Device-Level Cybersecurity for the Water Sector

Device-level protection and zero-trust principles

BY JAY SMILYK

Images: 151802324; 699455; 134071780; 179907303; 122475953; 61507196; 965001 | dreamstime.com, 166313656; 120610880 | Getty Images

Cyberattacks on U.S. water infrastructure are rising. The National Cyber Strategy includes new regulations directing an increased focus on cybersecurity to ensure the safety of public drinking water.

Threat actors and nation-states have already attacked U.S. water systems, like the failed Iranian cyberattack on a New York dam in 2013, and the January 2021 cyberattack, when a water treatment plant in the San Francisco Bay Area suffered an attack where an undisclosed hacker deleted crucial programs used to treat drinking water.

The most significant cybersecurity risk for water facilities often comes from insider threats: human error, stolen credentials, and malicious actors. While incidents stemming from the first two categories are more common, all insider attacks are on the rise, as indicated by the Ponemon Institute's research, which found that every surveyed company had experienced an insider incident last year.

The 2021 incident in Oldsmar, Florida, demonstrated the impact of human error when an employee accidentally clicked the wrong button. The recent attack on the Discovery Bay Water Treatment facility in Tracy, California, by a contractor, shows how dangerous a malicious insider can be when using their access to set out to cause intentional harm.

Securing more than 55,000 decentralized public water systems and 16,000 wastewater systems in the United States poses a considerable challenge, especially in an industry with limited cyber awareness and resources. It only takes one unsecured device or a single human error or worker manipulation by an outsider to jeopardize the water safety of hundreds of thousands if not millions of residents.

The key to combating insider attacks is managing and monitoring insider privileges, not the individuals, which can effectively eliminate the attack vector.

UPCOMING REGULATIONS DON'T ADDRESS CORE ISSUES

While securing Programmable Logic Controllers (PLCs) eases many of the cybersecurity burdens on water facilities, centralized regulations governing these protections do not yet exist.

The National Institute of Standards and Technology (NIST), American Water Works Association, Department of Homeland Security, and Cybersecurity and Infrastructure Security Agency (CISA) all provide some degree of risk management oversight and best practice recommendations, but no enforceable national standards or regulations exist. Without greater involvement from private-sector cybersecurity companies and industry groups, the feasibility and scalability of any such standards remain questionable.

In March, the U.S. EPA issued a memorandum that stated that cybersecurity needed to be included in water system audits. That was later struck down by the U.S. Supreme Court. However, cybersecurity of critical infrastructure is still a major concern of both the EPA and Biden administration.

NIST has recently emphasized the need for the "protection of individual OT components (devices) from exploitation."

On a global scale, both the Cyber Security Agency of Singapore and the European Union have issued regulations and recommended best practices to address the importance of adopting zero-trust principles and configuring devices to protect OT assets at the device level.

WHY DEVICE-LEVEL PROTECTION IS CRITICAL

There is an urgent need to implement zero-trust cyber protection at the device level for critical infrastructure and industrial operations, especially within operational technology (OT) and industrial control systems (ICS) in industrial devices.

The reasons why regulators and standards bodies consistently point to device-level protections as foundational to ICS security are multifaceted.

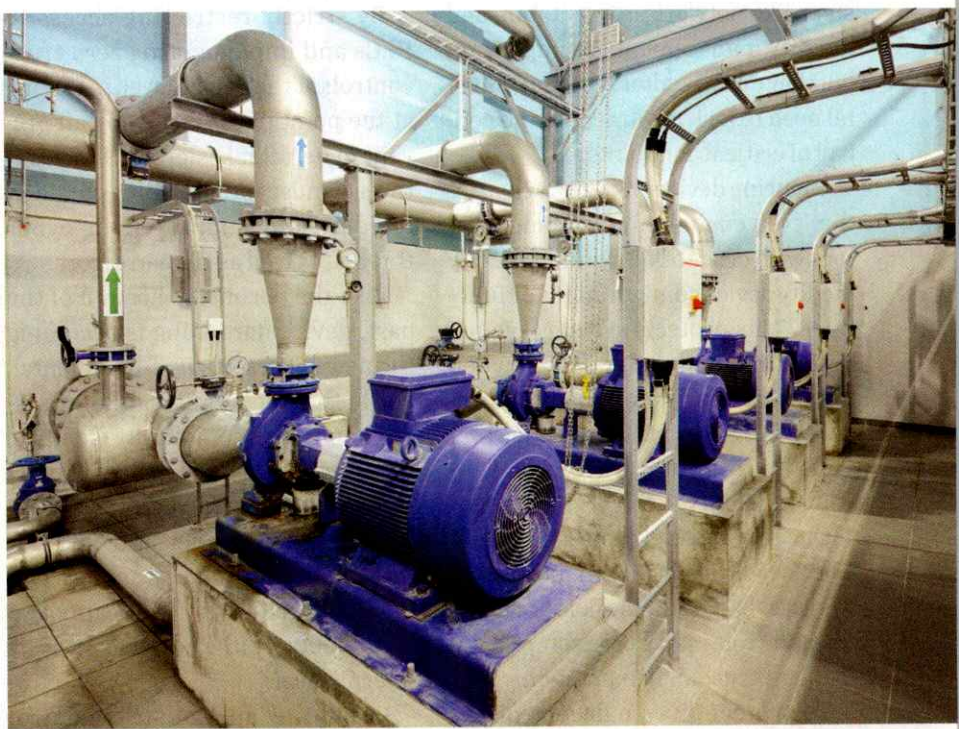
It becomes the frontline defense against both outsider and insider threats. While perimeter defenses like firewalls help keep out external attackers, only device-level controls can protect against a malicious, manipulated, or even careless insider.

It removes reliance on expert in-house staff to monitor and secure systems. Maintaining highly skilled and constantly vigilant security staff is unrealistic for small water facilities. Device-level protections enforce security at the source.

It does not become outdated as new cyberattacks emerge. Controls based on devices, roles and privileges remain effective even as threats evolve. Knowledge-based protections require constant updating.

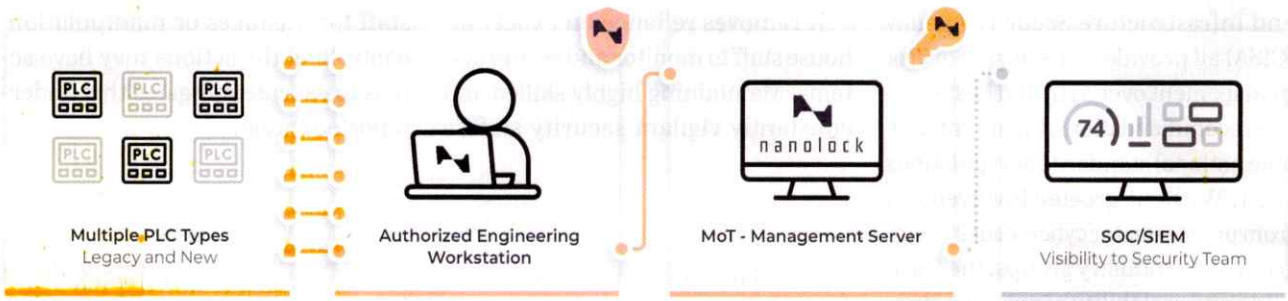
It prevents unintentional insider actions. Impractical as it is to monitor staff for mistakes or manipulation, controlling the actions they have access to execute mitigates this underreported threat.

"THE MOST SIGNIFICANT CYBERSECURITY RISK FOR WATER FACILITIES OFTEN COMES FROM INSIDER THREATS: HUMAN ERROR, STOLEN CREDENTIALS, AND MALICIOUS ACTORS."



For water facilities of all sizes, the journey toward a zero-trust architecture needs to start at the device level.
Images courtesy NanoLock Security.

Strong cybersecurity practices can prevent cyberattacks across the entire threat landscape — from outsider attacks to human errors.



The programmable logic controller can be the smallest common asset for water utilities with the largest operational impact.

STARTING THE JOURNEY TOWARD DEVICE-LEVEL ZERO TRUST

For water facilities of all sizes, the journey toward a zero-trust architecture needs to start at the device level. Initial steps like network segmentation and identity management are important, but they do not address the fundamental need to lock down access and control of critical endpoints.

Securing devices like PLCs ensures that even engineers and administrators with credentials cannot directly modify device configurations or functions. This protects systems against both outside intruders and trusted users who may intentionally or accidentally tamper with processes that could impact water safety and availability.

Once device-level protections are in place, water facilities can move on to privileges based on individual user identities and roles as part of a comprehensive zero-trust implementation.

To protect diverse decentralized infrastructure, our focus must be on the smallest common asset with the largest operational impact — the PLC. These simple industrial computers are crucial to defeating insider threats, as the issue does not lie with the insiders themselves but rather with insider privileges.

By strictly restricting access to PLCs and implementing zero-trust controls at the device level, including at the point of contact, you can prevent cyberattacks across the entire threat landscape, including outsider, insider, and supply chain cyber threats, as well as human errors.

Like the perimeter firewall of the past, device hardening is becoming the new cybersecurity fundamental. For both large municipal water systems and small community facilities, securing devices is a crucial first step in protecting infrastructure from today's blended insider and outsider threats. It grants operators peace of mind that critical systems cannot be manipulated, either externally or by internal users.

Protecting all industrial control systems, whether they are new or legacy systems, with a prevention-based, device-level, zero-trust approach is crucial for ensuring the continuity and integrity of production lines and operations, even in the event of a cyberattack, including insider threats.

By recognizing that the greatest threat is not the people within, but the privileges they hold, and controlling that privilege at the device level, water authorities can move one step closer to adopting a device-level zero trust mechanism. Avoiding regulatory missteps and proactively adopting device-level protections are key to providing the cyber resilience and safety assurances the public expects. **WW**

Jay Smilyk, VP of the Americas at NanoLock Security, has more than two decades of experience in leadership and technology. Jay has held executive positions and sales management roles and has served as CRO of Tripleblind and Sepio Systems. Before that, he was the Eastern Regional Director of Sales for Vectra Networks. Jay also previously served as VP of Sales at Safend, where he built a team of security professionals to bring endpoint data protection solutions to the U.S. market.