CUSTOMER STORY

Multi-utility provider defends communities' health and safety

Enhancing security posture with Trellix solutions

Utility provider stewards community necessities and customer data

Customer profile

Utility industry

This utility provider is a leader in the implementation of sustainable water, wastewater, district energy, and natural gas distribution utilities for small to mid-sized communities across North America in 20 states and three provinces.

Solutions and services

Trellix Helix

Trellix Endpoint Security

Trellix Email Security – Cloud Edition

Trellix Network Security

Benefits

- Streamlined security operations and increased visibility across threat vectors for proactive hunting
- Saved money and cut personnel costs with a shared services model
- Fortified security posture with experts functioning as an operational extension of the team

This multi-utility provider harnesses economies of scale to ensure the communities it supports have reliable access to safe, affordable, and sustainable services. The provider is responsible for the public and environmental health of one million customers, a vote of public trust that it considers one of its most valuable assets.

The provider works to ensure its utility infrastructure solutions function harmoniously with the surrounding environment and that its communities have continuous access to basic life necessities such as clean drinking water and proper sanitation. The provider also stewards significant volumes of customer data, including information about individual consumers and the data entrusted to it by municipalities and military installations.

The utility provider's IT and OT environments were previously safeguarded by multiple security products that it sourced through different vendors, but the disparate tools impeded visibility across the provider's infrastructure. Investigating alerts became an arduous task of tracing these alerts across disparate system logs. When a cyberattack swept the globe in late 2016, the provider's IT team had to work through the weekend to coordinate security patches from each vendor to defend against the vulnerability.

The CIO recounted, "It became very apparent how incredibly difficult it would be for our small team to respond to a major incident at our company. We have a profound commitment to the people and the communities we serve. Preventing an attacker from exploiting plant operations to instigate an environment-harming spill or contaminate drinking water is paramount."

Cost savings plus a managed service bonus

To improve the security team's ability to quickly identify and remediate high-risk threats, the provider set out to reinvigorate its security posture. Its goal was to improve visibility across the company's environment, augment the team's daily working capacity, and reduce complexity in the security technology stack.

The CIO explained, "We wanted a strategic partnership with a single vendor that offered an end-to-end solution and a managed detection and response (MDR) service. Our team needed a more efficient way to manage alerts and analyze threats and their potential movement through the environment quickly and efficiently."

> Deploying Trellix was more cost-effective than paying for the eight separate, independent security products we had deployed at the time."
>
> — Chief Information Officer, Multi-Utility Provider

The provider's search for a strategic cybersecurity partner landed on Trellix. The provider replaced all the functionality provided by the eight different security vendors in its environment with a cohesive suite of Trellix solutions.

Trellix Endpoint Security, Trellix Network Security, and Trellix Email Security – Cloud Edition proactively exchange intelligence to fortify defenses along all threat vectors from the core to perimeter. Trellix Helix centralizes the collection of security data and management of the infrastructure, facilitating informed and efficient detection and analysis of threats. The provider also feeds firewall logs from its plants' SCADA systems through Helix to provide real-time visibility into its OT infrastructure. By unifying visibility and control, the provider created a path to Trellix extended detection and response (XDR) solutions for living security embedded in its environment.

The CIO highlighted, "Deploying Trellix was more cost-effective than paying for the eight separate, independent security products we had deployed at the time. Plus, we added a managed service component on top of the technologies, further enriching the new capabilities and visibility established across the environment and providing for full 24x7 visibility. This was important as our operations span five time zones."

An operational partnership and extension of the team

To improve the quality-of-service delivery to constituents, the provider has embarked on a company-wide transformation project to consolidate IT operations under a shared services model. The initiative will align core business processes across corporate offices and includes plans for an enterprise security program.

The CIO enthused, "The team meets regularly with our security group to discuss the most recent events in our environment, cybersecurity trends in the utility industry, and ideas for fortifying our defenses. The operational partnership and extension of our team are really important to us."

She continued, "The support from highly trained security experts to scrutinize incidents and contextualize our security efforts with global trends is extremely valuable. Having frontline insights on major attackers and threats brings me great peace of mind."

To learn more about Trellix, visit trellix.com

> The support from highly trained security experts to scrutinize incidents and contextualize our security efforts with global trends is extremely valuable."
>
> — Chief Information Officer, Multi-Utility Provider

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com