FORCEPOINT

Customer Story
forcepoint.com

# This Energy Provider Keeps the Public's Trust by Doing More Than Keeping the Lights On

A major green energy enterprise safeguards critical assets and business functionality with an integrated solution focused on user and system behavior

Facing multiple external and internal vulnerabilities to both the power grid and their multi-pronged operations, this U.S. company partnered with Forcepoint to deploy a humanly attuned cybersecurity solution that safeguards customer data, intellectual property, substation activity, money movement, and more through a solution, grounded in behavioral analytics, that addresses its challenges holistically instead of in silos.

**Customer Profile**
This large, U.S.-based enterprise energy provider serves tens of millions of customers, with operating revenues in the tens of billions

**Industry**
Energy

**HQ Country**
United States

**Products**
Forcepoint DLP Suite
Forcepoint Behavioral Analytics
Forcepoint Insider Threat

For this major utility, the cyber threats faced by all companies—like data loss and fraud—come with the added complexity of protecting critical infrastructure. Millions of people, companies, and government organizations depend on it, and failure is not an option. Breaches, downtime, and fraud can cause massive problems for both the enterprise and its customers, from loss of revenue and reputation to endangering human safety.

Safeguarding sensitive customer information is always paramount; in this case, that includes a number of high-profile individuals whose home addresses or social security numbers make a tempting target for data thieves looking for a quick payday. Then, of course, there are the millions of dollars flowing through the company, including funds from the resale of renewable energy that could be fraudulently rerouted through altered direct deposit information. Finally, the company's substations, not always managed by a human operator, run the risk of being taken over by an outside entity without the company knowing.

With all these priorities on the table, the enterprise needed a comprehensive and integrated security solution from a partner who understands and aligns with its strategy. That's why the enterprise cybersecurity team turned to Forcepoint.

## Securing the business by understanding user behavior

There was no possible way for the enterprise security team to safeguard the activity of tens of thousands of employees and substations across the region—even with a well-staffed team driven to push ahead. They needed a partner with the tools and commitment to help them address these issues.

**The enterprise needed a holistic solution grounded in a deep understanding of human and entity behavior.**

"They want to be on the edge, and they're always thinking five steps ahead," explains a Forcepoint account executive.

After reviewing the priority risks, the cybersecurity team and Forcepoint identified that, even among these numerous and diverse challenges, there was one through-line: they could all be addressed through a holistic solution grounded in a deep understanding of human and entity behavior. Working in a collaborative partnership, they developed an approach to couple the broad visibility and control of a data loss prevention (DLP) tool with the deeper, more attuned insight provided by Forcepoint Insider Threat and Forcepoint Behavior Analytics.

Forcepoint DLP provides data protection by preventing exfiltration of personally identifiable information and intellectual property across devices, networks, and cloud applications. Behavioral Analytics adds context and takes data protection to the next level by understanding the interactions between humans and data. It does this by ingesting information from multiple sources including cloud applications, email and chat communications, and other security and monitoring products and provides insights to create a comprehensive view of user and entity activity—and even alert to activity indicative of a compromised substation. Insider Threat can then analyze collected information for behavior indicative of fraud or sabotage—including when account numbers are manipulated to execute fraud—as well as provide contextual information to determine intent and archive forensic data to aid in investigations.

Building these three products into a seamlessly integrated solution allows the enterprise to become much more attuned to user behavior, identify anomalous activity, and understand the surrounding context—responding dynamically and minimizing the risk to the company.

**Challenges**

Safeguard high-profile and valuable customer information

Tamp down on potential financial fraud

Protect against threats to power grid from manipulation of headless substations

**Approach**

Forcepoint DLP to improve visibility into employee interaction with data and ensure sensitive info doesn't leave the company

Forcepoint Insider Threat and Behavioral Analytics for improved understanding and documentation of user behavior

## Greater context and specificity generate fewer false positives

Proofs of concept quickly demonstrated the value of this approach. Forcepoint DLP with Behavioral Analytics proved that it could identify, document, and even block file movement by people who have no legitimate need. It also won raves when it provided the flexibility needed to allow emergency response teams to restore power via USB during a natural disaster. Other data protection solutions would have delayed the response because those files would have been blocked, but Forcepoint understands the context and allows the action as part of legitimate business activity.

Behavioral Analytics pulls in historical data to create a baseline, which allowed for quick identification of high-risk anomalies. Insider Threat collects information and provides video recording to add context and confirm that findings are legitimate, not false positives. In a month-long proof of concept, the security team found incidents that led to a number of investigations, including three instances of credential sharing, four instances of data exfiltration, and collection of evidence in an employee investigation.

With all of these technologies working together from an aligned, human-centric approach, the enterprise security team will finally be able to focus on priority risks, without the noise. "They have so many fires to put out every day—it's constant chaos. They need quick, actionable information to actually know where their time is best spent. With our tools they're able to capture that quickly," said the account executive.

> "They need quick, actionable information to actually know where their time is best spent. With our tools, they're able to capture that quickly."
>
> **Forcepoint Account Executive**

## Onsite partnership continuously tunes the solution to stay ahead of threats

Forcepoint has been a constant presence to support deployment, and as the enterprise moves forward with its security strategy, Forcepoint will be there to scale with its needs. True relationships have formed among enterprise team leaders, Forcepoint account representatives, and Forcepoint engineers—including one engineer embedded inside the enterprise to focus on tuning analytics and policies across the platform to deliver the most valuable data.

> "Our overarching goal is to make sure our partnership helps them become future proof."
>
> **Forcepoint Account Executive**

Forcepoint consultants also conducted an insider threat vulnerability assessment based on industry-leading best practices to help the team identify additional susceptibilities and approaches, and is working closely with them to operationalize a holistic insider threat program. And Forcepoint representatives meet with the enterprise's executive team frequently to review deliverables or provide status updates. "We've become trusted advisors to them," said the account executive, "which allows us to dig in further to analyze the risks they face, so we can better protect them."

"Our overarching goal is to make sure our partnership helps them become future proof," said the account executive. "We do our best to keep them ahead of what could be coming their way as technologies advance and threats evolve."

**Results**

Forcepoint DLP considered "mission-critical"

Proof of concept found incidents that led to 10 investigations, including three credential sharing and four data exfiltration

FORCEPOINT



**Contact:** forcepoint.com/contact