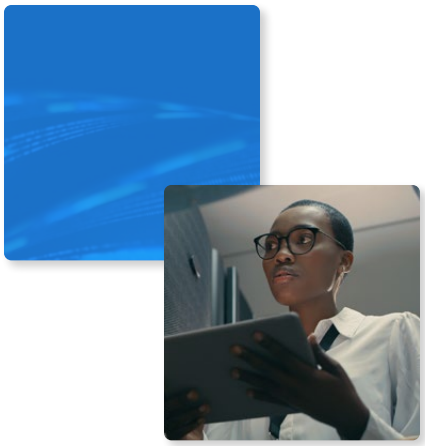
Major Water and Wastewater Treatment Facility Secures SCADA Systems

With Application-Aware Workload Protection

The Customer

One of the largest water utilities in the United States is responsible for the development and delivery of a high-quality water supply for nearly one million people. Recognized nationally for its water infrastructure development, the facility processes nearly 100 million gallons of water each day and is charged with protecting multiple water sources and providing clean, safe water to its target regions not only today but for future generations as well.

The customer had implemented AVEVA's control and monitoring solutions and sought to improve their overall ICS security. The security team wanted a tailored solution that expanded threat coverage and addressed the risk of service disruption caused by cyberattacks on utility operations and services at scattered water distribution, collection, and treatment facilities.



"Virsec has allowed us to ensure robust security for critical aspects of water district operations, as concerns about crippling attacks increase."

Director of Plant Security Operations

The Solution

The organization's decision to enhance its cyber defense strategy required a thorough evaluation of potential vendors and security platforms. Leaders considered its current infrastructure, available resources, and ongoing management requirements of vulnerabilities and configurations.

After careful evaluation, the customer selected the Virsec Security Platform for application control and memory control flow integrity (CFI), securing all aspects of their SCADA application and underlying workload components running in disparate environments.

Stop Evasive Attacks at the First Step in the Kill Chain

The Virsec solution instantly detects and stops sophisticated attacks, such as remote code execution exploits, before damage is done. This is done based on intrinsic knowledge of acceptable behavior, visibility into process control flow, and ongoing monitoring of file systems and memory.

Challenge the Status Quo

Virsec upends the status quo in cybersecurity with technology that protects critical application workloads from the inside against dangerous attacks that bypass conventional security like IDPS, EPP, and EDR. By combining deep application-awareness with automated runtime protection, Virsec instantly stops advanced attacks across the entire attackable surface of the water utility's infrastructure, without prior knowledge or signatures.

Ensure Good Vs. Chase Bad

Virsec extends and automates zero trust security across the customer's entire workload, ensuring that applications only execute as intended and are never derailed by malicious code. Rather than chasing bad, the Virsec solution ensures good by providing runtime visibility of process memory to prevent memory-based threats, fileless malware, and unknown or zero-day attacks.

Monitors file systems for unplanned file changes and malware installations

Ensures only legitimate libraries load whenever an application process is spawned

Distinguish authorized processes and detecting library injections or code that are not part of either an executable or core app component

Curtail malicious efforts to hijack, compromise, or leverage critical system files

The Results

With Virsec installed, the water utility stakeholders were assured that their applications were protected from the inside with runtime visibility and zero dwell-time. Automated protections instantly counter attacks on vulnerable aspects of their system. The customer can now respond immediately to attacks, whether known or unknown, at the earliest point of insurgency, while protecting the integrity of their most critical workloads.

Full-Stack Protection

The customer's entire application stack is now protected against advanced attacks at runtime across host and memory layers. Any memory-based attacks, fileless exploits, and filesystem changes levied against the utility's infrastructure are stopped at the first step of the kill chain. This added a critical layer of self-defense for their essential operational processes, integrated components, and services.

Secures SCADA Systems and Operations Control Technology

The Virsec solution hardened the customer's AVEVA System Platform, including Historian, SCADA, and HMI cyber exploits and ransomware.

Protection for Legacy Applications

The customer's legacy applications are fully protected because the Virsec solution prevents vulnerabilities from being exploited, regardless of the platform or patch status.

Continuous Operations

The water utility's systems are protected from the broadest range of attacks, especially those bypassing their existing endpoint and EDR solutions, while their operational integrity remains intact. Out-of-the-box protection does not require signatures, learning, tuning, or policy updates.

Scalable, Lightweight and Easy to Manage

Virsec's lightweight, scalable security solution simplified management for the water utility's stakeholders and reduced resource consumption and operational costs. Once deployed, the Virsec solution mapped all acceptable application and software execution, providing continuous, automated protection across the entire workload. Any deviation from the norm is detected within milliseconds, treated as a threat, and stopped.

Cybersecurity Redefined

The water utility facility now has full, automated protection across their entire application workload attack surface at the host and memory layers. With full visibility and control at runtime, they have the assurance that even the most vulnerable aspects of the system will be automatically defended, whether the attack is known or unknown. And their expanded, proactive threat coverage prevents service disruptions and ensures continuous operations across all their water distribution, collection, and treatment facilities.

> "Before Virsec, malicious activities went unnoticed until long after the attacks when we brought in consultants. Today we are alerted instantly, and we're able to respond immediately."

Director of Plant Security Operations

Server and Application Workload Protection

The cyber battleground today is on the server. 80% of breaches happen on the server, and the weapon of choice is the Remote Code Execution (RCE) attack. When attackers bypass perimeter and detect-and-respond security tools, Virsec prevents exploitation of software vulnerabilities in unpatched, out-of-support and modern server workloads.

Eliminate Zero-Day Threats

Protect workloads from zero-days and other unknown attacks.

Take Adversary Dwell Time to Zero

Put an end to long-term data damage and loss.

Embrace Zero Noise

Give your analysts low false positives, high accuracy.

Discover

Scan workload for all executable files

Analyze

Verify executable's reputation & dependencies

Map

Automated allow-listing & executable memory mapping

Enforce

Stop malicious code execution

(file, file-less, memory injection, buffer error & web attacks)

Securing the World's Most Critical Applications

Virsec is deployed globally protecting mission-critical applications and infrastructure in industries including financial services, healthcare, government, defense, power, oil & gas, transportation, telco, technology, and more.

Server & Application Workload Protection

Application-Aware Mapping Technology

No Signatures, No Tuning, No Noise

Zero Dwell Time

Recognition

Cyber Catalyst · CRN · Cyber Defense Magazine Global Awards 2019 Winner · Gartner · Cyber Security Excellence Awards Winner 2020 · MITRE · Info Security Products Guide 2020 Global Excellence Gold · Ovum

Customers

InfoArmor · Bottomline · GroundProbe · GreenLight Biosciences · Alabama A&M University · Karnataka Bank Ltd. · Raytheon Technologies · GE Healthcare · Boston Red Sox · LUMICELL · U.S. Department of Energy · Salvarita · Independence Contract Drilling · Bloomenergy · BROADCOM · Godrej · Gwinnett · QDB · FREEDOMPAY · TATA · inspirage · vivriti capital · SVCW · भारत सरकार Government of India

About Virsec

Virsec offers continuous protection for application workloads, stopping known and unknown attacks—including zero days. With our patented technology, we take a defense-in-depth approach with a Zero-Trust model that allows only authorized code and executables to run and nothing else. Battle-tested against 200+ of the top government red-teamers and trusted by several Fortune100 companies, Virsec has repeatedly proven a protection-first model works. Virsec is headquartered in San Jose, California, with offices worldwide. For more information, please visit **virsec.com**.