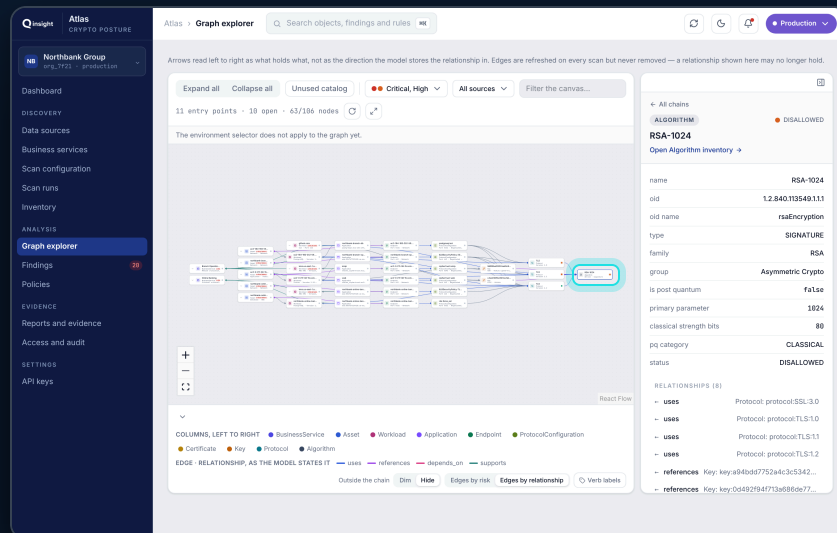


Cryptographic posture management
for quantum readiness

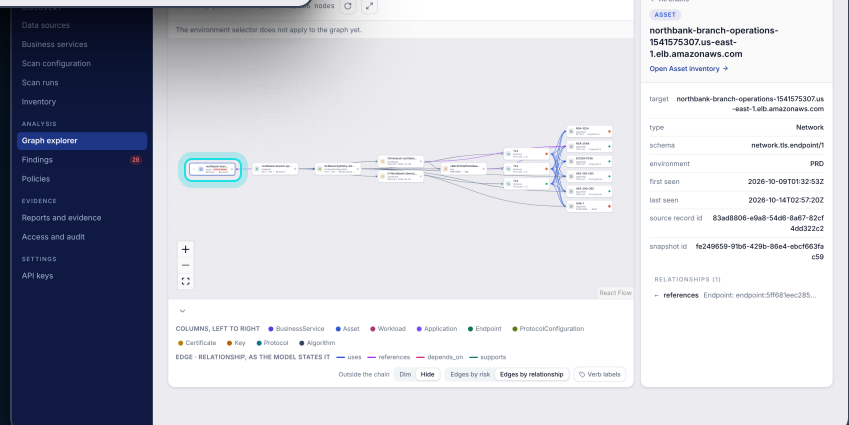
Follow the chain from either end.

Atlas discovers your cryptography, preserves the evidence, and maps the certificates, keys, protocols and algorithms it finds to the applications and business services that depend on them, so you can see the impact of a change before you make it.

Bottom-up



Top-down



Bottom-up

Start from a weak algorithm such as RSA-1024, or from a priority exposure on the dashboard, and see every protocol, endpoint, application and business service that still depends on it.

Top-down

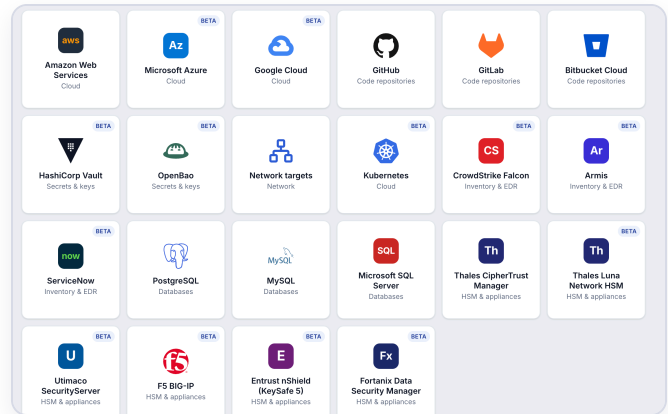
Start from a business service, application or asset and see every certificate, protocol and algorithm it relies on. Disallowed items are flagged.

The CPM workflow | **DISCOVER** → **CORRELATE** → **ANALYZE** → **ACT**

Discovery and inventory

Leverage the tools you already have

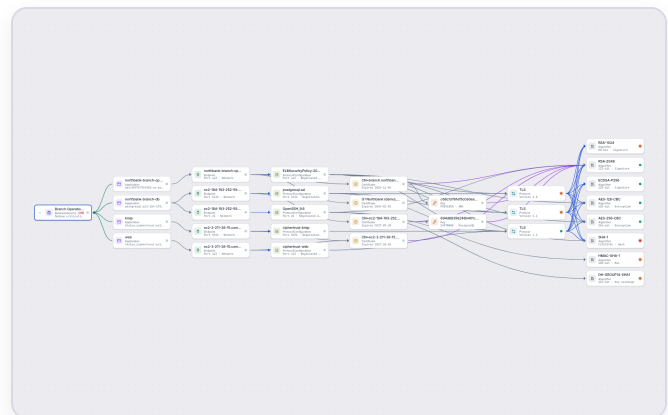
API-based, read-only connections to cloud, code, key stores, HSMs and CMDBs use existing data before deploying agents or sensors; active and passive network discovery covers the rest. Atlas gathers metadata only, on keys, certificates, protocols, protocol configurations, algorithms and libraries: a living CBOM, with evidence import and export including CycloneDX CBOMs.



Correlate and normalize

Map what depends on what

Every observation is normalized into one model and correlated across sources: a certificate, key or algorithm seen by several tools is deduplicated into one object, enriched with CMDB fields such as owner, CI name and system criticality, and mapped to the business services, applications, assets and endpoints that depend on it. That dependency graph is the one on the front.



Policy evaluation and findings

Your policies, your priorities

Every scan is judged against versioned, severity-rated policies, each evaluation pinned to its snapshot. Add policies for your own requirements and prioritization, and apply profiles that surface exposures such as HNDL and compliance needs such as PCI DSS, CNSA 2.0 and DORA. Findings record what was wrong, where, since when and whether it was fixed, with evidence and a read-only API.

Latest evaluation
A snapshot closed · 14 Oct 2026, 03:41 UTC · snapshot r234955, closure 1

[Fail: 7](#) [Pass: 2](#) [View details](#)

[Run all policies](#)

Identifier	Policy	Version	Severity	Status	Latest result
POL-CRY-001	Every algorithm in use carries a governance status An algorithm the catalogue does not know reaches the graph with no status, so nothing can say whether it is acceptable. The first policy RFC-005 recommends: it needs nothing the platform lacks...	1.0	Medium	Active	Pass
POL-CRY-002	No algorithm in use has a proscribed governance status	1.0	High	Active	Fail
POL-TRU-001	Certificates are not signed with a proscribed algorithm	1.0	High	Active	Fail
POL-TRU-002	End-entity certificates are not expired or about to expire An undated certificate is UNKNOWN, never a pass. A null date does not fail a comparison, it fails to match, so treating it as a pass would make silence read as health.	1.0	Medium	Active	Fail
POL-TRU-003	No self-signed end-entity certificate is served in production Scoped to end-entity certificates, because every scan observes a self-signed root and a root is supposed to be one. An endpoint whose environment could not be classified is outside the scope...	1.0	High	Active	Fail
POL-TRU-004	Production certificates are not signed with a proscribed algorithm POL-TRU-001 narrowed to production: only a certificate a production endpoint serves is judged, so a weak signature that lives in staging fails POL-TRU-001 and leaves this one alone. A certificate no...	1.0	High	Active	Pass
POL-PRB-001	Endpoints do not negotiate an obsolete protocol version Read from the protocol configuration the endpoint negotiated, not from what it advertised. Edges are refreshed and never removed, so a stale edge can keep an endpoint failing after it was fixed, an edge...	1.0	High	Active	Fail
POL-PQC-001	Endpoints negotiate a post-quantum key exchange Judged over endpoints that negotiated a protocol configuration; one with none is outside the scope rather than a pass or a fail, since there is nothing to read. A TLS 1.3 endpoint passes when its...	1.0	Medium	Active	Fail
POL-PQC-002	Certificates are not signed with a quantum-vulnerable algorithm A classical signature RSA, ECDSA, Ed25519 can be forged by a quantum adversary. Low severity: almost every certificate fails today, so this measures how far the migration has to go rather than...	1.0	Low	Active	Fail

Remediation

From finding to fix, in one place

Atlas consolidates cryptographic evidence from many tools into a single pane of glass, where crypto debt is found, prioritized and paid down. Ticketing and remediation workflows into ServiceNow are under development, available by year end 2026.

Since the last evaluation	
Opened	Medium 1 1
Reopened	0
Remediated	Medium 1 1
Closed, not remediated	Low 1 1
Across all environments.	
Triage	