Deloitte. | ANTHROP\C



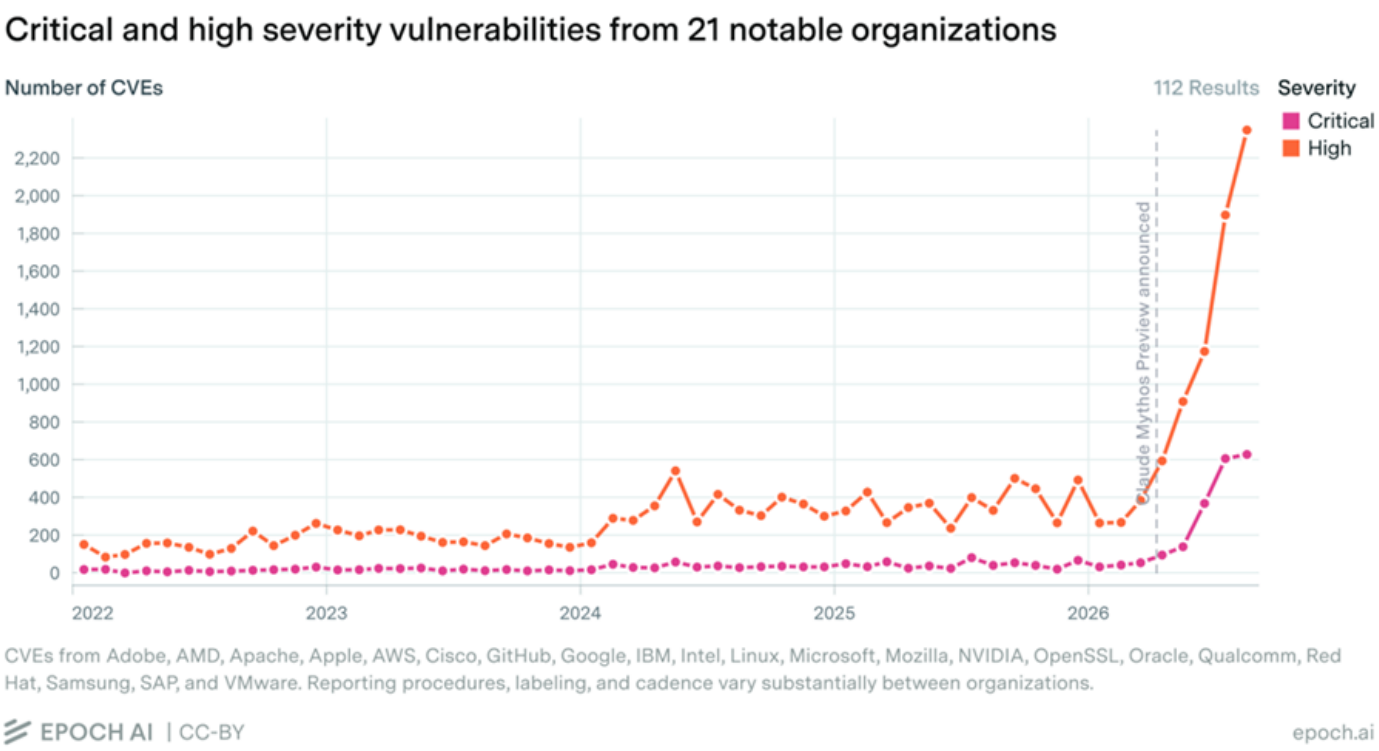
ACCELERATING VULNERABILITY REMEDIATION AND IMPROVING RESILIENCE FOR CRITICAL INFRASTRUCTURE

As threats to critical infrastructure continue to rise, Deloitte is pleased to announce it will join Anthropic's Critical Infrastructure Defense Program to help organizations implementing transformative artificial intelligence (AI) protect these environments from advanced threats. For operators in energy, utilities, financial services, health care and transportation, a delayed patch isn't just a compliance gap. It's a window an attacker can use to disrupt services that entire communities depend on. For Deloitte's clients, using AI to detect vulnerabilities and build stronger defenses is a key part of transformation, and Claude can help cybersecurity teams do more.

Participation in the Critical Infrastructure Defense Program will expand Deloitte's capabilities through its industry-leading Critical Infrastructure Cyber program to deliver the AI-powered services clients need to address an evolving threat landscape. By leveraging Claude in cybersecurity workflows, organizations can strengthen operational technology (OT) governance, improve their compliance posture and reduce regulatory risk.

As AI accelerates how quickly vulnerabilities are found and exploited, closing the gap between discovery and safe, machine-speed remediation is critical.

The stakes are highest where systems keep the lights on, the water running and the financial system functioning. According to Epoch AI, more vulnerabilities have been discovered in 2026 alone than in the previous five years combined.[1]

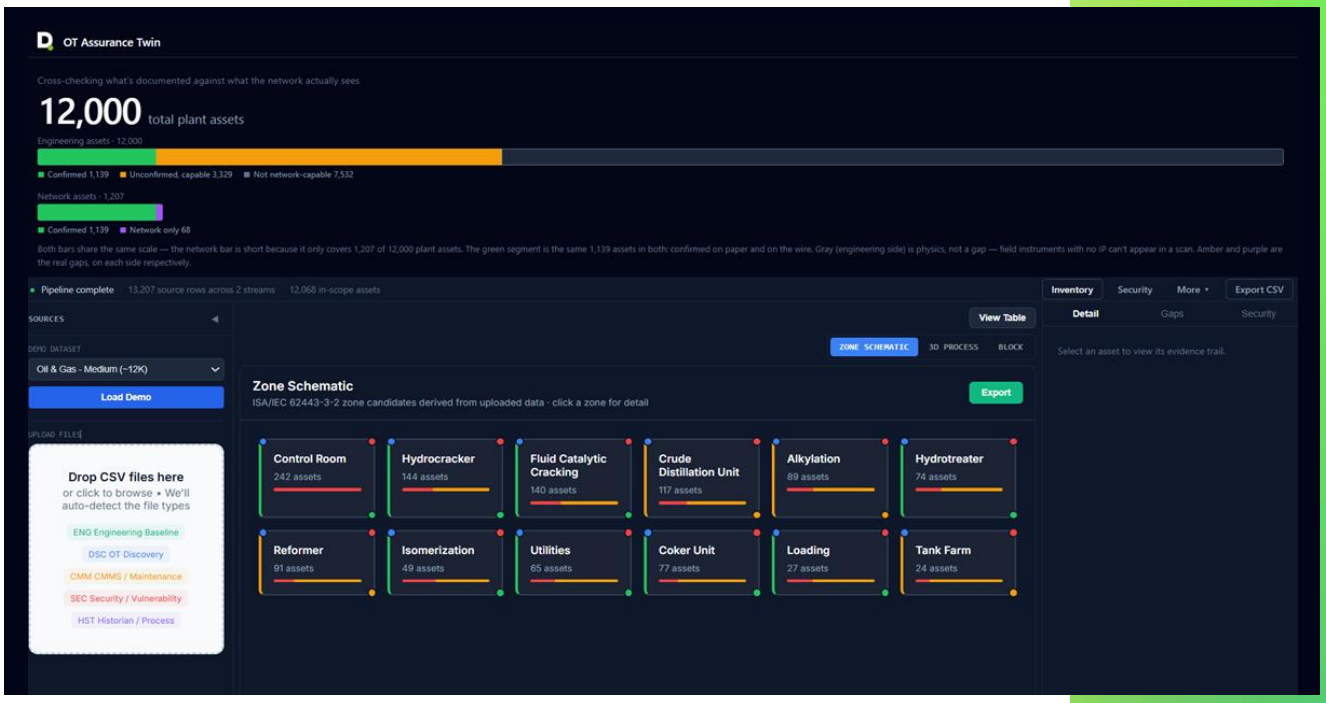


WHY THIS MATTERS MOST FOR CRITICAL INFRASTRUCTURE

As AI grows more sophisticated, nation-state actors increasingly probe critical infrastructure defenses for weaknesses. Operators face this challenge under tighter constraints than many other enterprises. Legacy systems, operational technology and industrial control environments often can't be patched as quickly as standard IT, and outages carry consequences well beyond the business. These operators are also among the most targeted because a successful attack can ripple far beyond a single organization. High consequences, low tolerance for disruption and outsized attacker interest make closing the gap between discovery and a validated fix a resilience necessity—not just a security metric—with public safety and essential services on the line.

Organizations also can't patch vulnerabilities on assets they can't see. To help operators turn visibility into risk reduction, Deloitte has worked with Anthropic to enable Claude to enrich asset data and conduct discovery. Combined with Deloitte's AI Remediation Suite™ powered by Claude, this approach can support patch creation at machine speed.

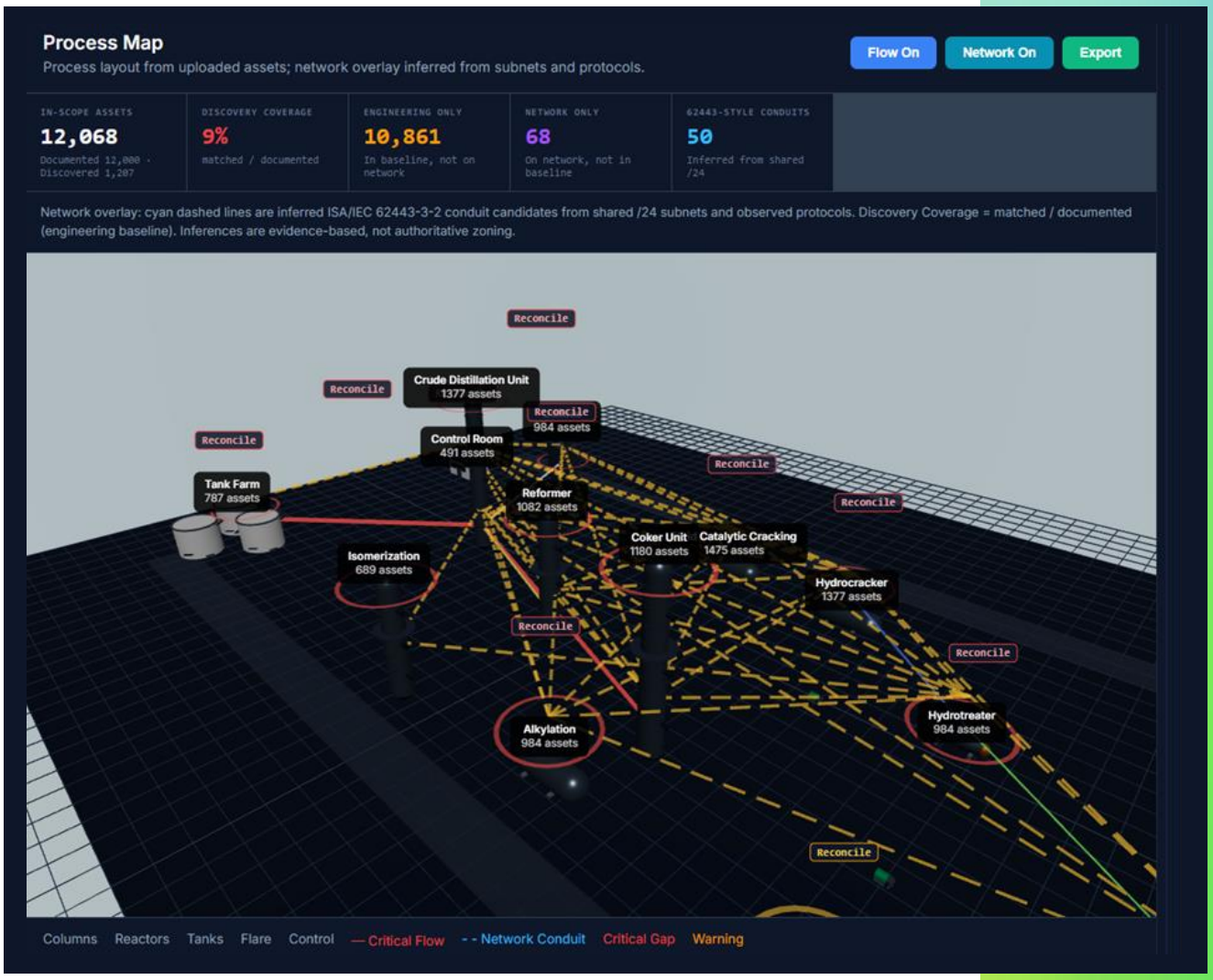
Many organizations have invested heavily in network monitoring and asset discovery, yet still struggle to fully understand the assets behind their operations. Traditional visibility solutions depend on network connectivity, which leaves blind spots such as disconnected equipment and industrial systems behind intermediary devices.



Documented versus observed: Of 12,000 engineering assets, only 1,207 are visible on the network, exposing assets that exist on paper but not on the wire, and vice versa.

A CLAUDE-POWERED APPROACH COMBINING ASSET VISIBILITY AND REMEDIATION

Claude creates dynamic visibility into network assets, discovers vulnerabilities across them and helps create patches, acting as a resilience assistant for critical infrastructure organizations.



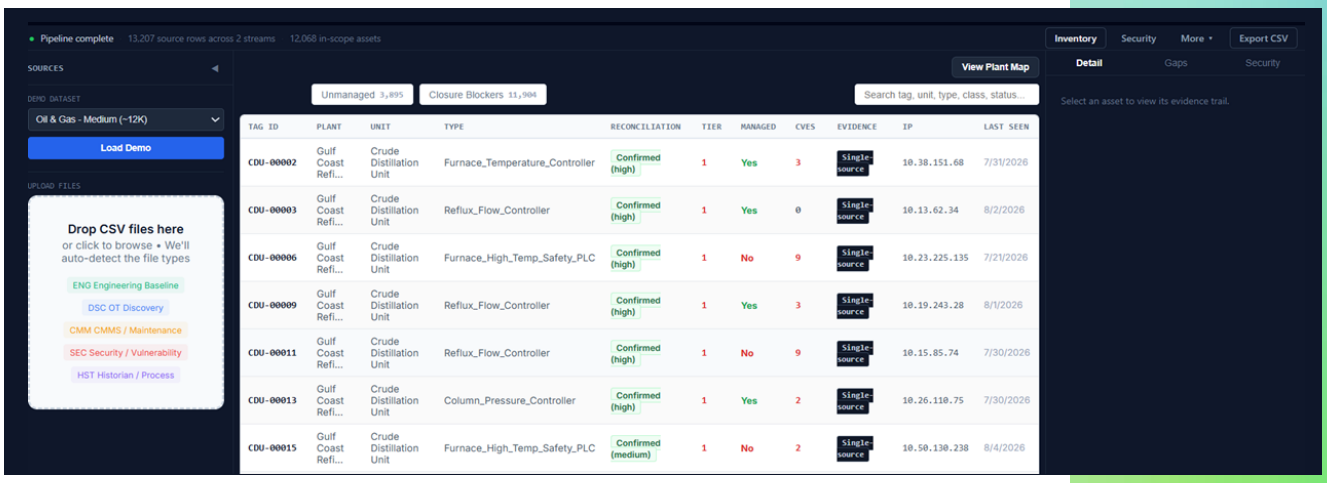
A process-level view created by Claude maps assets to the units they support, turning a flat asset list into an operational picture and flagging gaps for reconciliation.

The capability goes beyond cataloging. By mapping how assets support production processes, it helps teams understand where a system fits within a plan or workflow, respond faster and collaborate more effectively.

That enriched data also underpins smarter risk management: combining visibility, asset context and operational importance enables organizations to prioritize the risks that matter most to mission-critical operations. But visibility alone isn't enough. Turning fragmented data into operational intelligence makes visibility a genuine enabler of resilience and a natural complement to Deloitte's AI Remediation Suite.

USING VISIBILITY TO DRIVE REMEDIATION AND RESILIENCE

Patching every system at once is difficult. Operators need to make strategic choices and find ways to deploy countermeasures and harden systems that can't be patched immediately.



Down to the individual device: Each asset is reconciled with a confidence tier, managed status, CVE exposure and evidence trail.

AI-ENABLED CAPABILITIES OPERATORS NEED

- **Asset reconciliation:** Reconcile data across the Configuration Management Database (CMDB), passive OT systems, engineering drawings and vendor lists to surface gaps and conflicts between sources.
- **Ownership and criticality:** Establish ownership and criticality for each asset.
- **Shadow and orphaned assets:** Expose assets that may carry risk without an owner or budget.
- **Reconciliation layer:** Provide a layer within an organization's data fabric or as a standalone tool.
- **Vulnerability discovery:** Find vulnerabilities and attack vectors across the estate and scan code for novel risks.
- **Software remediation:** Generate, source, validate and orchestrate fixes across open-source and proprietary code.
- **Testing and validation:** Verify fixes through automated application, infrastructure, regression and deployment testing.

"WE CAN'T PATCH ALL OF THE SYSTEMS ALL OF THE TIME"

Patching every system at the speed needed to reduce risk isn't always practical. Visibility and discovery help operators prioritize, and AI has made finding vulnerabilities easier than ever. The harder problem is what comes next: prioritizing intelligently, engineering fixes that hold up, testing them rigorously and deploying them safely.

Deloitte's AI Remediation Suite, powered by Claude, was designed to help close that gap and give operators the control they need to secure critical infrastructure.

 Copyright © 2024 For information contact Deloitte Global.



Contact to learn more:

Adnan Amjad
Partner
US Cyber Leader
Deloitte & Touche LLP
aamjad@deloitte.com

Naresh Persaud
Principal
US Cyber Leader
Deloitte & Touche LLP
napersaud@deloitte.com

Endnotes

1. Epoch AI. Cyber vulnerabilities - interactive explorer. 2026.

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

As used in this article, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.