code42

5 Ways the Damage from Insider Threats is Hiding in Plain Sight

Data breaches from insider threats have risen 44% from 2000 to 2022 — outpaced only by the rising cost of those threats, which increased 67% to an average of $4.6 million per incident.[1] The rapid expansion of the perimeter-less, cloud-driven, remote-hybrid world of work is driving the insider threat landscape. But perhaps the biggest problem is that the very things that make insider threat appear less threatening than external threats actually make them much harder to detect and remediate.

WHAT YOU MIGHT SEE	WHAT'S HIDING BENEATH

ACTOR

Trusted colleagues

Instead of highly organized and resourced nation state or criminal actors, insider threats come from employees and contractors with shared interests and values.

Authorized access raises no alarms

Inside actors don't have to hack in — they already have the keys to move about without arousing suspicion.

INTENTION

Rarely Malicious

Most employees are genuinely trustworthy and are just trying to work faster and smarter.

Damaging regardless of intent

Exposing IP or sensitive data causes serious damage to the business — regardless of intent.

SPEED & BREADTH

Isolated incidents

Insider threats are typically isolated incidents involving a specific set of files.

Undetected and persistent

Insider threats typically go undetected for months — or years — giving your IP or sensitive data more time to fall into the wrong hands.

INCIDENT RESPONSE

Shared responsibilities

Security teams aren't on their own — HR and Legal play a critical role in response.

Collaborative response depends on full visibility

Security needs to detect the issue and give definitive context to HR and Legal ASAP to enable effective response.

BUSINESS IMPACT

Won't bring business to a halt

There's rarely an urgent race to block insider threats, which require a more nuanced approach to understand the context.

Losing IP = losing competitive advantage

Insider threats target the most valuable information in your business: your IP. Day-to-day business will keep running, but leaked IP can be exponentially more costly in the long run.

Insider Threat Demands Serious Attention — and a New Approach

$15M

The average annual **cost of remediation**

Data exposure & exfiltration events are **outpacing policies + controls**

Understand data exposure by **focusing on the data that matters** and responding confidently.

[1] 2022 Ponemon Cost of Insider Threats Global Report

See the Incydr Approach

Security teams need a new approach that gives you the visibility, context and controls needed to stop valuable data from going to places you don't trust without slowing the business down. **Learn More About Incydr**