cyberhaven + torq

DATASHEET

Automate *Data-Centric* Threat Detection and Response

Turn every sensitive data incident into immediate, orchestrated action.

The Business Challenge

Sensitive data is the target of nearly every modern attack, yet most organizations still cannot see how their data actually moves. Source code, customer records, and IP flow continuously across endpoints, cloud apps, browsers, and GenAI tools, exposing the business to insider risk, IP theft, and accidental leakage.

Traditional DLP relies on static patterns and noisy rules, drowning analysts in false positives while real incidents slip through. By the time a data exposure surfaces, it is often weeks too late.

The Solution

Cyberhaven + Torq makes data security smarter and faster by turning visibility into action. Cyberhaven traces every piece of sensitive data across its full lifecycle, origin, movement, transformation, and destination, detecting insider risk, IP theft, and risky GenAI usage based on behavior and context, not static rules.

Torq takes those high-fidelity findings and automates the next steps by enriching them with user and asset context, opening cases, blocking risky actions, and orchestrating response across the SOC stack while closing the gap between data exposure and containment from days to minutes.

The Value

Incidents arrive enriched with full data lineage, user behavior, and business context. Response flows through the SOC via automated containment, IAM action, or analyst approval. This reduces analyst fatigue, accelerates response, and neutralizes insider and exfiltration risk before sensitive data leaves the business.

CYBERHAVEN + TORQ BENEFITS

Automated Detection to Response
Cyberhaven data incidents flow into Torq workflows, turning every high-fidelity event into instant action.

Context-Rich Decisions
Pull data lineage, user behavior, and asset context from Cyberhaven into Torq to prioritize the highest-risk incidents.

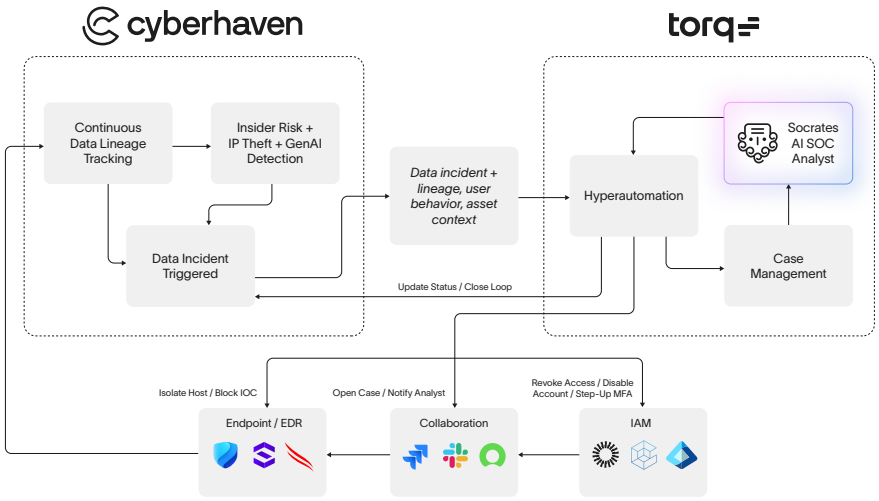
Seamless SOC Integration
Cyberhaven incidents trigger Torq workflows that connect to Case Management, Okta, Entra ID, Slack, or ServiceNow.

Reduced Analyst Fatigue
Torq gathers user, device, and data-movement context automatically, freeing analysts for high-value work.

Closed-Loop Remediation
Torq updates Cyberhaven incident status after action, keeping the data security source of truth in sync with SOC outcomes.

How It Works

Cyberhaven delivers continuous, lineage-based visibility into every sensitive data flow across endpoints, cloud, browsers, and GenAI tools, surfacing insider risk, IP theft, and risky data movement as it happens. When Cyberhaven raises an incident, the event flows into Torq, where Hyperautomation enriches it with user, device, identity, and data-lineage context.



Socrates AI SOC Analyst evaluates the enriched event, correlates it against historical signal, and decides the right path. High-confidence incidents trigger automated containment, blocking the data action, isolating the user through IAM, or notifying owners through collaboration tools.

Once the action is taken, Torq closes the loop by updating Cyberhaven with resolution status so the data security source of truth stays current.

USE CASES

Insider Risk and IP Theft Response

When Cyberhaven detects sensitive data moving to personal accounts, USB, or unsanctioned destinations, Torq enriches with HR and identity context, blocks the action, notifies the manager, and opens a case.

GenAI Data Exposure Containment

When Cyberhaven flags sensitive data flowing into GenAI tools, Torq applies the right policy, blocks or coaches the user, and routes a notification through Slack, preventing IP and customer data leakage at the moment it happens.

Accelerated Data Incident Investigation

Cyberhaven's full data lineage flows into Torq workflows that auto-build the incident timeline, correlate across tools, and surface the highest-risk events to analysts, replacing hours of manual investigation with seconds of context.

About Cyberhaven

Cyberhaven is the leading AI and Data Security platform, protecting sensitive data across its full lifecycle. By tracing every piece of data from origin through every movement and transformation, Cyberhaven detects insider risk, IP theft, and risky GenAI usage based on behavior and context, not static rules.
cyberhaven.com

About Torq

Torq is the AI SOC platform transforming how enterprises manage risk. Using adaptive agentic reasoning and automation, Torq identifies, prioritizes, and remediates critical threats at machine speed. Global leaders like PepsiCo, Siemens, and Virgin Atlantic trust Torq to power AI-driven security operations.
torq.com

Ready to automate your data security response?
Request a demo at cyberhaven.com/demo

Request a demo