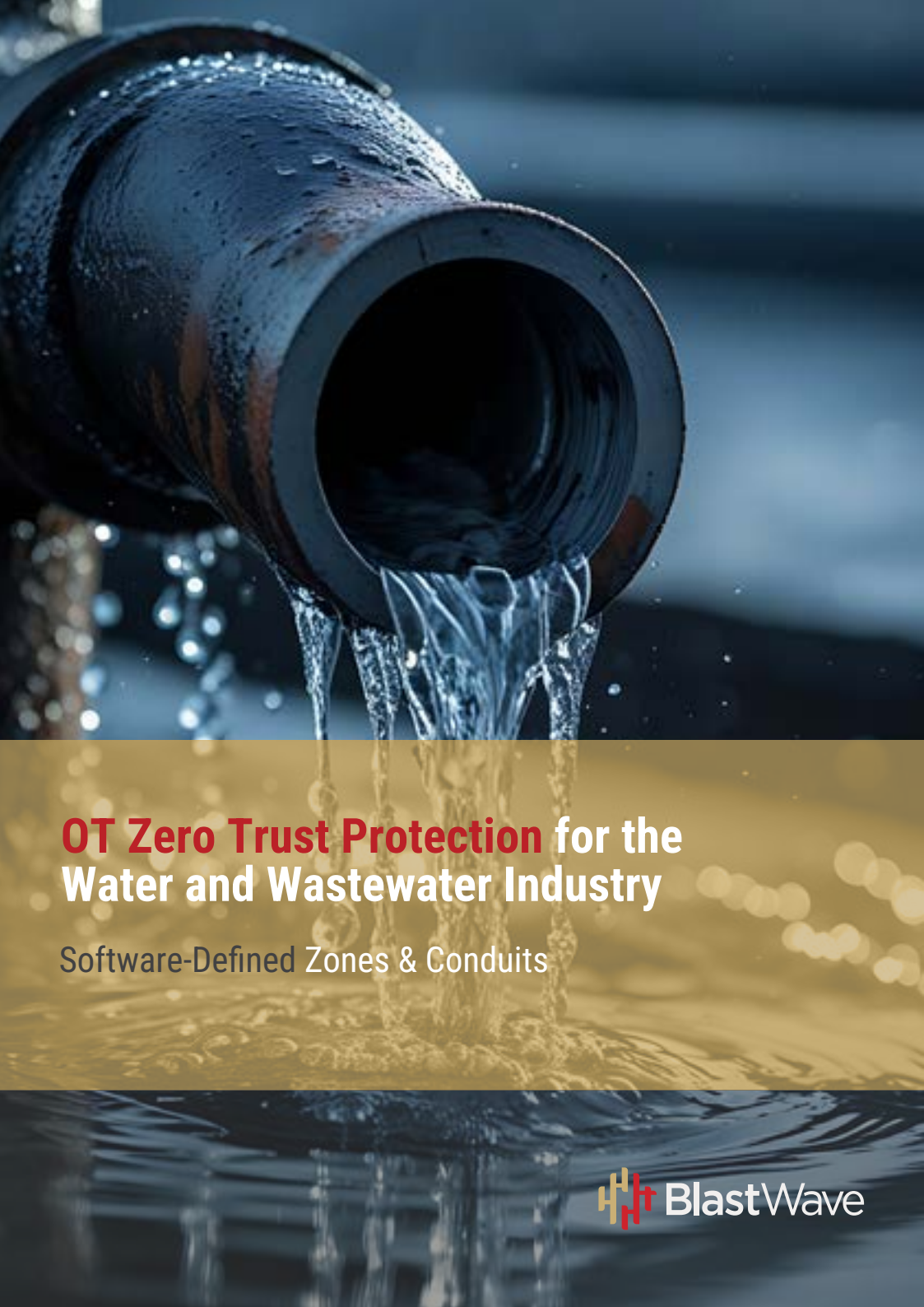


OT Zero Trust Protection for the Water and Wastewater Industry

Software-Defined Zones & Conduits

BlastWave

The water and wastewater industry has increasingly been the target of cybercriminals, bad actors, and hostile nation-states, and recent incidents highlight the importance of cybersecurity in this sector.

The US alone has about 150,000 public water systems and 16,000 publicly owned wastewater systems. This industry has been specifically targeted by bad actors recently, and in recognition of this ongoing threat, CISA announced a free Cyber Vulnerability Scanning Service for Water Utilities.

Recent hacks include the Municipal Water Authority of Aliquippa, Hawaii Water Utility, and the North Texas Municipal Water District. In January of 2021, San Francisco Bay Area experienced a cyber attack when a group of hackers used a former employee's username and password, which had not been removed from the system, to access to a water treatment facility.

Using outdated software and widely shared login credentials, hackers also accessed controls for a water treatment facility in Oldsmar, Florida, in February 2021. The hackers attempted to increase the levels of sodium hydroxide to toxic levels and contaminate the water supply of the town's 15,000 residents. Luckily, an alert user noticed the mouse movement and informed the authorities. This incident brings attention to the vulnerabilities posed by remote access systems, which are becoming increasingly prevalent in critical infrastructure IT systems and represent significant cybersecurity risks.

As Generative AI (GenAI) is used to enhance phishing and reconnaissance of public utilities, these threats will grow, and the consequences could be fatal for communities.

CONTENTS

Security Challenges in the Water and Wastewater Industry

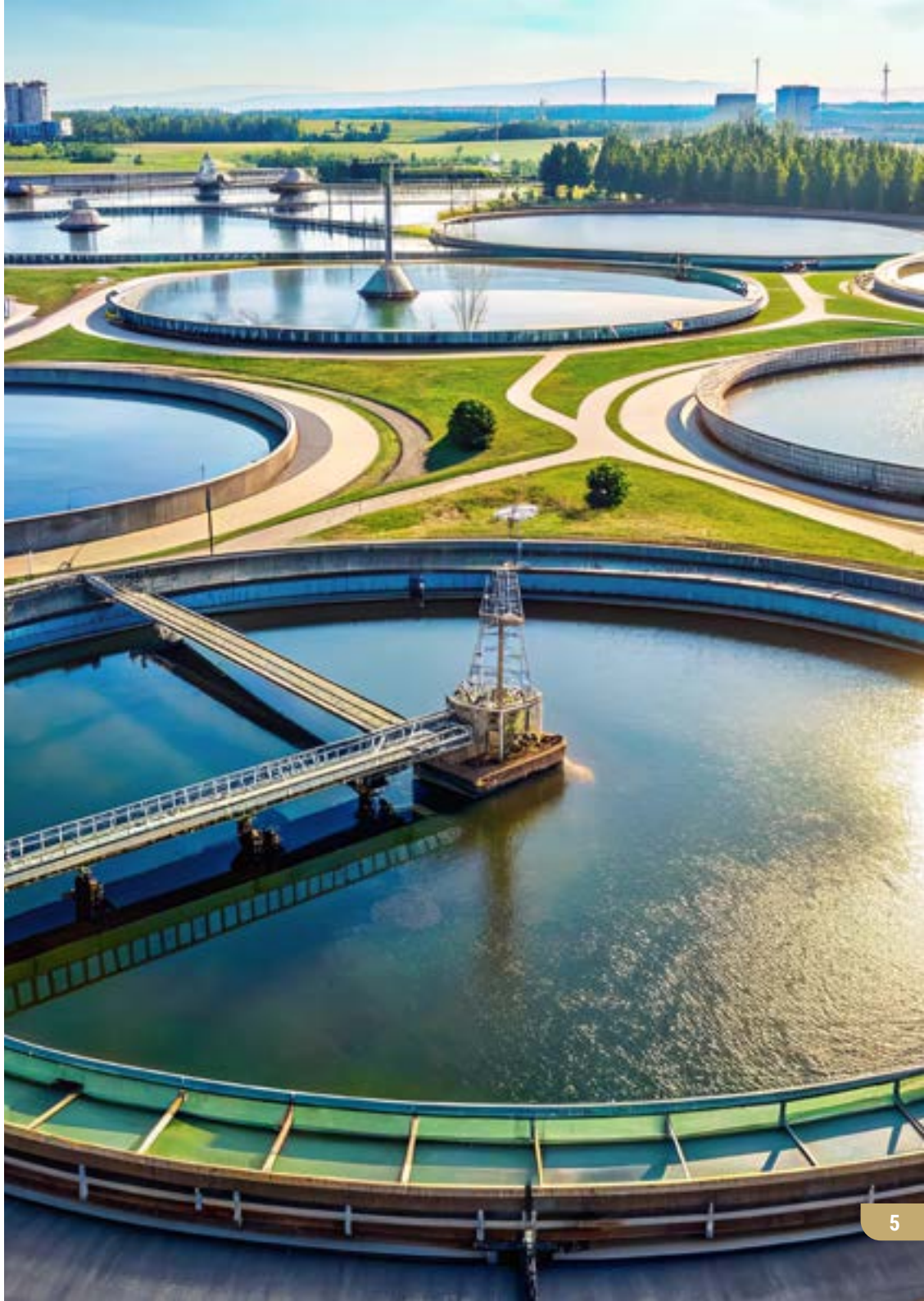
The water industry faces unique security challenges in the realm of cybersecurity. Although all utility sectors encounter these challenges, the water industry is particularly vulnerable and is being specifically targeted by bad actors. Unlike the electric, oil, and gas industries, no standardized set of rules or regulations for securing water utilities existsthere's no standardized set of rules or regulations for securing water utilities. As a result, there are numerous potential security gaps due to the disparate nature of system implementation.

Additionally, cybersecurity practices are outdated in many parts of the country, and weaker identity monitoring and access management tools increase vulnerability. The facilities are usually lightly staffed, and the existing IT security solutions are a poor match for the cybersecurity needs of an OT network.

Potential Consequences of Cyber Attacks on the Water and Wastewater Industry

Successful cyber-attacks on the water and wastewater industry can have far-reaching consequences.

These attacks can disrupt treatment and conveyance processes by manipulating equipment, disabling pumps, or overriding alarms. Attackers can also deface the utility's website or compromise the email system, putting customer data and billing information at risk of theft. In some cases, malicious programs such as ransomware can be installed, causing severe damage to business operations.



OT Cybersecurity Water Protection Use Cases

Securing Critical SCADA Systems

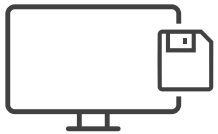
- Protect SCADA systems by making them invisible to external threats and unauthorized users through network cloaking.
- Access is then restricted through phishing-resistant, passwordless MFA.
- Secure remote access with secure, encrypted tunnels directly to the SCADA system, with access limited to the specific user and their assigned task.

Protecting Geographically Dispersed Assets: Remote Pump Stations and Reservoirs

- Create a secure boundary that protects these assets regardless of their physical location.
- Enable secure remote monitoring and control, allowing maintenance and engineering crews to diagnose and repair equipment without exposing these remote systems to cyber threats.
- Establish a full mesh of peer-to-peer encrypted tunnels to secure sensitive but unclassified data traffic from remote users to OT networks and any agent-enabled systems, protecting data-in-flight from manipulation.

Enabling Secure Remote Access: For Maintenance Crews and Third-Party Vendors

- A passwordless and phishing-resistant remote access solution eliminates a primary initial attack vector used by hackers.
- Enforces a least privilege access model, ensuring that third-party vendors or maintenance personnel are only granted access to the specific systems they need for a limited duration, without allowing them to view or access any other network assets.



Mitigating Legacy System Risks: The "Virtual Air Gap" for Unpatchable Equipment

- Provides a "virtual air gap" for unpatchable legacy devices.
- Network cloaking shields legacy equipment by making it undiscoverable and invisible to unauthorized users, a proactive defense that prevents an attacker from ever discovering the vulnerable device, let alone exploiting its weaknesses.

.

Safeguarding Specialized Processes: Securing Chemical Injection, Filtration, and Purification Systems

- Prevents unauthorized access and manipulation of these specialized systems.
- Protects the telemetry units (RTUs) used for data collection and transmission, ensuring that data-in-flight is encrypted to prevent manipulation of sensor data and control signals with cloaking and encrypted tunnels.
- Granular microsegmentation ensures that only the personnel directly responsible for these processes have visibility and access, confining them to a secure zone and mitigating the risk of a breach affecting other parts of the network.

Ensuring Operational Continuity: Preventing Disruptions to Water Distribution Networks

- Blastwave's Zero Trust architecture ensures that network access to these distribution control systems is strictly verified and controlled.
- Creates a layered defense, combining network cloaking, passwordless authentication, and microsegmentation, providing robust protection against both external cyberattacks and internal, unauthorized manipulation, guaranteeing the continuous operation of the water system.

For more information on BlastWave's Water and Wastewater Industry Use Cases, please visit: www.blastwave.com/water

BlastWave's Water and Waterwaste Industry Solutions

The water and wastewater industry provides essential services to the public and relies on technology like SCADA systems, making them a prime target forvulnerable to cyber attacks threats. Cybersecurity breaches in these OT systems can lead to disruptions in service, financial losses, and reputational damage.

BlastWave offers three key technologies to protect the Water and Wastewater industry:

Network Cloaking:

Network Cloaking ensures that critical yet outdated legacy infrastructure such as PLCs, sensors, and pumps—becomes invisible to external threats. Rather than just obfuscating these systems, they do not appear in any scans or probes from a hacker. With BlastShield, water systems operators ensure security and compliance with industry standards and guidance like NIST 800-53, 800-207 (Zero Trust), and IEC 62443. AI-enhanced reconnaissance tools cannot probe into the internal workings of a water facility because they have no path to reach the internal OT networks.

.

OT Secure Remote Access:

BlastShield provides OT Secure Remote Access to critical OT water systems, ensuring operators can monitor and manage them without exposing them to cyber threats. BlastShield's phishing-resistant MFA biometric authentication protects against GenAI-powered phishing attacks and MFA hijacking. A full mesh of P2P encrypted tunnels is created to secure traffic from remote users to the water facility and any agent-enabled systems, protecting against Man-in-the-middle attacks.

Network Segmentation (MicroSegmentation):

BlastShield simplifies the challenge of microsegmentation by creating simple peer-to-peer encrypted and authenticated tunnels to each device or group of devices without complex firewall rulesets. IT and OT network staff and temporary contractors are permitted access to only the systems they are responsible for, and privileges can be granted and revoked in real-time. BlastShield prevents lateral movement by Secure Remote Access users within the network and can even provide lateral movement protection at Layer 2 for local network connections.

BlastWave

BlastWave's Approach:

BlastWave implements a true Zero Trust architecture, assuming no user or device is inherently trustworthy. We verify every connection, enforce least privilege access, and continuously monitor network activity to detect and respond to threats in real-time. Our solution is designed to be easy to deploy and manage, minimizing disruption to existing operations.

By implementing BlastWave, manufacturers can strengthen their OT security posture, protect their critical assets, and ensure their facilities' continuous and secure operation in the face of evolving cyber threats.

BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to www.blastwave.com

v20250320

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use.
Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499