

**CASE STUDY**

# Fortune 500 Energy Provider Enhanced Threat Management & Business Resilience with SafeBreach

Learn how this leading energy provider utilized the SafeBreach Exposure Validation Platform to reduce detection and response gaps, enable cross-functional collaboration, and deliver executive-level metrics to measure security program ROI and resilience.

<b>Industry</b>	Energy
<b>Challenge</b>	As cyber threats continue to evolve in complexity and frequency, this Fortune 500 energy provider sought to find a way to move beyond traditional assumptions, silos, and reactive measure
<b>Solution</b>	SafeBreach Exposure Validation Platform
<b>Use Cases</b>	<ul style="list-style-type: none"><li>■ Security Control Validation</li><li>■ Detection Engineering</li><li>■ Executive-Level ROI Reporting</li></ul>
<b>Results</b>	Improve detection and response capabilities.
With SafeBreach, this Fortune 500 energy provider transformed its approach to threat management to:	Enable cross-functional collaboration between Intelligence, Infrastructure, Engineering, and Operations teams.
	Delivered executive-level metrics to measure security program ROI and resilience.

As the largest power provider in its state, this Fortune 500 energy provider has more than 9,000 employees and provides electric and natural gas services for close to 3.5 million people. Its mission to deliver safe, reliable, and affordable power to its customers means they have long prioritized robust cybersecurity practices to safeguard their critical infrastructure and customer trust. As cyber threats continue to evolve in complexity and frequency, this organization's cybersecurity team sought a way to move beyond traditional assumptions, silos, and reactive measures.

## Challenges

### **ASSUMPTIONS AND SILOED OPERATIONS:**

Like many large enterprises, this Fortune 500 energy provider faced challenges due to static security controls and untested configurations. Their teams often operated in silos, with limited feedback loops. This created gaps in detection coverage and left the organization reliant on reactive security measures.

### **NEED FOR EVIDENCE-BASED ASSURANCE:**

The Fortune 500 energy provider needed to replace assumptions with validated, data-driven confidence in its security posture. They sought a proactive approach that would build continuous feedback into detection and response cycles—improving mean time to detect and respond (MTTD/R).

### **SMALL TEAM CONSTRAINTS:**

Unlike global enterprises, which may have three-to-four times the cybersecurity headcount, this organization operates with a relatively lean security team. This disparity in resources makes it challenging to keep pace with the scale and sophistication of modern threats. SafeBreach addresses this gap by acting as a force multiplier—automating continuous validation, capturing logs during simulations, and fetching and analyzing related security data. In doing so, the SafeBreach platform enables smaller teams to achieve the same level of operational effectiveness as much larger organizations.

## Solution: SafeBreach Exposure Validation Platform

This Fortune 500 energy provider partnered with SafeBreach to operationalize an Adversarial Exposure Validation (AEV) program. This program provided the first scalable, repeatable way to:

- Simulate attacker techniques across the **MITRE ATT&CK framework**.
- Continuously validate the effectiveness of security controls.
- Generate evidence-based metrics to guide executive decision-making.

The **SafeBreach Exposure Validation Platform** also enabled this organization to integrate continuous validation into its broader **Continuous Threat Exposure Management (CTEM)** initiatives—aligning closely with scoping, discovery, prioritization, validation, and mobilization cycles.

## Impact Across Teams

### BREAKING DOWN SILOS

This Fortune 500 energy provider used SafeBreach to drive cross-team collaboration:

- Intelligence teams leveraged TTP data from prioritized cyber threat intelligence to refine threat hunting.
- Infrastructure teams used baseline OS configuration data to better manage tool effectiveness.
- Engineering teams evaluated competing security products via controlled simulations.
- Operations teams ran real-time attack scenarios to develop detections.

This holistic approach helped eliminate blind spots, turning detection gaps into actionable improvement areas.

### BOARDROOM RELEVANCE

SafeBreach translated AEV outcomes into business language that resonated with leadership. The executive team of this Fortune 500 energy provider received clear metrics and scorecards—tracking improvements in detection, tool performance, and overall resilience.

## Measuring Success

### THE COMPANY'S SUCCESS METRICS INCLUDED:

<b>Enhanced detection coverage</b>	Enabling blue teams and SOC analysts to develop new detections based on real, validated attacks.
<b>Effective security tool evaluations</b>	Objectively measuring whether new solutions improved defensive posture before full deployment.
<b>Executive dashboards</b>	Providing visibility into simulation trends (e.g., APT test outcomes) and security tool efficacy.

This quantifiable approach turned cybersecurity from a cost center discussion into a strategic business enabler.

"SafeBreach gave our teams the power to validate assumptions, break down organizational silos, and deliver measurable cybersecurity improvements that directly tie back to business priorities."

Lead Threat Management Engineer  
Fortune 500 Energy Provider

## Looking Ahead: Strengthening CTEM with SafeBreach

As part of its broader CTEM strategy, this Fortune 500 energy provider plans to deepen its integration with SafeBreach to continuously validate its entire security ecosystem across Windows, Linux, macOS, and multi-cloud environments. SafeBreach's capabilities—from breach mirroring and **advanced AI remediation** to **Propagate identity-based lateral movement testing**—will provide the company with the tools it needs to stop tomorrow's breaches today.

---

### Get Hands-On with the SafeBreach Platform

**Schedule a personalized demo** today to learn why enterprise security leaders choose the SafeBreach Exposure Validation Platform to enhance the quality, efficacy, and value of their security programs.

#### ABOUT SAFEBREACH

SafeBreach is the leader in enterprise-grade exposure validation, providing the world's largest brands with safe and scalable capabilities to understand, measure and remediate threat exposure and associated cyber risk. The award-winning SafeBreach Exposure Validation Platform combines pioneering breach and attack simulation and innovative attack path validation capabilities to help enterprise security teams measure and address security gaps at the perimeter and beyond. Backed by a world-renowned original threat research team and world-class support, SafeBreach helps enterprises transform their security strategy from reactive to proactive safely and at scale. To learn more about how SafeBreach helps enterprises with end-to-end exposure visibility, visit [www.safebreach.com](https://www.safebreach.com).



#### US Headquarters

526 W Fremont Ave #2880  
Sunnyvale, CA 94087

#### Israel Offices

HaMasger St 35, Sky Tower, Floor 8  
Tel Aviv-Yafo, Israel