Datasheet

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, notifiying 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

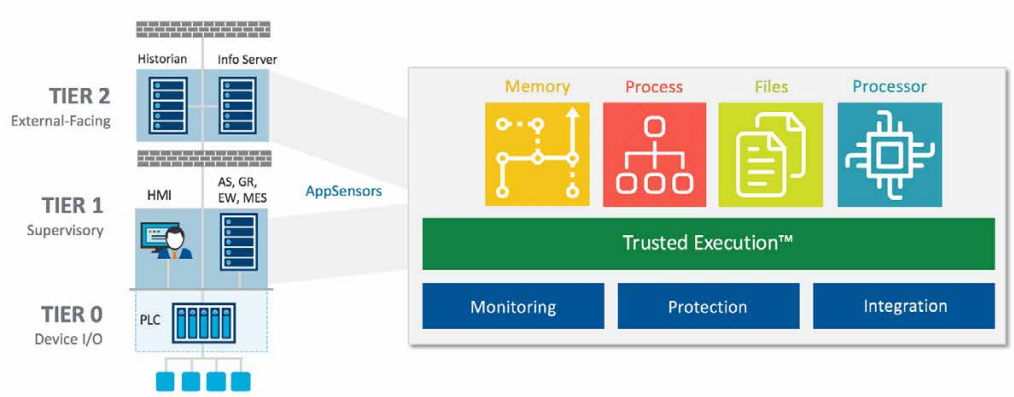
- **Hardens applications from the inside,** increasing operational integrity without re-compiling code
- **Only technology that protects against Spectre/Meltdown** without upgrades and minimal performance impact
- **Most advanced application defense** protecting against known, unknown and evasive memory-based 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