virsec

Solution Brief

ICS-SCADA SECURITY

Protection for Critical Infrastructure Services and Information Systems

Industrial Control Systems (ICS) are the backbone and supportive foundation of every industry and nation. A single compromise can result in devastating physical, financial and environmental damage impacting thousands and amounting to millions in losses.

Advanced cyber attacks like **Stuxnet, BlackEnergy, Triton**, and **Industroyer** that weaponize at runtime in application memory are posing an increasing risk to critical infrastructure and industrial environments. The level of sophistication and frequency of these attacks continuously challenge operation and security teams, as they bypass traditional security—making threats on critical infrastructure seem indefensible.

Protection against attacks, blind spots, and internal negligence or bad actors is a top concern, requiring a new generation of tools that continuously secure critical application operations, protect memory and reduce risk while helping to drive responsive actions that ensure safe, reliable system operations.

VIRSEC ICS SOLUTION

Virsec ICS provides disruptive cybersecurity that safeguards ICS/SCADA/IT/OT systems from advanced targeted cyberattacks that enter the system without a trace to affect processes, registries, libraries, and memory. Virsec effectively prevents attackers from gaining control of memory space or registers, inserting malicious code into memory and orchestrating attacks by executing malicious code, allowing them to assume full control of critical systems. Virsec uniquely identifies memory misuse and changes to application libraries, then initiates responsive actions for immediate protection—providing in-depth protection where necessary memory execution protections fail.

Virsec ICS provides disruptive security for sectors including:

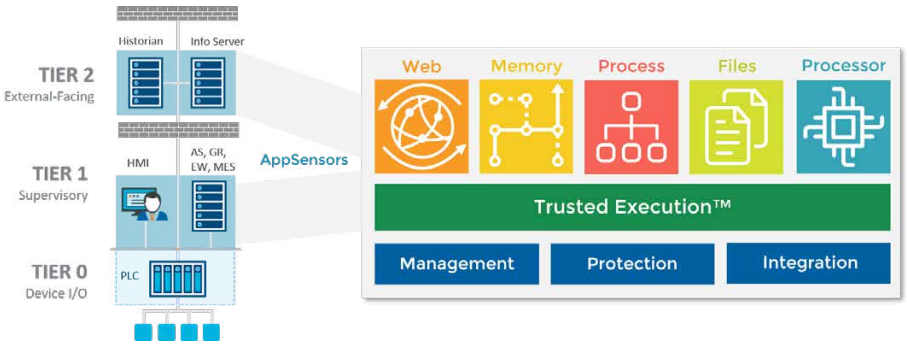
- **Government & Defense**
- **Oil & Gas**
- **Transportation & Logistics**
- **Power & Energy**
- **Water & Wastewater**
- **Chemical**

Built on patented Trusted Execution™ technology, Virsec Security Platform secures the entire ICS system stack from human error, internal threats and targeted external attacks aimed at specific ICS components at each level in the infrastructure. Virsec ensures supervisory and operational systems, including human machine interface systems (HMI), process control software, instrumentation and Historian functions without compromise even when under threat.

COMPREHENSIVE PROTECTION FOR ICS

Using real-time, deterministic threat detection that accurately identifies malicious memory-based events at runtime, Virsec can automatically

protect ICS systems from malicious actors that leverage flaws in chips, code, tools and applications that expose critical infrastructure services, processes, management interfaces and controls to dangerous exploits.

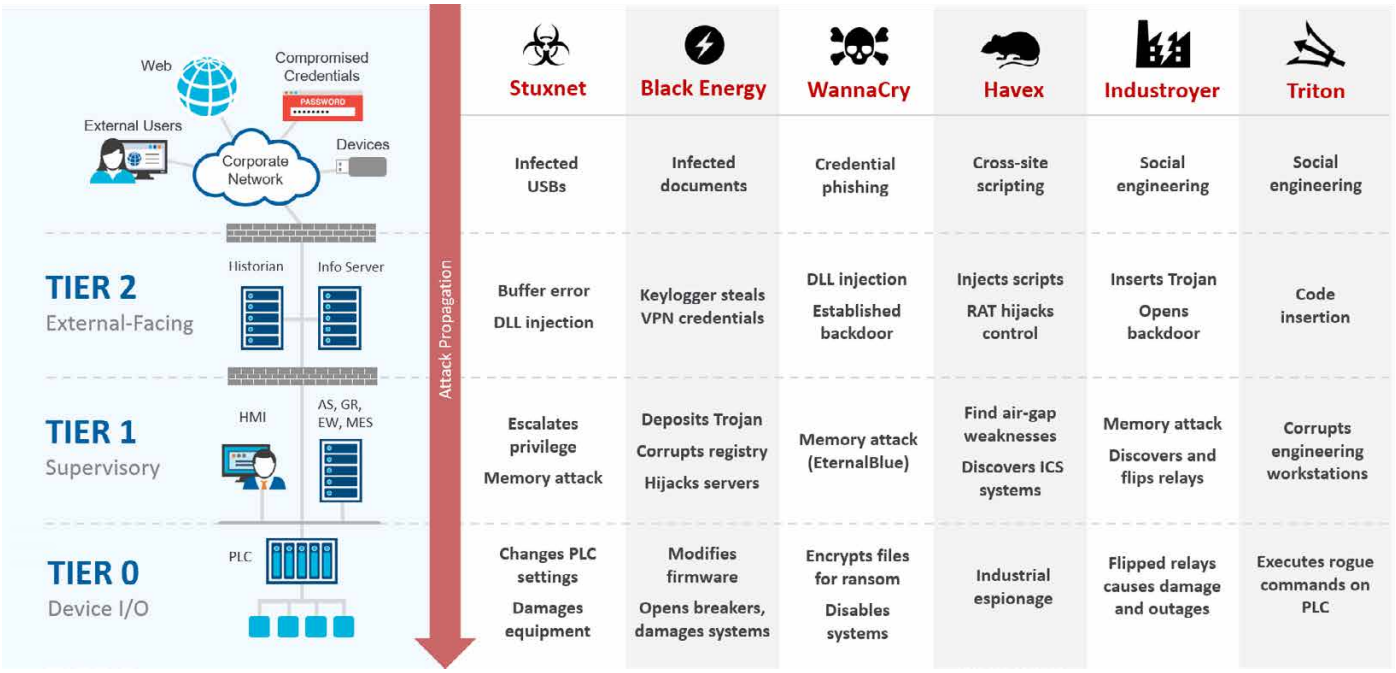


Deployed where the application resides, Virsec operates deep within the application system realm, thwarting attacks in memory and as code and commands execute. Virsec ISC can be extended with enterprise capabilities to secure not only compiled/ binary code, but interpreted code and microcode that drives critical system processes at every ICS/SCADA tier including Web. Organizations gain assurance that complex, modern and legacy environments are protected, without dependencies on ongoing signature tuning, policy management, and up-to-date heuristics.

HARDENS ICS/SCADA SYSTEMS

Virsec Trusted Execution technology helps ensure ICS system integrity by identifying illegal or uncommon application behavior at the code and memory levels as exploits take place, preventing memory manipulation, file systems changes, malware execution, code injection, and trusted function manipulation.

With Virsec ICS, infrastructure operators and owners can harden vulnerable legacy systems and maintain functioning and resilient critical infrastructure operations in the face of uncommon known exploits, zero-day attacks and severe cyber attacks like deserialization, ROP, DLL and registry attacks. Virsec identifies attacks and instruments protections before things get out of hand.



Virsec Hardens Applications Across the ICS Infrastructure

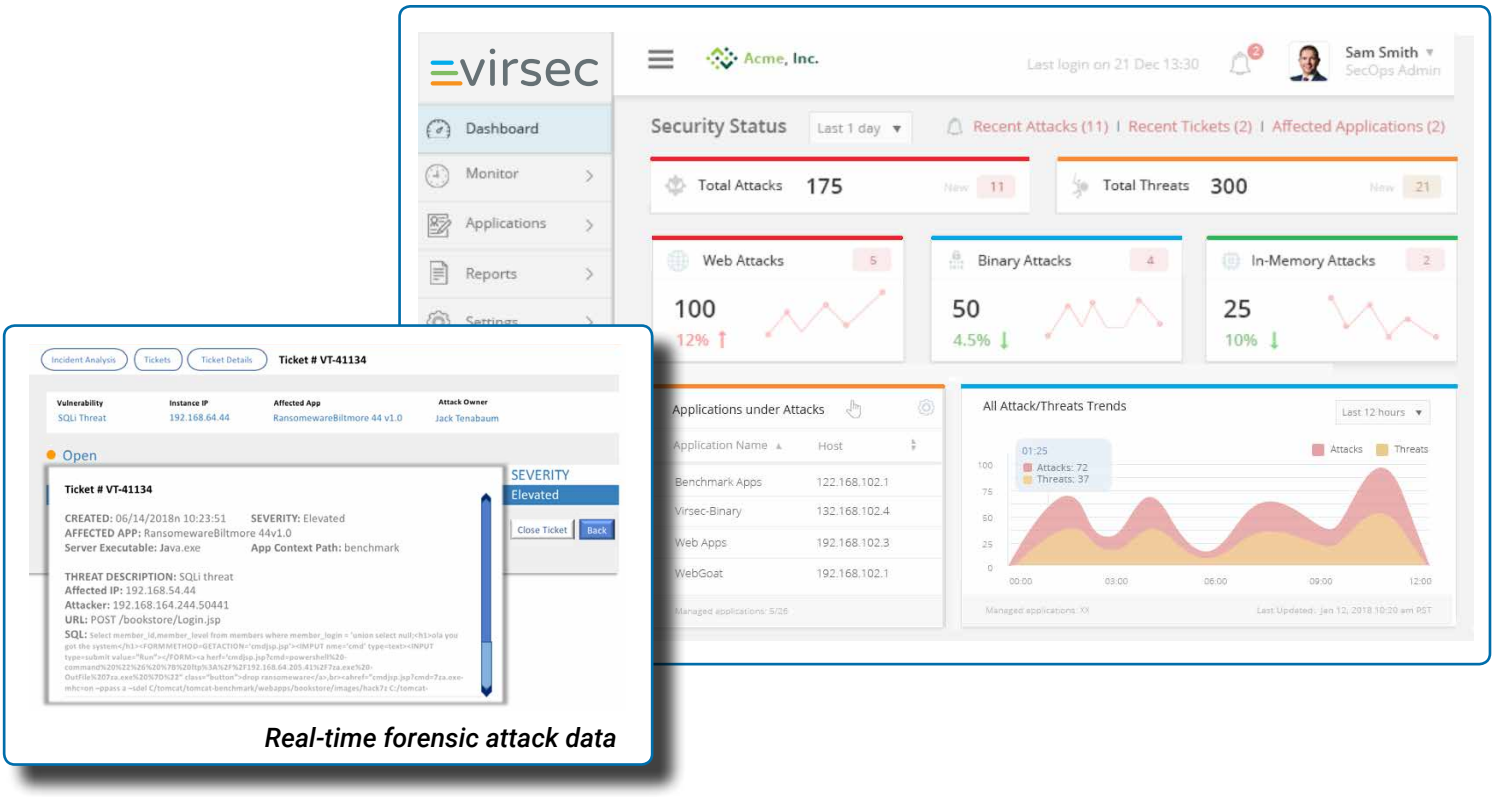
EFFICIENTLY SOLVES THE PATCHING PROBLEM FOR ICS

Virsec relieves operations teams of the rigors of patching and unscheduled downtime. The platform's unique approach to real-time threat detection, combined with automatic protective action, effectively prevents critical exploitation of known flaws and those yet to be discovered, even for variations of Spectre and Meltdown. The preemptive patching capability reduces the need for immediate and continuous patching of vulnerable hardware, software and operating systems. It further unburdens resources, while minimizing exposure to cybercriminals and risks to vulnerable critical systems, controls and safety sub-systems.

With Virsec, critical infrastructure operators gain confidence that they have proven security in place to safeguard vulnerable plants, refineries and city grids against malicious exploits that affect programmable logic controllers, human machine interfaces (HMI), industrial process devices, communications infrastructure, and the environment.

ELIMINATES SECURITY BLIND SPOTS

Virsec ensures visibility into sophisticated and uncommon attacks on ICS/SCADA services as they happen. With real-time detection, Virsec accurately pinpoints attacks in milliseconds, then performs an analytical data capture and alerts security specialists of the event. ICS security teams gain intelligent forensics that ensure full context visibility into the entire attack lifecycle from initial exploit to callback destinations and more. Virsec delivers unique insight into the entire threat scope, with increased clarity into the impact an attack has on critical services, origin, and attribution—to drive the most effective response, remediation, and investigation.



Real-time forensic attack data

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 Options

Virsec protects vulnerable IT/OT/ICS systems with three flexible software options. Download the Software Comparison Sheet to learn more about the Virsec software options and select the option that's right for you.

Enterprise

Comprehensive OT/ICS defense with Advanced Plus capabilities, added Web server OWASP 10 defense & threat intelligence monitoring

ICS

Advanced memory-based threat defense and comprehensive ICS/OT file system protection

Advanced

Files system protection including binaries for ICDS/OT environments

"Virsec stands out when compared to the most common solutions"

Paul Forney, Schneider Electric

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. Virsec provides organizations with confidence that critical services, applications and high valued information are protected from the most advanced targeted attacks today and tomorrow.

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