

**CLIENT STORY**

# POWER COMPANY SECURES CRITICAL INFRASTRUCTURE FROM STATE-SPONSORED RISK

## How Checkpoint Identified a Crucial Vulnerability

### Securing Critical Infrastructure

Our client is a prominent power and energy company that services some of the largest metropolitan areas in the United States, along with critical facilities in their service area. More than IP and talent security, this client wanted to ensure that its organization's critical infrastructure was safeguarded from state-sponsored risk.

### Utilizing Checkpoint

Strider initiated the review by identifying all entities who had technology embedded in the infrastructure, including third-party partners used in operations. Strider then utilized Checkpoint to screen all identified third-party partners for potential connections to foreign government entities, military, and defense organizations.



### Discovering An Alarming Connection

During the assessment, Strider learned that a substantial portion of the client's critical infrastructure was managed by a third-party company connected to the People's Republic of China (PRC) government, military, and defense organizations. This connection posed a serious risk where the client could potentially lose control of their critical infrastructure to a PRC government entity or actors working on their behalf.

After this discovery, the client severed ties with the management company linked to the PRC government. This action better ensured the safety of their operations and uninterrupted service.

