

A Practical Guide to CI Fortify

What the new federal isolation and recovery mandate requires of critical infrastructure operators, and where BigID fits into meeting it.

CISA's CI Fortify initiative, built with the Australian Signals Directorate, the UK's NCSC, and Canada's Cyber Centre, tells critical infrastructure operators to plan for cloud, telecom, and third-party connections going unreliable in a conflict scenario, and to keep essential services running through it. The isolation path runs six steps: identify vital systems, map every connection, classify by criticality, build separation points, test the plan, recover what's compromised. Nearly every step assumes an organization already knows where its sensitive data lives.



What CI Fortify Requires

Step	What It Means
Identify vital systems	Know the minimum systems needed to deliver a critical service
Map connections	Document every link to cloud, vendors, remote access, third parties
Classify by criticality	Tier systems by trust and sensitivity, not guesswork
Build separation points	Harden and segment access ahead of an incident
Test the isolation plan	Validate against the real environment, not a stale audit
Recover	Rebuild the highest-impact systems first



Where This Sits Against NIST CSF

Most operators already have some of this mapped to NIST CSF. Identify covers asset inventory and data flow mapping. Recover covers restoration planning. CI Fortify doesn't replace that work, it stress-tests it against a scenario CSF was never built to test for.

- **Where CSF already gets you partway there.** If Identify and Recover are mature, the asset inventory and recovery planning CI Fortify asks for aren't starting from zero.
- **Where CI Fortify goes further.** CSF is a voluntary, risk-based maturity model measured against a documented recovery time objective. CI Fortify asks for something more specific and more extreme: sustained isolation from every third-party dependency for weeks or months, not a best-effort restoration window.
- **Where the mandate changes the stakes.** CSF adoption is self-assessed. CI Fortify comes with CISA running targeted assessments directly, turning a framework gap into an active audit question rather than an internal maturity score.

That's the shape of it: a mandate layered on top of a framework most operators already have in some form, with a harder scenario and a federal agency now checking the work. The starting point for closing that gap is the same data question CI Fortify assumes is already answered.



How BigID Helps, Step by Step

- **Know what data lives where.** BigID discovers and classifies data across structured and unstructured sources, cloud and on-prem, so an organization can see which systems genuinely hold the data behind a critical service instead of relying on an architecture diagram that's years out of date.
- **Map every connection.** Data mapping traces flows to third-party vendors, SaaS platforms, and cloud environments, turning a manual connection audit into something that can be queried on demand and kept current as the environment changes.
- **Classify by real criticality.** Sensitivity classification gives isolation tiers an actual basis: a system holding regulated customer data gets prioritized differently from one holding marketing assets, based on the data itself rather than assumption.
- **Harden access ahead of an incident.** Access intelligence surfaces who and what has standing access to sensitive data, including vendors, remote access tools, and service accounts, the same surface CI Fortify wants segmented before isolation, not discovered during it.

- **Keep the isolation plan current.** A living, continuously updated data inventory means the plan gets tested against the real environment instead of a stale audit, so it holds up the first time it's actually needed.
- **Sequence recovery by impact.** A classified, prioritized inventory answers the first question of recovery directly: which systems come back online first, based on sensitivity and business impact rather than whichever system happens to boot first.
- **Run without a cloud dependency.** On-prem and air-gapped deployment options mean the platform doing this work isn't itself one of the third-party dependencies severed the moment isolation begins.



AI Classification and Data Sovereignty

Most data classification tools call out to a third-party model to do the work. Every scan sends sensitive data, or metadata about it, to a provider outside the organization's control, a sovereignty exposure that holds on a normal Tuesday, independent of any crisis. CI Fortify's isolation scenario turns that standing exposure into a hard operational failure, since a cloud-dependent AI tool goes dark right along with the connectivity it needs. BigID runs data intelligence and classification without a dependency on an external LLM provider. Processing stays inside the customer's environment, reachable or not.



Air-Gapped: From Edge Case to Baseline

Most vendors treat air-gapped deployment as a rare federal ask. CI Fortify makes it a baseline requirement for anyone running critical infrastructure: isolation takes down every cloud dependency at once, including whatever tool watches the data.

- **No external calls required.** Discovery, classification, and governance operate with zero outbound connectivity.
- **No phone-home telemetry.** The platform doesn't need to reach BigID or any other outside service to keep functioning.
- **No dependency on a hosted API.** Processing and policy enforcement run locally, inside the customer's environment.

- **No silent failure mode.** The security tooling doesn't go dark alongside the systems it's supposed to help isolate.



Priority Actions

- **Inventory the real map.** Establish where sensitive and operational data actually lives, not where it's documented to live.
- **Map every third-party flow.** Trace data flows to every vendor, cloud platform, and remote access tool touching that data.
- **Classify by criticality.** Tier data and systems so isolation and recovery priorities reflect real risk, not guesswork.
- **Audit AI dependencies.** Check whether AI-driven tooling depends on an external model provider, and treat that as a sovereignty gap even outside a crisis.
- **Confirm air-gapped capability.** Verify the platform doing this mapping can run fully air-gapped, not just cloud-optional.
- **Build a tested recovery sequence.** Base it on data sensitivity and business impact, and test it before it's needed.

Where to start: for most organizations, the fastest path through this list runs through one question first, where sensitive data actually lives. Connection mapping, criticality tiers, and recovery sequencing all depend on getting that answer right before anything else on this list will hold up.

CI Fortify asks critical infrastructure operators to prove they can run blind to the outside world for months at a stretch. The organizations that can do that will be the ones that already know, in specific and current detail, what data they're protecting, where it lives, and whether the tool watching over it needs the outside world to keep working.

CUSTOMER VALIDATION

Proof in Action

"BigID gives me better visibility into sensitive data, helps prioritize security protections, reduces attack surfaces, strengthens compliance, and increases operational efficiency overall — a strategic pillar of our AI-First Cybersecurity Transformation"

- CISO, Global Healthcare Company

"We needed to automate processes and data management across systems for the data of a few million customers across a lot of systems and data. BigID was the one solution that did this in the most efficient and sophisticated way - and had more use cases we could add on moving forward."

- Chief Privacy Officer, Global Telecoms Company

ANALYST RECOGNITION

Validated by Industry Leaders

- 2025 Company of the Year for AI Governance - Frost & Sullivan
- Named a Leader across all DSPM research including Omdia DSPM Universe, CB Insights for DSPM, TAG, GigaOm, Frost & Sullivan
- Named a Leader in all Privacy Management evals including Forrester Privacy Management Wave & IDC Privacy Compliance MarketScape
- BigID named a Leader across 4 GigaOm evals: DSPM, Data Security Platforms, Unstructured Data Management, Data Access Governance
- Named in Gartner's 2025 DLP Market Guide
- Named in Gartner's 2025 AI TRiSM Market Guide
- Represented 30+ times in Gartner's 2025 Hype Cycles for Security, Privacy, AISPM

FREE RISK ASSESSMENT

Discover Your Data & AI Risk

An agentless, cloud-native assessment to enable security, privacy, and compliance: pinpoint where sensitive data and AI risks live - and how to fix them.

What You Get:

- Complementary 2 week engagement on real data to gain visibility on risk across data and AI
- Executive-ready report identifying high-risk data and AI across cloud environments with next-step recommendations

NEXT STEPS

Ready to Connect the Dots in Data & AI?

Schedule your free risk assessment or ask for a deeper demo across DSPM, DLP, AI SPM, Privacy Automation, AI Risk, and Data Lifecycle Management

► www.bigid.com/demo

► www.bigid.com/risk-assessment

► info@bigid.com



BigID Next

"The features they offer are the moat that they have built around the product. This is what makes them the market leader in Data Privacy and Protection."



IT Security & Risk Management Associate - Banking

Gartner
Peer Insights.

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.



BigID Next

"Exceptionally powerful and easy to use tool that integrated smoothly into our environment and delivered value from day one. The BigID team is fabulous to work with."



Senior Vice President & Chief Data Officer - Banking

Gartner
Peer Insights.

Gartner® and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.