important.

4. Relying on IT organizations for the security of control systems is a major deterrent to adoption of new solutions. Security must be seamlessly integrated into OT systems and easily accessible to control system engineers. Even the legacy Application Control solution which did not rely on an Internet connection, was more cumbersome to implement than expected.
System Architecture and POC Environment

The customer was primarily concerned about a class of attack their security experts were finding to be “indefensible”—memory-based attacks on known or unknown, zero-day vulnerabilities that could bypass an Application Control whitelist or Anti-Malware products and take malicious action. For example, the Stuxnet malware took advantage of over 20 zero-day vulnerabilities and caused systems to report erroneous data back to control system engineers.

Figure 1 shows a typical ICS system. Tier 0 includes I/O devices such as sensors, actuators, Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCSs).

Tier 1 is the Supervisory SCADA layer, which includes functional components like a Central Object Repository, Application Servers, Tier 1 Historian, Human Machine Interface (HMI), Engineering Workstation, etc. They configure, monitor and control the elements in Tier 0 while feeding information to the upper tiers. These components reside on Windows-based servers that aggregate information or perform specific functions in the solution such as logging live data (alarms and events) received from Application Engines, the HMI or the operator station, and being the repositories holding factory configuration information.

Tier 2 is Web-facing and generally segregated from Tier 1 by a firewall. Here information is aggregated and made available to analysts connecting from a corporate location through an Intranet. At this tier, vital servers such as a Tier 2 Historian can aggregate information from various Tier 1 Historians and an Information Server acts as web portal to visualize information from factory systems. In addition, the Microsoft SQL Server typically provides the persistent data repository and is also susceptible to attack.
Vulnerability and Attack Concerns

The customer was particularly concerned about DLL Hijacking and memory-based attacks such as Library Injection. For example, with DLL Hijacking, an attacker might swap a language support DLL (for internationalization) with a compromised DLL which could open a reverse shell in addition to performing all the expected localization functions.

In addition, zero-day attacks on unpatched Microsoft components, like SQL Server, were also a concern. In these environments, automatic software patching generally turned off due to uptime constraints.

Figure 2 shows the ICS-SCADA environment used for the tests of the Virsec Security Platform (TM). The primary OS was Windows Server 2012 running on VMware ESX VMs on off-the-shelf servers.

![Figure 2: POC Deployment Architecture](image)

The customer’s Chief Security Architect tested capabilities for detecting "indefensible" memory-based attacks like library injection and buffer overflow exploits using its Trusted Execution approach. They also evaluated how Virsec could extend or improve existing Application Control options for the ICS-SCADA solution.

Results

In order to validate the solution, the customer uses the Virsec Application Integrity Protection, to protect Windows application components from memory-based attacks.

The key performance metrics were:

1. Efficacy of attack detection
2. Performance impact
Specifically, the customer tested Virsec’s claims of near perfect accuracy and performance impact of less than 5% additional CPU utilization.

A key aspect of protection Virsec provides was the ability to protect both 32-bit and 64-bit Windows applications, particularly during complex mixed-mode initiation paths where child processes of ancestor processes might change in mode support. Given the use of legacy Windows and application types in ICS-SCADA, this was a key requirement for a runtime execution protection product. To measure the performance impact, measurements were taken both with and without Virsec.

To measure accuracy, a DLL injection attack was staged on every component of a protected application, along with a proprietary exploit on a buffer error vulnerability that the customer had recently encountered.

**DLL Injection Attack Detection**

**Runtime Execution Integrity.** The system was subjected to a simulated DLL Injection attacks by using the “Syringe” utility, which can be used by hackers to inject malicious code into running applications.

In all cases, regardless of where in the application sub-process chain the attack took place, Virsec detected the malicious event immediately. Virsec’s memory corruption and memory-based attack protection is deterministic and detects even non-malware, fileless memory attacks the moment the normal execution path is subverted.

**File Integrity Monitoring,** which uses checksum and disk location checks of application components to detect potential attacks. For example, threat or attack alerts can be raised when unknown or tampered-with application libraries are discovered when being loaded into memory, or when a malicious DLL that violates file integrity is dropped into the application’s home directory. It also flags changes to file system attributes like file modification timestamps, ownerships, etc.

**Average Performance Impact**

Given reliability and uptime requirements for ICS-SCADA systems, ensuring a low performance impact on the protected application components was a key requirement for the customer.

Measurements were taken over long periods of time, ranging from 90 minutes to several hours to determine the average CPU impact of the Virsec solution on the customer’s ICS software. In all cases, Virsec protection added less than 5% to the CPU load.
**Conclusion**

Virsec Security Platform with Trusted Execution technology delivers breakthrough ICS-SCADA security designed to meet stringent critical infrastructure requirements.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Virsec Requirement</th>
<th>Virsec Security Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>100% ICS system uptime without reboots of OS servers</td>
<td>No OS reboot required. Does not depend on signatures packages being delivered</td>
<td>Detects zero-day, or fileless attacks in microseconds</td>
</tr>
<tr>
<td>Windows patches installed infrequently</td>
<td>Does not depend on the latest application patch being applied</td>
<td>Detects zero-day attacks against any application including unpatched binaries</td>
</tr>
<tr>
<td>Support for legacy Windows versions including 32 and 64-bit application processes</td>
<td>Binary protection supports legacy Windows versions and any 32-bit and 64-bit applications</td>
<td>Protects runtime execution integrity of all 32-bit or 64-bit applications and all subprocesses.</td>
</tr>
<tr>
<td>Seamless enablement of security within ICS-SCADA</td>
<td>Exposes attack alerts via RESTful API for integration</td>
<td>Seamless integration of ICS security protection into control system interfaces</td>
</tr>
</tbody>
</table>

Virsec Security Platform successfully demonstrated protection from “indefensible”, fileless, memory-based attacks which easily bypass Application Control whitelists or Anti-Malware products. The solution detected DLL Injection and buffer error vulnerability attacks 100% of the time, with CPU performance impacts well under 5% under various load conditions.
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.

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, organizations 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.

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.

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.

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.

**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.

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

“Virsec stands out when compared to the most common solutions”
“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.