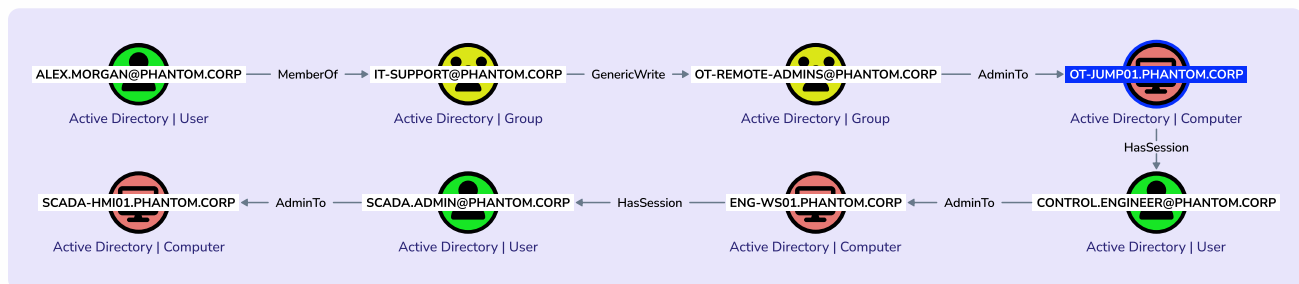


Protecting Energy Environments with BloodHound Enterprise

Adversaries who disrupt energy operations rarely touch the turbines or the plant floor. They ride the identity layer beneath them, the directories and trust relationships linking a corporate account to a facility half a world away, whether it generates power, moves oil and gas, or runs renewable assets. **By the time operators see the disruption, an administrative account has already become the way in.**



The Problem

In energy, a breach that never reaches a control system can still stop production. The business runs on the corporate and IT identity layer that schedules dispatch, moves product, and administers operations. When ransomware or a state-linked operator seizes that layer, facilities go offline even when the operational technology is untouched, and the cost shows up as lost output, threatened safety, and slow recovery.

That layer is harder to defend in energy than almost anywhere else, because it is fragmented and hybrid at once. Many sites run their own directory for autonomy while corporate identity lives in the cloud and federates down into them, alongside the service accounts and AI agents that automate operations. Security review stays limited, vendors install tooling with domain administrator rights by default, and acquisitions fold in trusted forests no one has mapped. **Over time, standing privilege and unmapped trust reach from a cloud login to the boundary of operations.**

The Solution

BloodHound Enterprise gives defenders the adversary's map of the directories that run operations. Deployed on-premises where sites cannot depend on the cloud, it reveals the attack paths inside an autonomous directory and gives teams a way to build or enforce a tiered model and hold it as the environment changes. **Directories that grew up as plumbing for tooling become environments where teams can see, prioritize, and contain privilege and trust, with each finding carrying the remediation that removes the most attack paths.**

Beyond the isolated site, BloodHound Enterprise maps what adversaries see across the connected enterprise. OpenGraph, its extensible attack graph engine, extends that map across Active Directory, Entra ID, cloud platforms, and SaaS. Identities chain across all of them in a single graph, including the service accounts, workloads, and AI agents that automate the business and inherit privilege the moment they exist. Where corporate identity federates or trusts into operational directories, it surfaces the relationships and reachability adversaries count on.

How BloodHound Enterprise Meets Energy's Security Needs

BloodHound Enterprise maps the attack paths that reach an organization's critical assets and pinpoints the fixes that eliminate the most risk. Privilege Zones extend that protection to the assets specific to energy operations: **the privileged access workstations and jump hosts that bridge toward the OT boundary, and the scheduling, dispatch, and energy-trading systems** whose loss halts the business. It reveals which identities can cross those boundaries, and because it maps the environment as it runs today rather than as the documentation claims it was built, teams can secure what actually exists after decades of change and the turnover that erodes institutional memory.

BloodHound Scentry brings SpecterOps' attack path experts alongside your team, from uncovering complex paths to designing coverage for the applications an operation depends on. BloodHound Hunter puts that intelligence into natural language, so an analyst, an identity admin, and an executive can each understand what their exposure means and act on it. Together, this meets a regulatory landscape moving from checklists toward threat-informed, attack-path-based assessment.

- ✓ **Tiered Model Resiliency**
Reveals where routine directory changes open unintended paths into the administrative tier, so teams can sustain a tiered model as the environment changes.
- ✓ **Trust Sprawl Across Sites**
Traces trust across domains and forests to show where an account in one environment reaches administrative control in another, including the trusts acquisitions leave behind.
- ✓ **Cloud, Non-Human, and AI Identity**
Follows identity from the corporate cloud into on-premises and operational directories, exposing how federated users, service accounts, workloads, and AI agents reach privilege they were never meant to hold.
- ✓ **Accounts That Outlive Their Purpose**
Surfaces the stale, contractor, and vendor accounts that keep their privilege long after the work ends, and the access they still hold toward critical systems.

Taken together, that coverage answers the question no configuration audit can: given everything in place across your environment, where can an adversary go from any particular point in your identity and application network?

Energy Is One Piece of a Larger Attack Surface

The paths that reach energy operations rarely start there. One can begin with a corporate cloud login, cross a trust an acquisition left behind, and land on the accounts that administer a remote facility, one step from production. Each hop looks legitimate to the system that owns it; the full path appears only when cloud, identity providers, and on-premises directories sit in one graph.

BloodHound Enterprise brings the same attack path analysis to every identity source that touches the enterprise, from identity providers and cloud platforms to endpoints, code repositories, and the AI identities entering operations. Brought into one graph, those sources expose the cross-platform paths that form between systems, across administrative boundaries, and beyond the reach of any single platform review.

Ready to see your energy environment the way adversaries do? Request a demo of BloodHound Enterprise.

specterops.io/get-a-demo

