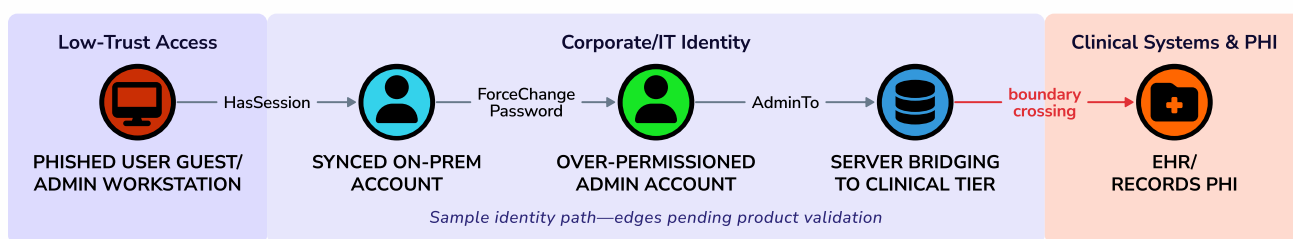




Protecting Healthcare Environments with BloodHound Enterprise

A hospital's patient records sit behind boundaries an adversary never has to break. Reaching them takes one compromised identity, human or machine, riding the trust relationships that link every corner of a health system.

The account that opens the records was never meant to touch them.



The Problem

Roughly 190 million people had their personal and health data exposed in the [2024 Change Healthcare breach](#), the largest in the history of American healthcare. An adversary signed into the company's remote-access portal with a stolen credential and no multi-factor authentication in the way, then moved through the environment and deployed ransomware that took down the systems routing a large share of the country's prescriptions, claims, and payments. **Pharmacies could not fill orders and providers went unpaid for weeks.** Nothing about Change Healthcare made it uniquely exposed; the same paths from a stolen credential to patient records exist in any healthcare organization.

What makes that layer so hard to defend in healthcare is an estate that can neither be pruned nor held still. A hospital runs separate networks for its waiting rooms, its staff, and its clinical systems, and because care cannot go down, the boundaries between them soften as access piles up and is rarely revoked. Mergers accelerate it. Every hospital absorbed into a larger system and every payer that consolidates brings its own identity systems and trust into an environment no one had fully mapped, and the complexity compounds with each deal. Service accounts, workloads, and AI agents automate the rest, inheriting reach the moment they exist. **Over time, standing privilege and unmapped trust outpace anyone's ability to track them, until a path opens from a low-trust foothold to the records at the center.**

The Solution

Healthcare teams live with a hard constraint: they cannot freely change an environment that has to stay up for patients and claims. BloodHound Enterprise works within these constraints, mapping every path an adversary could take from a low-trust identity to the clinical systems and PHI at the center, then surfacing the choke points where those paths converge.

Because one choke point can carry thousands of attack paths, remediating it becomes a force multiplier, closing the most exposure with the fewest changes to a live environment. Privilege Zones extend that control to a healthcare organization's business-critical assets, the EHR where records live, the platforms managing connected medical devices, and the billing and claims infrastructure, flagging any identity or change that could reach across those boundaries before an adversary does.

Beyond any single environment, BloodHound Enterprise models the whole estate an adversary would traverse.

It maps on-premises Active Directory and Entra ID, and OpenGraph, its extensible attack graph engine, extends that same graph to the cloud platforms and SaaS that run the business, so an identity that starts on a managed laptop and ends at a records system stays visible the entire way. That graph includes the service accounts, workloads, and AI agents that automate clinical and administrative work and inherit privilege the moment they exist. It also resolves the trust a merger folds inward, where an acquired environment's forests and tenants join the estate carrying access no one has mapped, along with the inbound trust that vendors and contractors hold into it.

How BloodHound Enterprise Meets Healthcare's Security Needs

Because BloodHound Enterprise maps the environment as it is configured now rather than as its documentation describes, teams can secure the estate they operate today, after years of change and the turnover that erodes institutional memory.

BloodHound Scentry brings SpecterOps' attack path experts alongside the team to uncover the highest-risk paths and design the Privilege Zones that fit a given environment. BloodHound Hunter turns that analysis into natural language, letting an analyst, an identity admin, and a compliance officer each see where their exposure leads and what to do about it. Together, this answers HIPAA and HITRUST on the terms they are moving toward, threat-informed and grounded in the attack paths that reach patient data.

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?

Capability Categories

- ✓ **Boundaries Between Care and Everything Else**
Reveals where a routine change or an over-permissioned account opens a path across the boundaries that separate clinical systems and PHI from everything else, so teams can close it before an adversary crosses.
- ✓ **Trust That Mergers Leave Behind**
Traces the trust an acquisition folds inward, exposing where an account in a merged environment reaches administrative control across the combined estate.
- ✓ **Cloud, Non-Human, and AI Identity**
Follows identity across on-premises, cloud, and SaaS, 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 device-vendor accounts that keep privilege long after the work ends, and the access they still hold toward clinical systems and records.

Healthcare Is One Piece of a Larger Attack Surface

The paths that reach patient data rarely start near it. One can begin with a login to a corporate cloud account, cross a trust an acquisition folded inward, and land on the accounts that administer a newly acquired practice, one hop from the clinical systems and records at the parent organization's core. **Each step looks legitimate to the system that owns it, and the full path appears only when cloud, identity providers, endpoints, and on-premises environments sit in one graph.**

BloodHound Enterprise brings the same attack path analysis to every identity source that touches the organization, from identity providers and cloud platforms to endpoints, code repositories, and the non-human and AI identities entering the environment. 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 healthcare environment the way adversaries do? Request a demo of BloodHound Enterprise.

specterops.io/get-a-demo

