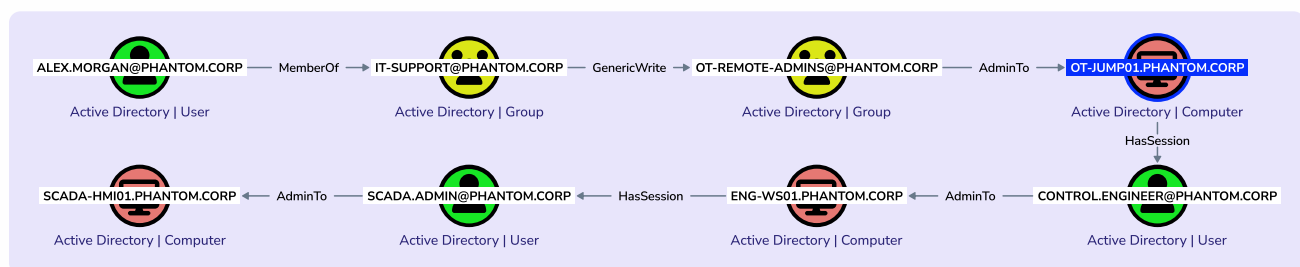


Securing Manufacturing at the Identity Layer

Protect Production by Securing Paths That Lead to It, From IT to the Plant Floor

Many manufacturing lines cannot stop. A steel mill with molten metal in the furnace cannot pause for a patch window, and a just-in-time plant that comes to a halt takes its suppliers down with it. Adversaries know that security fixes compete with uptime. **They rarely need an exploit on the production floor when a valid account on the IT network and an identity attack path to the systems that run production will do the job.**



The Problem

[Norsk Hydro estimates](#) the March 2019 attack on its operations cost around NOK 800 million. Adversaries captured administrator credentials, [escalated to domain administrator, and used Active Directory](#) to push ransomware across the company's global network. The ransomware did not directly reach control systems, yet the damage still landed on production. Hydro's smelting and other continuous businesses held output near normal only by switching to labor-intensive manual procedures, and its extrusion business absorbed the heaviest losses.

Hydro's exposure is common across manufacturing. Engineers reach production systems, vendors connect for remote support, service accounts link business applications to the plant floor, and identity systems span every site. Each connection serves a legitimate purpose, but together they form paths an adversary can follow from a compromised IT account toward production.

Closing those paths the usual way means touching the systems that cannot stop. Patching, reconfiguring, or isolating production infrastructure requires a maintenance window, and continuous and just-in-time operations rarely have one to spare. An unplanned stop costs far more. After an IT-side incident [halted Jaguar Land Rover's global manufacturing for five weeks](#) in 2025, the UK's [Cyber Monitoring Centre estimated the economic impact at £1.9 billion](#).

The Solution

BloodHound Enterprise closes the paths to production without waiting for a maintenance window. It traces how identities and privileges chain from the IT network toward the plant floor and shows where to cut them, and the most effective cuts usually sit several steps upstream of production. Removing an unneeded permission or tightening a service account breaks the path on the IT side, so the systems that cannot stop rarely have to.

It adds the adversary's view to the security stack manufacturers already run. Segmentation, OT monitoring, and privileged access management each protect their own layer. BloodHound Enterprise answers the question that spans them: what can reach production through identity.

Assess the Identity Risk in an Acquisition

Every acquired plant arrives with its own directory, administrators, and years of accumulated permissions. BloodHound Enterprise brings an adversary's view to cyber due diligence and maps what changes when that environment connects to yours: which inherited identities can reach your production assets, and which of yours can now reach theirs. Teams can close those paths during integration, while the fixes are still cheap.

Built for Isolated Plant Networks

Many plants run on networks with limited or no internet access. BloodHound Enterprise deploys fully on-premises for those environments, with the same coverage as SaaS and identity data kept inside your boundary. Connected sites can run it as SaaS.

Ready to see what can reach your production systems through identity? Request a demo of BloodHound Enterprise.

specterops.io/get-a-demo



What BloodHound Enterprise Does for Manufacturers

✓ Draw the Boundary

Place your critical production assets in a Privilege Zone, including MES and engineering systems that sit outside the admin tiers security teams usually protect, and BloodHound Enterprise turns that boundary into a continuous identity check.

✓ Find the Crossings

BloodHound Enterprise surfaces every identity path that reaches into the zone from the IT side and keeps watching as plants, vendors, and accounts change.

✓ Cut the Most Paths

Guided remediation prioritizes the choke points where one upstream fix eliminates the most routes, including the stale accounts and lingering permissions that years of change leave behind.

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?