virsec®

CASE STUDY

Major Water Utility Enlists Virsec to Secure SCADA Systems

Needed to Ensure Operational Integrity for Water & Wastewater Facility

With many critical infrastructure facilities having experienced cyberattacks that led to disruption of operations, along with an EPA warning to the Industrial Sector, a county department of water resources sought tools to prevent assailants from compromising AVEVA Wonderware SCADA software used to provide clean and safe water to customers.

Customer Profile

- **Top 5 US water utilities**
- **Serves more than 1M people**
- **Multiple water treatment plants & pumping stations**
- **Processes almost 100M gallons of water daily**

As one of the largest water utilities in the US, the customer uses AVEVA Wonderware control & monitoring solution to supervise the operation of remote telemetry units (RTUs) and programmable logic controllers (PLCs), and manages the information generated throughout water management processes. The customer wanted assurance that automated security was in place to counter attacks on vulnerable aspects of the system, whether known or unknown. Their goal was to ensure responsiveness to attacks at the earliest point – as they happen.

Virsec Security Platform Secures Digital Transformation

This water resources department recognized nationally for water infrastructure development, rolled-out a full-stack application security strategy using Virsec Security Platform™ (VSP) to prevent disruption of water service operations and control due to mounting risk of cyberattacks on critical infrastructure.

"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

As the customer implemented AVEVA's control & monitoring solutions they sought to improve their overall ICS security. The 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.

After careful evaluation, the customer selected VSP for application control and memory control flow integrity (CFI), securing all aspects of their SCADA application and underlying workload components running in disparate environments. VSP allows them to stop devastating attacks before damage is done, based on intrinsic knowledge of acceptable process behavior, visibility into process flow, and ongoing monitoring file systems and memory.

Key Challenges

The county water utility had multiple security challenges before working with Virsec including:

- Limited IT resources and security specialists to assist with monitoring and maintaining cybersecurity
- Persistent vulnerabilities across various applications, and integrated components and services in areas where visibility and control were often lacking
- Advanced attacks on critical infrastructure attacks required a depth of security expertise not common in utility IT teams
- Rapid response to events that threaten operations was crucial for the health and safety of communities

Definitive Results with Virsec

- **Hardened AVEVA Wonderware software** including Historian, SCADA and HMI cyber exploits and ransomware
- **Delivered 100% attack coverage** for known & unknown threats that bypass IDPS, EDR and EPP
- **Reduced attack exposure to milliseconds** especially for memory-based attacks, fileless exploits, & filesystem changes
- **Unburdened Security Resources** no automation, tuning or false positive analysis
- **Does not rely on signature updates** unlike the conventional EPP, EDR solutions, making it ideally suited for air-gapped facilities

VSP Protects ICS Environments from the Inside

- Monitoring file systems for unplanned file changes and malware installations
- Ensuring only legitimate libraries load whenever an application process is spawned
- Distinguishing authorized processes and detecting library injections or code not part of either an executable or core app component
- Curtailing malicious efforts to hijack, compromise, or leverage critical system files.
- Providing runtime visibility of process memory to prevent memory-based threats, fileless malware, and unknown or zero-day attacks

"Virsec reduces the possible dwell time for attackers to zero. Because of the precision and real-time remediation of the solution, we now have the confidence to enforce security without disrupting operations."

Director of Plant Security Operations