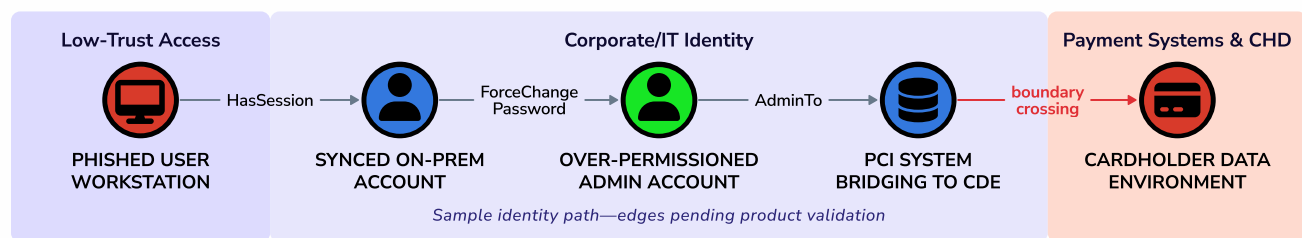


Protecting Financial Services Environments with BloodHound Enterprise

The systems that move money and hold customer financial data sit behind identity, and the attack paths that reach them pass through accounts no one is watching. A service account, a cloud role, or a contractor login can hold standing access across banking, insurance, capital markets, and payments long after anyone remembers granting it. **Adversaries follow that access to the systems it was never meant to reach.**



The Problem

Roughly 106 million people in the United States and Canada had their data exposed in the [2019 Capital One breach](#), one of the largest in the history of American banking. An adversary obtained a temporary credential for a cloud role, and because that role held standing read access far beyond its function, a single identity had access to customer records, credit applications, Social Security numbers, and bank account numbers stored across the environment. The role was the vehicle, and **the same over-permissioned roles exist in any institution running a hybrid cloud estate.**

What makes that layer so hard to defend in finance is that access only accumulates. An institution runs banking, trading, insurance, and payments across on-premises directories and the cloud at once, and because money movement can never go down, permissions get granted and rarely revoked. Acquisitions fold in identity systems no one has fully mapped, vendors and fintech partners hold standing access into the environment, and service accounts, cloud roles, and AI agents inherit privilege the moment they exist.

Regulation keeps the hybrid seam permanent by requiring both on-premises control and cloud resilience. Over time, over-permissioned identities outnumber the people who could account for them, until a path opens from an ordinary identity to the systems that move money or store highly sensitive data.

The Solution

A frustrating reality for security teams: An over-permissioned identity is the shortest path to the assets and data a financial institution runs on, and no configuration review can show where it leads. BloodHound Enterprise maps every path an adversary could take from an ordinary identity to the systems that move money and hold customer records. It then surfaces the Choke Points where those paths converge. Because one Choke Point can carry thousands of attack paths, remediating it resolves the most exposure with the fewest changes to an estate that can't afford downtime.

Privilege Zones draw a hard line around the assets a financial institution cannot afford to lose: money movement across wire, ACH, and card rails, and the core banking and customer-data systems of record. BloodHound Enterprise flags any identity that could cross it before an adversary does.

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

OpenGraph, its extensible attack graph engine, extends the graph beyond Active Directory and Entra ID to the cloud platforms and SaaS that run the business, so an identity that starts on a managed laptop and ends at a payments system stays visible the whole way. The graph includes the service accounts, cloud roles, and AI agents that inherit privilege the moment they exist, and the trust an acquisition folds into the environment. BloodHound Hunter lets an analyst, an identity admin, and a compliance officer query the graph directly in plain language, each asking where their exposure leads, and brings that attack-path intelligence into the AI systems the institution runs.

How BloodHound Enterprise Meets Finance's Security Needs

BloodHound Enterprise maps the environment as it is configured today rather than as its documentation describes, so teams can secure the estate they operate after years of mergers, migrations, 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.

Financial institutions answer to PCI DSS, the Gramm-Leach-Bliley Act, FFIEC guidance, and DORA, each of which turns on who can reach the data and systems they protect. BloodHound Enterprise gives teams that evidence by showing which identities can reach cardholder data, customer financial records, and the systems that move money, and as FFIEC and DORA move toward threat-informed, attack-path-based assessment, that same map meets them on the terms they are adopting.

Coverage Across Your Identity Attack Surface

✓ Boundaries Around the Systems That Move Money

Reveals where an over-permissioned identity can cross into the systems that move money and hold customer records, so teams close the path before an adversary exploits it.

✓ Trust That Mergers Leave Behind

Traces the trust an acquisition or consolidation 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 a cloud role or service account carries standing access far beyond the function it was created for.

✓ Accounts That Outlive Their Purpose

Surfaces the stale, contractor, and vendor accounts that keep privilege long after the work ends, and the access they still hold toward money and customer 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?

Finance Is One Piece of a Larger Attack Surface

The paths that reach money and customer financial data rarely start near them. One can begin with a corporate cloud login, cross a federated trust into a production cloud account, and land on an over-permissioned role that reaches the stores holding customer financial records. **Each step looks legitimate to the system that owns it, and the full path appears only when cloud, identity providers, endpoints, and on-premises directories sit in one graph.**

BloodHound Enterprise brings the same attack path analysis to every identity source that touches the institution, 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 financial services environment the way adversaries do? Request a demo of BloodHound Enterprise.

specterops.io/get-a-demo

