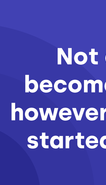
DoControl.

Unmasking Insider Risk

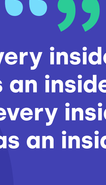
Today's increasingly digital age along with the surge in remote work has created a heightened awareness of insider risks among security and risk management leaders. As more organizations look to cloud technologies and SaaS applications to drive their business and become more agile, they need to ensure they are effectively mitigating the risk of insider threats.

The Cost of Insider Risk



Spent

*On average in 2021 to deal with insider threats.



of Insider Threats

*Involved intellectual property (IP) or data theft.

Increase

*Of insider incidents from 2020 to 2021.

> **Not every insider risk becomes an insider threat; however, every insider threat started as an insider risk.***

Insider Threat Profiles: Hidden in Plain Sight

Accidental Insider

Unknowingly causes harm to the business through carelessness or human error.
Example: A developer mistakenly stores production code in a public repository in GitHub.

Malicious Insider

Abuse of legitimate access to steal sensitive data or sabotage the business.
Example: A disgruntled employee exfiltrates sensitive data by sharing files to their private email account.

Compromised Insider

Access becomes compromised by unauthorized malicious third parties.
Example: An employee falls victim to an email phishing campaign, and the attacker takes over their account and gains an initial foothold on the endpoint.

Mandatory Capabilities of Enterprise Insider Risk Management Platforms*

#1 Orchestration with other cybersecurity tooling (including SOAR)

Sends logs, intervention workflows execution summaries and custom incidents to SIEM (e.g. Datadog sends logs, Datadog creates incident actions); for SOAR the solution ties external remediation paths to DoControl to trigger SOAR playbooks.

#2 Monitoring of employee activity and assimilating into a behavior-based risk model

Aggregates and correlates all SaaS users and activities by leveraging SaaS metadata sources to monitor and control all activities throughout the SaaS estate.

#3 Dashboarding and alerting of high-risk activity

Conducts end-user behavioral analytics to establish a baseline of standard business activity, and automatically notifies security teams of potential insider threats.

#4 Orchestration and initiation of intervention workflow

Security Workflows allow for data access control policies (i.e. intervention workflows) to be applied consistently throughout the environment, preventing the loss, leakage and misuse of sensitive company data.

Request a demo to see how DoControl can help your organization reduce insider risk.

Learn More

*Reference: Gartner's Market Guide for Insider Risk Management Solutions, April 18th 2022, Jonathan Care, Paul Furtado, Brent Predovich