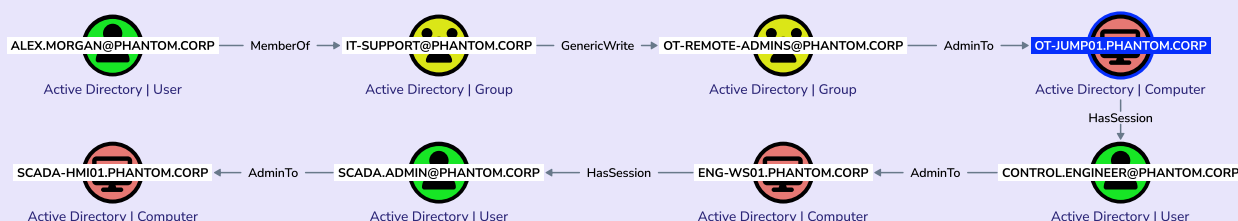




Securing the IT/OT Boundary at the Identity Layer

Protecting Operational Technology Environments with BloodHound Enterprise

Reaching operational technology (OT) environments rarely takes an OT exploit. It takes a valid account on the IT network and a path across the boundary. The control systems on the other side run building HVAC, a power grid, or a water treatment plant. **An air gap stops network traffic. It does not stop an account that already has access on both sides.**



An identity path from a standard IT user to a SCADA HMI, as BloodHound Enterprise maps it. Placing OT assets in a Privilege Zone flags every path like this one that crosses into OT.

The Problem

For at least five years, the PRC state-sponsored group Volt Typhoon held footholds inside the IT networks of some US critical infrastructure organizations. [CISA, the NSA, and the FBI reported the campaign in 2024](#). The actors relied on valid accounts and living-off-the-land techniques, leaving little for malware-based defenses to catch. The agencies assess that their purpose was to pre-position on IT networks to enable lateral movement into OT and disrupt operations in a crisis or conflict. The compromises concentrated in energy, water, communications, and transportation.

The exposure Volt Typhoon exploited is not unique to those sectors. Operational technology is supposed to be isolated, and on paper it often is. **But an OT environment no one can reach is an OT environment no one can run**, so engineers, vendors, and management systems connect through accounts that cross the boundary. The far side is rarely defended: integrators stand up the Active Directory inside an OT environment to bring production online, then seldom return to assess or patch it.

The Solution

BloodHound Enterprise enforces the boundary an air gap can't: it finds the identity paths that cross into OT and severs them before an adversary can walk them. It is the identity layer of an OT security strategy. Where OT asset discovery and passive monitoring watch the control network, **BloodHound Enterprise answers the question they cannot: who can reach OT through identity.**

That answer starts with the OT crown jewels. Privilege Zones place the domain controllers, jump hosts, engineering workstations, and historians that run and reach the OT environment inside a defined boundary, and BloodHound Enterprise flags any identity or change that could cross it. Paths into the zone converge on Choke Points, and because a Choke Point can carry thousands of attack paths, fixing it closes the most exposure with the fewest changes to an environment that cannot go down.

Beyond the boundary, BloodHound Enterprise models the whole estate an adversary would traverse. It maps on-premises Active Directory and Entra ID natively. With OpenGraph, BloodHound Enterprise's extensible attack graph engine, that same graph extends to the cloud and SaaS platforms that run the business. Where corporate domains trust into an OT directory, it collects across that trust and maps the reach it creates, along with the service accounts, workloads, and vendor accounts that hold standing access into OT.

Built for Restricted Environments

BloodHound Enterprise supports both federal deployment models. For agencies that consume authorized cloud, it is available as FedRAMP High authorized SaaS.

For the restricted and air-gapped networks common to OT, it deploys fully on-premises, with the same coverage and no sensitive identity data leaving your boundary, aligned with NIST 800-171, NIST 800-53, and CMMC.

How BloodHound Enterprise Meets OT's Security Needs

Zero Trust assumes an adversary will cross the boundary and requires segmentation and least privilege to hold under that assumption. BloodHound Enterprise is the verification layer for OT, continuously testing whether the IT/OT boundary segments identity and surfacing where it does not, so teams can enforce least privilege across the boundary with evidence that it holds.

It maps the environment as it runs today, after years of change and the turnover that erodes institutional memory, so OT teams can secure the directories they run as they exist now. BloodHound Scentry brings SpecterOps' attack path experts alongside the team to uncover the highest-risk paths into OT and design the Privilege Zones that fit a given environment.

What BloodHound Enterprise Does for OT

✓ The IT/OT Identity Boundary

Reveals where a routine change or an over-permissioned account opens an identity path from the enterprise into the OT environment, so teams can close it before an adversary crosses.

✓ Trust Sprawl Across IT and OT

Traces trust across domains and forests to show where an account in the corporate environment reaches administrative control in the OT directory, along with the trusts acquisitions leave behind.

✓ Remote and Vendor Access

Follows the jump hosts, remote access infrastructure, and vendor accounts that bridge into OT, showing which identities can ride them across the boundary.

✓ Accounts That Outlive Their Purpose

Surfaces the stale integrator, contractor, and vendor accounts that keep privilege long after commissioning ends, and the access they still hold toward OT 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?

OT Is One Piece of a Larger Attack Surface

The paths that reach OT rarely start there. One can begin with a corporate cloud login, cross a trust into the OT directory, and land on the accounts that administer an engineering workstation, one step from the control systems. BloodHound Enterprise brings every identity source that touches the enterprise into one graph, from identity providers and cloud platforms to endpoints and the non-human identities entering operations, so the full path stays visible across each system it crosses.

Ready to see who can reach your OT through identity? Request a demo of BloodHound Enterprise.

specterops.io/get-a-demo

