DEFENDING AGAINST UTILITY CYBERATTACKS WITH HONEYWELL AND AMI 2.0

Honeywell's AMI 2.0 solutions are backed by a strong legacy of cybersecurity and come standard with advanced features that help harden assets, systems and data from disruptive utility cyberattacks.

The increase in the amount of data available to utilities precipitates an increase in opportunities for enhanced collection, analysis and action taking.

Historical data and real-time insights, especially from advanced metering infrastructure (AMI) 2.0 — a holistic, advanced system comprising smart meters, head-end systems, digital platforms and customer portals — help utilities make the world smarter, safer and stronger.

AMI 2.0 gives utilities the tools they need to enhance demand forecasting, strengthen smart grid reliability, lower operating costs, simplify regulatory compliance and enable accurate customer billing. Not only does it benefit our entire energy ecosystem, but it also helps improve customer services and experiences. That's because, when utilities can see everything happening across their networks from granular to overarching levels, they can make improvements that benefit their businesses and customer satisfaction. It all starts with data, a powerful performance tool.

What happens when company and customer data is stolen? Breached? Compromised? Unfortunately, many utilities are finding out firsthand. But, with a partner like Honeywell that has prioritized utility cybersecurity for decades — increasing functionalities, adding new layers and advancing alongside new intelligence and trends when needed — they don't have to.

Honeywell

UTILITY CYBERATTACKS ARE ON THE RISE

The modern interconnection and digitalization of utility operations, data and networks leave room for cybersecurity vulnerabilities. Cyberattacks threaten the privacy and critical information belonging to electric, water and gas utilities and their customers, and they also affect the operability and functionality of these elemental services.

- Data breaches — at least one — have been experienced by 87% of utilities in the last three years.[1]
- Cyberattacks on utilities increased by more than 200% in 2023.[2]
- On average, electric, gas and water utilities were the target of more than 1,100 cyberattacks a week in 2022.[3]
- Energy sector data breaches cost, on average, an estimated USD 4.78 million in 2023.[3]

Despite the growing popularity and adoption of AMI 2.0, another leading cause of cyberattacks is that many utilities still rely on legacy infrastructure. Outdated meters, older operating systems and decades-old software can weaken a utility's data security since they weren't usually designed with separation and control mechanisms. They're also typically incompatible with today's security solutions, upgrades and patches.

WHAT HAPPENS WHEN UTILITY CYBERATTACKS OCCUR?

Personal customer data and confidential company information are often targeted during a cyberattack. This includes, but is not limited to addresses, billing information, future business plans and employee credentials. Failure to protect these details can lead to identity theft, loss of customers and downtime as data is recovered.

Infrastructure may be getting more secure, but so are hackers and cyberattacks. Often, data is just the start of how utilities can be targeted. In their many forms — ransomware, hacking, phishing, theft, data breaches — cyberattacks produce different outcomes and effects across electric, gas and water utilities.

- **RESOURCE CONTAMINATION:** Cyberattacks can interrupt water treatment, storage equipment and distribution processes. When process controls and other infrastructure that protect water utility operations are compromised, it can lead to the damage of pumps and valves, and the dangerous alteration of chemical levels.[4] Water shortages and scarcity may occur as a result, which can negatively affect public health and the economy.
- **INFRASTRUCTURE DAMAGE**: Cyberattacks can physically damage utility infrastructure of high value. Take gas utilities, for example. Cyberattacks obtain sensitive data and can target control systems, which can cause valves and pipelines to malfunction. When damage occurs, it can disrupt gas supply, resulting in resource loss and even causing dangerous leaks.
- **POWER OUTAGES:** Cyber weaknesses within aging and modern electric utility infrastructure make sensitive data and control of grid systems more accessible to hackers and threats. As widespread power loss is increasingly attributed to cyberattacks, essential services, devices and appliances are affected in parallel.

Where in the World Are Utility Cyberattacks?

Cyberattacks against electric, water and gas utilities are experienced globally:

- In 2016, malware caused 20% of Kyiv's citizens to lose power during a cold Ukrainian winter.[5]
- At the beginning of 2024, water utilities in the United States and the United Kingdom experienced the theft of personal data and corporate information in addition to the malfunction of online billing portals.[6]
- The Amsterdam-Rotterdam-Antwerp refining hub was targeted in early 2022, with oil terminals failing to load and unload cargoes. This was the first event in a series of cyberattacks on European oil terminals.[7]

Data theft, resource contamination, infrastructure damage and power outages stemming from cyberattacks subject utility companies, and customers, to financial strain. Not only are infrastructure repair costs high, but downtime and resource loss prevent homeowners and businesses from operating normally. This can, sometimes irrevocably, cause revenue loss. Data breaches are also grounds for fines by utility regulatory bodies.

UTILITIES CAN HELP PREVENT CYBERATTACKS WITH HONEYWELL ENERGYAXIS AND AMI 2.0

Cyberattacks will try to find a way to target operations, data and resources, regardless of how old or young utility infrastructure may be. But **when infrastructure is specially designed and engineered to protect data, limit tampering and handle routine software and hardware upgrades**, utilities can operate with greater security, mitigating the chances of hacking and the damaging effects that follow.

Honeywell has followed these engineering and design principles for decades, taking a comprehensive approach to utility cybersecurity by providing confidentiality, integrity, availability and auditability within a utility's entire network via EnergyAxis. EnergyAxis is a meticulously constructed AMI system that provides protection against all types of security breaches and includes the following fundamental features:

ACCESS

EnergyAxis controls access to the network at the end devices, the SynergyNet routers and the Connexo NetSense AMI head-end system. We recommend integration with active discovery services that utilities employ.

AUTHENTICATION

EnergyAxis uses sophisticated authentication techniques that feature unique keys for each device. The techniques limit transmissions on the network to authorized devices and personnel only.

ENCRYPTION

Because encryption prevents unauthorized parties from reading private data, EnergyAxis uses National Institute of Standards Technology-approved encryption modes and algorithms, including AES-128.

MONITORING & REPORTING

For early detection of any potential security breach, EnergyAxis enables security audit logging and reporting. Utilities will receive notifications in the event of security concerns and have the ability to integrate third-party intrusion detection and prevention systems.

EnergyAxis uses the AES-128 encryption method to help protect meters, routers, head-end systems and more, with unique, individually managed keys on all components. While this method sufficiently addresses commercial and top-secret government applications, we're developing an AES-256 encryption method with increased resistance to potential brute-force attacks.

At Honeywell Smart Energy, we encourage the adoption of our AMI 2.0 solutions for many reasons. Not only do these solutions improve data collection, data analysis and communication between utilities and customers, but they also take cybersecurity seriously. With EnergyAxis' tamper identification, encryption technologies and advanced monitoring, Honeywell AMI 2.0 solutions help keep utilities online with little fallout and disruption from cyber incidents.

The EnergyAxis system provides stringent security measures throughout a utility's AMI network at all levels because our engineers design and build the security features directly into end devices, radio communications networks, SynergyNet routers and network management systems. This means full data protection exists in the endpoints and SynergyNet routers as well as in transit.

To learn more about EnergyAxis and our solutions for cybersecurity, please click here.

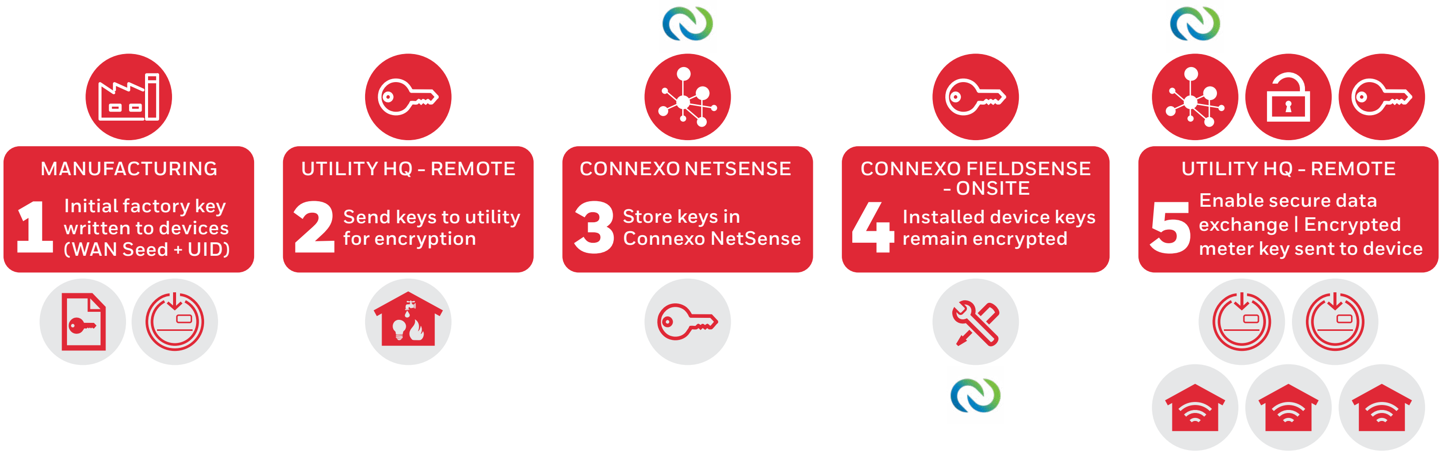
Here's a breakdown of how each robust AMI 2.0 component is hardened against cyberattacks and threats with an end-to-end, security-by-design approach:

SMART METERS

These intelligent devices capture consumption information, time-of-use data and customer insights, then send it to the head-end system, like Connexo® NetSense, for storage and analysis.

- The **Alpha® 4 EA** smart electric meter has expanded data gathering and enhanced processing power to help utilities gain deeper insights into service areas, usage and more. Its security features include magnetic tamper detection, a secure 128-bit encryption using ANSI C12.22 communication and a legally relevant parameters log (LRP) to help keep insights and data protected.
- The **AC-250 NXS** smart gas meter has field-proven, time-tested measurement capabilities, an autonomous shutoff valve for enhanced safety and next-generation hardware and software that helps guard assets from cyber threats.
- The **V200H** volumetric cold-water meter has a proven grooved piston for excellent durability and reduced blockages, and sealed tamper-proof registers to reduce condensation and water ingress. This metering solution has security features that help protect billing and revenue analytics, as well as protection notifications that alert utilities if suspected cyber or manual tampering occurs.

There are five steps to enable a meter/device to work in the field and report to Connexo NetSense, securely.


MANUFACTURING
1 Initial factory key written to devices (WAN Seed + UID)
UTILITY HQ - REMOTE
2 Send keys to utility for encryption
CONNEXO NETSENSE
3 Store keys in Connexo NetSense
CONNEXO FIELDSENSE - ONSITE
4 Installed device keys remain encrypted
UTILITY HQ - REMOTE
5 Enable secure data exchange | Encrypted meter key sent to device

1. **MANUFACTURING** — Each EnergyAxis has a network interface card (NIC). During manufacturing, each NIC is given its own unique encrypted identity consisting of a WAN Seed and a unique identifier.
2. **UTILITY HQ - REMOTE** — A manifest with encrypted initialization keys is sent to utilities.
3. **CONNEXO NETSENSE** — Connexo NetSense is configured and implemented, then keys are stored within the head-end system.
4. **CONNEXO FIELDSENSE - ONSITE** — Replace old meters/devices in the field with new Honeywell smart meters. Once field installation is confirmed, the meter is fully functional with encrypted keys but awaits Connexo NetSense acknowledgement.
5. **UTILITY HQ - REMOTE** — After Connexo NetSense receives meter/device installation information, initialization begins. The head-end system will validate that the NIC is trusted to operate on this system, then move the meter to an active state once all application traffic is encrypted.

It is extremely unlikely that a Honeywell meter will fall victim to cyberattacks and security breaches. But, if an incident occurs, hackers and cybercriminals will only have access to that singular meter. The network, routers and meter data management platform are not accessible.

NETWORKS AND HEAD-END SYSTEMS

Using an AMI 2.0's network, Connexo NetSense speaks to smart meters and preliminarily processes the data before sending it to the router and a meter data management platform. Honeywell head-end system solutions integrate data, workflows and business processes for cost-effective performance. And, the EnergyAxis network is not limited to RF mesh; it can use direct connect/cellular meters because all devices are completely autonomous and communicate meter data back to utilities via the SynergyNet router back to the head-end system.

METER DATA MANAGEMENT PLATFORMS

Honeywell Forge Performance+ for Utilities is the ultimate meter data management platform for AMI 2.0 infrastructure and operations. It is a unified digitalization platform that captures, stores, prepares and analyzes utility and grid data, turning information into actionable insights that are secure, scalable and nonintrusive. Honeywell Forge Performance+ for Utilities enhances utility operations with greater visibility and reliability. It also enhances operations with protection against physical damage and cyber threats using advanced tamper identification, threat detection capabilities and encryption technologies. These security features help limit data breaches and outages, keeping customer and company data private.

CUSTOMER ENGAGEMENT PORTALS

Honeywell's portals and access channels for customers contain billing information, real-time consumption data, utility rates and energy resources. All data is safely stored and encrypted across interfaces where customers access and interact with insights (web servers mobile apps, etc.).

A strong, secure AMI 2.0 system with Honeywell brings data, productivity, efficiency and especially security to utilities when these qualities matter most.

CONCLUSION

Utility cyberattacks are disruptive and dangerous and multiplying. This means it's the perfect time for electric, gas and water utilities to explore and adopt robust solutions that enhance data collection, analysis and action taking without making company and customer data vulnerable to threats.

Supported by a history of continuous cybersecurity innovation, Honeywell adds value, advancement and security to utilities' AMI 2.0 journeys, processes and operations. Get started, today.

RESOURCES

1. Galante, Meredith. "87% of Utilities Have Experienced at Least One Data Breach in Last Three Years." Dimensional Insight®. 5 February 2024. https://www.dimins.com/blog/2024/02/05/87-utilities-experienced-data-breach-last-three-years/.
2. Glassman, Jonathan. "Cyberattacks on Utilities Rise 200% in 2023." Exponent. 29 February 2024. https://www.exponent.com/article/cyberattacks-utilities-rise-200-2023.
3. Pujiastuti, Ratih. "The Downside of Digital Transformation for Utilities: Data Privacy and Cybersecurity Risks." Sustainalytics. 6 June 2024. https://www.sustainalytics.com/esg-research/resource/investors-esg-blog/the-downside-of-digital-transformation-for-utilities--data-privacy-and-cybersecurity-risks.
4. CBS News. "Cyberattacks on water systems are increasing, EPA warns, urging utilities to take immediate action." 20 May 2024. https://www.cbsnews.com/news/cyberattacks-on-water-systems-epa-utilities-take-action/.
5. Cerf, Emily. "Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world." UC Santa Cruz. 17 May 2024. https://news.ucsc.edu/2024/05/ukraine-cybersecurity.html.
6. Wisdiam. "9 recent cyberattacks on the water and wastewater sector." 5 May 2024. https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/.
7. Argus Media. "Cyberattack causing problems at ARA storage terminals." 2 February 2022. https://www.argusmedia.com/en/news-and-insights/latest-market-news/2297896-cyberattack-causing-problems-at-ara-storage-terminals.

For more information

https://automation.honeywell.com/us/en/solutions/smart-energy

Honeywell Smart Energy
2101 CityWest Blvd.
Houston, TX 77042

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell