



WHITEPAPER

When remote access reaches the physical world

What attacks on U.S. water systems
reveal about securing privileged access
across critical infrastructure





Executive summary

Water utilities increasingly depend on remote connections to operate and maintain physical infrastructure. Recent attacks have shown what can happen when those pathways are exposed or poorly controlled.

Removing operational technology (OT) from the public internet is an essential first step. It does not remove the need for engineers, administrators, equipment manufacturers, systems integrators, and other specialists to reach critical systems. In many water utilities, particularly smaller ones, some of the expertise required to keep equipment running does not exist on-site.

That creates another security problem after unnecessary internet exposure has been addressed: governing the legitimate privileged access that remains.

This paper looks at that problem through recent attacks and cybersecurity findings across the U.S. water sector. It examines the role of employee and third-party identities, the challenges utilities face in keeping track of vendor access, and what happens on the other side of the connection when a technology provider needs to support hundreds of customer environments.

The evidence points toward a broader approach to privileged access. An approach that accounts for who is connecting, what they can reach, the credentials they use, and what happens during the session. Privileged access management and vendor privileged access management address different user populations within that strategy. Vendors providing remote support into customer environments face a related challenge of their own.

Water is a useful place to examine the issue because the connection between digital access and physical operations is unusually clear. The same access patterns already exist across energy, manufacturing, healthcare, transportation, and other critical environments.

Water systems are already feeling the pressure

The U.S. water sector includes close to 170,000 drinking-water and wastewater systems, ranging from large metropolitan utilities to small community operations. The U.S. Government Accountability Office (GAO) has identified persistent cybersecurity challenges across the sector, including aging technology, workforce shortages, limited financial resources, and greater connectivity between OT and internet-enabled systems.

Remote connectivity has practical value in an environment like this. Water infrastructure can be spread across large geographic areas, and utilities may need outside specialists to help administer or repair equipment. The same connectivity can give attackers more opportunities to reach systems controlling pumps, valves, and other physical devices.

Recent incidents have made that risk difficult to ignore.

On July 26 and 27, 2026, a coordinated cyberattack targeted operational technology at more than 30 Minnesota community water systems. Minnesota IT Services activated statewide incident-response capabilities and worked with federal, state, and local partners to investigate the attack and support affected utilities.

It was not the first campaign to put water OT in the crosshairs. Between November 2023 and January 2024, actors affiliated with Iran's Islamic Revolutionary Guard Corps compromised at least 75 U.S.-based Unitronics devices, including at least 34 in water and wastewater facilities. According to the Cybersecurity and Infrastructure Security Agency (CISA), the devices were internet-connected and had either a default password or no password. Attackers changed device configurations and interfered with operators' ability to connect remotely.

Incident counts tell only part of the story. In 2025, the U.S. Environmental Protection Agency (EPA) identified cybersecurity vulnerabilities at 277 water systems and says it worked directly with those systems to eliminate 350 vulnerabilities. Some affected technology was used to control drinking-water and wastewater processes.

A separate assessment by EPA's Office of Inspector General (OIG) provides a sense of scale. The OIG passively assessed 1,062 drinking-water systems serving more than 193 million people. Ninety-seven systems serving approximately 26.6 million people had critical or high-risk cybersecurity vulnerabilities. Another 211 systems, serving more than 82.7 million people, had externally visible open portals associated with medium- or low-risk findings.



Water cybersecurity risk at a glance

30+

MINNESOTA COMMUNITY WATER
SYSTEMS TARGETED IN JULY 2026

277

WATER SYSTEMS WHERE EPA
IDENTIFIED CYBERSECURITY
VULNERABILITIES DURING 2025

26.6 million

PEOPLE SERVED BY SYSTEMS
WITH CRITICAL OR HIGH-RISK
FINDINGS IN THE EPA OIG
ASSESSMENT

Sources: Minnesota IT Services, U.S. EPA, EPA Office of Inspector General.

The numbers should not be read as evidence that all water utilities face the same level of risk. They show something more practical: cybersecurity maturity remains uneven across a sector made up of organizations with very different infrastructure, staffing levels, and budgets.

Remote access remains part of the job

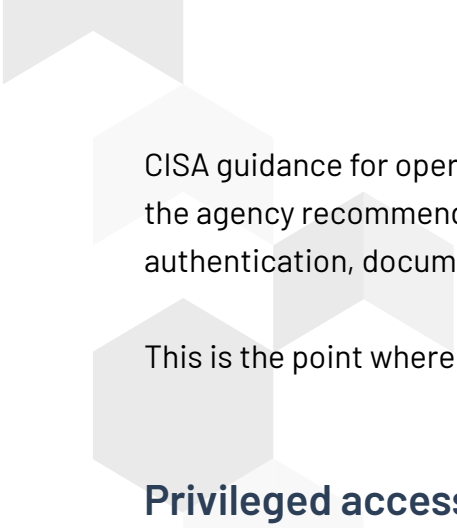
Federal guidance has been clear about some of the basic steps water systems can take. CISA, EPA, and the Federal Bureau of Investigation recommend reducing exposure to the public-facing internet, changing default passwords, inventorying OT and IT assets, assessing cybersecurity regularly, maintaining backups, and addressing known vulnerabilities.

Those actions can remove a large amount of avoidable exposure. They do not solve the day-to-day problem of how an engineer, administrator, or outside specialist reaches equipment when something actually needs attention.

Consider a pump controller that begins behaving unexpectedly at a small water facility. The utility may know exactly what is wrong but lack an employee with deep expertise in that particular controller. The person best equipped to diagnose it could work for the manufacturer or an integrator several states away.

Remote support may be the fastest way to restore normal operations. Once that connection is allowed, however, the utility has another set of decisions to make.

It needs to know who the technician is, whether that person is still authorized by the vendor, and which controller or service they actually need to reach. The technician may not need to know the privileged password at all. And when the repair is finished, access that made sense during an outage may make considerably less sense six months later.



CISA guidance for operational technology reflects this reality. Where remote access is essential, the agency recommends moving OT assets off the public internet, applying multifactor authentication, documenting remote access, and using least-privilege principles.

This is the point where network security and access security meet.

Privileged access belongs in the OT security conversation

A privileged account allows someone to make changes that an ordinary user cannot. In an operational environment, the consequences of those changes may extend to the behavior of equipment.

That makes the identity behind the account important, but identity is only part of the picture. A utility also needs to understand what the person can access, which privileged credentials are involved, how long those permissions should last, and whether activity can be reviewed later.

The risk is not limited to outside vendors.

A 2025 study conducted by Ponemon Institute on behalf of Imprivata surveyed 1,942 IT and IT security practitioners in the U.S., U.K., Germany, and Australia. Respondents included professionals in public-sector and industrial and manufacturing organizations. Forty-seven percent said their organization had experienced a breach or cyberattack involving third-party network access during the previous 12 months. Among that group, 34% said excessive privileged access granted to a third party contributed to the incident.

The same study found that 44% had experienced a breach or attack involving an internal user with privileged access. Of those respondents, 45% said excessive employee privilege played a role.

Verizon's 2026 Data Breach Investigations Report adds independent evidence that third parties are becoming more prominent in breach investigations. Verizon found third-party involvement in 48% of breaches in its dataset, up 60% from the prior year.





Internal and third-party privileged access

THIRD-PARTY USERS

47% experienced a breach or attack involving third-party network access

34% of that group cited excessive third-party privilege

INTERNAL PRIVILEGED USERS

44% experienced a breach or attack involving an internal privileged user

45% of that group cited excessive employee privilege

Source: Ponemon Institute research conducted on behalf of Imprivata.

The distinction between the two populations matters operationally.

A utility usually knows when an employee joins, changes jobs, or leaves. It controls the employee's manager, role, and account lifecycle. Privileged access management can apply controls to the privileged identities, accounts, and credentials those users rely on.

Vendor identities are harder to manage because part of their lifecycle sits outside the utility. An equipment manufacturer may change which technician supports the account without the utility knowing. A contractor can leave the vendor while an access method established months earlier remains active. Vendor privileged access management is designed around the additional identity, approval, and lifecycle issues that come with those external users.

Both sit within the broader discipline of controlling privileged access to critical systems.

Third-party visibility is still uneven

The Ponemon findings suggest that many organizations have only a partial picture of their external access.

Respondents estimated that an average of 20 vendors had access to their organization's network. Yet only 50% said they maintained a comprehensive inventory of all third parties with network access, and 59% said third-party access was not monitored.

It is easy to see how the gap develops in an operational environment. A pump vendor needs one form of access. An instrumentation provider needs another. The SCADA integrator has its own connection, as does an IT service provider supporting infrastructure elsewhere in the environment.

None of those decisions has to be reckless. Each may have been perfectly reasonable when the access was established. The problem appears later, when accounts, credentials, VPNs, and vendor-specific tools have accumulated across different parts of the organization and no one has a complete view of them.

EPA inspectors have encountered some very basic versions of this problem. In a 2024 enforcement alert, the agency described water systems that had failed to change default passwords, used a single login for staff, or had not removed access for former employees. EPA also reported that more than 70% of the systems it had inspected since September 2023 were violating basic requirements under Section 1433 of the Safe Drinking Water Act. Those violations were broader than cybersecurity alone, but the 70% does include cybersecurity failures.

Still, shared identities and lingering access are exactly the kinds of weaknesses that make it harder to answer a basic question after an incident: who actually did what?



The third-party visibility gap

Organizations report an average of **20 vendors with network access**

But:

50%

DO NOT HAVE, OR ARE UNSURE WHETHER THEY HAVE, A COMPREHENSIVE INVENTORY OF THIRD PARTIES WITH ACCESS

59%

DO NOT MONITOR THIRD-PARTY ACCESS

Source: Ponemon Institute research conducted on behalf of Imprivata.



Remote access from the vendor side

A company supporting hundreds of utility customers has a different version of the same problem. Remote connections have to be routine enough for support teams to use every day, while customers expect those connections to be controlled and auditable.

National Information Solutions Cooperative (NISC) is a useful example. NISC develops, implements, and supports software and hardware for telephone companies, electric cooperatives, and other public power entities. The company supports more than 750 customer organizations.

Its support teams historically relied on business-to-business VPN tunnels to access customer networks. According to an NISC case study, that model provided limited alerting and reporting and made it difficult to see and monitor remote connections across customer environments.

For NISC, the practical requirement was to preserve the support methods its teams already used while gaining more control over each connection. The company needed to know who was connecting to a customer and what type of support that person was providing.

After deploying Imprivata Customer Privileged Access Management (CPAM), NISC reduced approximately 1,500 endpoints that previously had access to VPN tunnels to only a handful of business servers that still required direct B2B VPN connectivity. It also gained audited access to customer environments rather than the wide-open, unmonitored access it had identified as a security and liability concern.

A utility has to decide how an outside provider reaches its environment. The provider, in turn, has to manage which of its own employees are allowed to enter customer environments and how those connections are made.

That relationship becomes increasingly important as remote support grows across critical infrastructure.

What stronger control looks like

Improving privileged access security starts with an accurate picture of what already exists. For some utilities, that work may uncover a formal remote-access architecture. For others, it may reveal a mixture of VPN accounts, vendor tools, shared credentials, and access methods that have grown over years.

The practical questions are relatively straightforward. Can the organization identify the people who currently have privileged access to critical systems? Are users working through individual identities or shared accounts? Do their permissions still match the work they perform? Can credentials be protected without exposing reusable passwords? When a vendor's work is complete, is there a reliable way to close the access?



Session visibility matters as well. If an administrator changes a configuration or a vendor connects during an outage, the organization should be able to reconstruct that activity without depending on several disconnected sources or asking a vendor who might have used a shared account.

This is consistent with federal guidance for the water sector. CISA, EPA, and the FBI recommend unique strong passwords, asset inventories, reduction of public internet exposure, and regular cybersecurity assessments. CISA's OT guidance also recommends MFA and least privilege for necessary remote access.

A privileged access program can build on those foundations.

Privileged access management helps organizations manage the elevated access used by employees and administrators, including privileged credentials, granular permissions, authentication, and session visibility. Vendor privileged access management applies controls to outside users while accounting for vendor-specific approval and identity-lifecycle requirements. Imprivata Privileged Access brings those privileged access management and vendor privileged access management capabilities into a centralized approach for employee and third-party privileged access.

For technology vendors providing support into customer environments, CPAM addresses the outbound side of that relationship, as the NISC example illustrates.

These controls do not replace network segmentation, vulnerability management, patching, backups, or OT asset inventories. Their purpose is to govern the people who still require authorized access after those safeguards are in place.

The lesson extends beyond water

Water makes cyber-physical risk unusually visible. A digital action can affect a pump, a valve, a treatment process, or an operator's ability to understand what is happening in the system.

The access pattern is already familiar elsewhere. Manufacturers rely on OEMs and outside specialists to maintain production equipment. Energy providers operate distributed infrastructure. Healthcare organizations depend on vendors to support specialized technology. The Unitronics devices compromised in the CyberAv3ngers campaign, for example, are used across multiple critical-infrastructure sectors rather than water alone.



As these environments become more connected, security teams have to look at more than whether a device is exposed. They also need to know who can legitimately reach it today, what that person can change, and whether the organization could explain what happened if something went wrong.

Recent attacks on U.S. water systems make the consequences easier to see. The privileged pathways behind normal maintenance, administration, and remote support deserve the same scrutiny.

[Learn more](#) about how Imprivata Privileged Access helps secure employee and third-party access to critical systems.



Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA

Waltham, MA

Phone: +1 877 663 7446

www.imprivata.com

European headquarters

Uxbridge, England

Phone: +44 (0) 208 744 6500

www.imprivata.com/uk

Germany

Langenfeld

Phone: +49 (0) 2173 99 385 0

www.imprivata.com/de

Australia

Melbourne

Phone: +61 3 8844 5533

Copyright © 2026 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.