CASE STUDY

Major Water and Wastewater Treatment Facility Secures SCADA Systems

With Application-Aware Workload Protection

VIRSEC

"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 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.

The Challenge

The utility uses AVEVA System Platform control and monitoring solutions to supervise the operation of Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and manages the information generated throughout the water treatment processes. The OT leaders wanted assurance that automated security was in place to counter attacks on vulnerable aspects of the system, whether known or unknown. The goal was to ensure an automatic and proactive response to attacks as they happen.

Always One Step Behind

Critical infrastructure sites are significant targets for malicious attacks, and this facility was no different. Threat actors are bypassing traditional perimeter and cybersecurity tools and executing at the memory layer during runtime, always leaving the security teams one step behind. The customer needed to be able to mount a rapid, accurate response to events that threatened their daily operations and maintain the health and safety of its customers and communities.

Operations Under Pressure

The customer wanted to be proactive with its cybersecurity efforts, but it also faced limited security expertise, resources, and personnel to assist with monitoring and maintaining effective cybersecurity.

Persistent Vulnerabilities

The facility was experiencing persistent vulnerabilities across various applications and integrated components and services in areas where visibility and control were often lacking.

Lack of Visibility and Control

Security stakeholders worried about critical gaps in their strategy that could open doors to exposing sensitive information. They lacked visibility and control at runtime and knew they needed to leverage technology to provide in-depth protection across host and memory layers.

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.

VIRSEC

Monitors file systems for unplanned file changes and malware installations

•

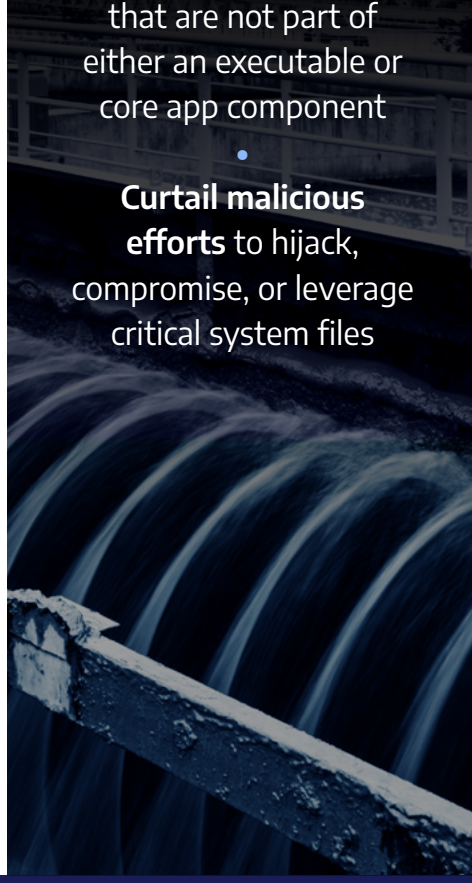
Ensures only legitimate libraries load whenever an application process is spawned

•

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.

"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

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 Easyto 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.

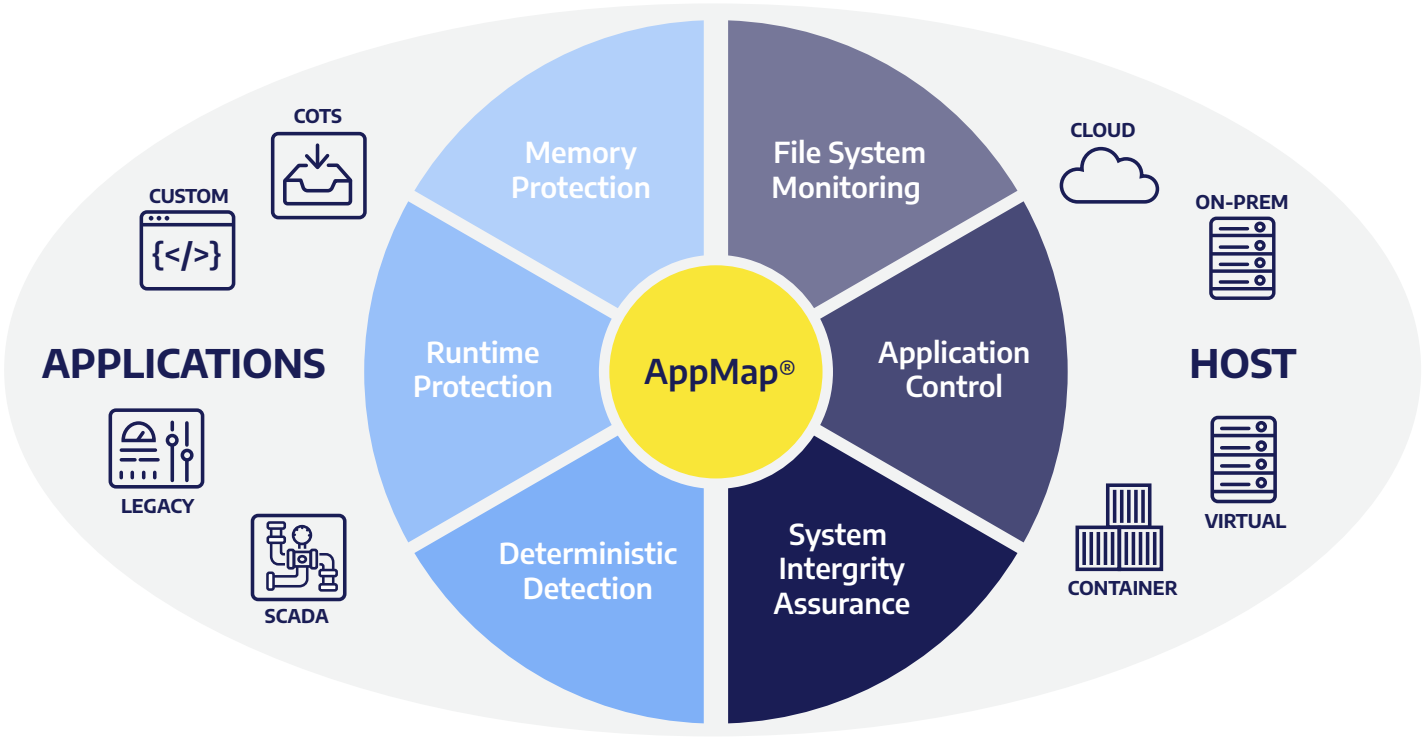
Cybersecurity Redefined

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.

Application-Aware Server Workload Protection

Virsec provides application-aware server workload protection against the widest range of cyberattacks—known and unknown—and secures applications from the inside. Virsec protects all your applications, including custom, COTS, third-party, legacy, SCADA and more. And the Virsec solution protects across any platform, including on-prem servers, virtual, cloud, hybrid, container, and edge.

ANYWHERE	ANYTHING	ANYTIME
On-prem, public/private cloud, hybrid, container	*Custom, legacy, COTS and air gapped applications*	*Deploys in minutes, protects continuously in real-time*



VIRSEC

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, SCADA systems, and more.

Recognition

Cyber Catalyst

CRN

Cyber Defense Global Awards 2019 Winner

Gartner

Cyber Security Excellence Awards Winner 2020

MITRE

Info Security Products Guide 2020 Global Excellence Gold

Ovum

Partners & Customers

Tech Mahindra

NCUA

Raytheon Technologies

Godrej

Schneider Electric

YOTTA

du

AVEVA

BROADCOM

inspirage

etisalat

GDIT

Server & Application Workload Protection

Application-Aware Mapping Technology

No Signatures, No Tuning, No Noise

Zero Dwell Time

Full-Stack Runtime Protection

 • 226 Airport Parkway, San Jose, CA 95110 • VIRSEC.COM

VIRSEC