PULSE CODE42

Security Leaders Know Insider Risk is a Major Problem, But Most Aren't Monitoring It

Insider Risk doesn't always come in the shape and size of disgruntled employees. All past and present users with access to company data can present risk—as can data that, if exfiltrated, could harm your company. That's why a holistic Insider Risk program must protect against data security risks that originate from employees and contractors in addition to risks from external attackers.

However, as this Code42 and Pulse survey has found, security leaders and practitioners are conflicted on what Insider Risk truly is—and very few have implemented comprehensive data security programs that check all the boxes.

Data collected from June 26 - July 17, 2020 | Respondents: 100 North American security leaders

75% of companies are aware of Insider Risk, but only react when things go "boom"

Three-quarters of all security leaders admit Insider Risk has been a problem for their organization, including 43% who are at least significantly concerned by the security challenge inside data risks pose.

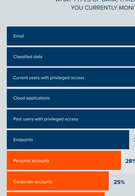
HAVE INSIDER THREATS BEEN AN ISSUE AT YOUR ORGANIZATION?

Despite the majority of respondents agreeing insider threats are a concerning risk, **more than half (51%) said they don't monitor Insider Risk at all.** A further 21% monitor only user behavior, leaving important files, vectors, and applications unmonitored.

DO YOU MONITOR BOTH USER AND DATA THREATS?

While some companies have implemented technologies like user activity monitoring (UAM) and data loss prevention (DLP) to monitor insider threats, **the majority are still reacting once the threat has already occurred.**

HOW DO YOU CURRENTLY MONITOR INSIDER RISK?



Stark contrast: This figure is **26%** lower than the number of respondents who admitted they don't monitor insider threats in the prior question.

NO, WE DON'T MONITOR USERS OR DATA.

"We've deployed a Zero Trust infrastructure with a sophisticated trust engine on the backend. We monitor many factors such as 'impossible travel', employment status, endpoint posturing, data loss prevention, to determine the risk and limit access accordingly."

- A director of security in the software industry

Few security leaders are monitoring data vectors—which present the most Insider Risk to a remote workforce

53% of security leaders don't believe monitoring data, in addition to user behavior, is an important component of a comprehensive Insider Risk security program.

DO YOU AGREE THAT MONITORING DATA (I.E. FILE AND VECTOR ACTIVITY) IN ADDITION TO USER ACTIVITY IS IMPORTANT FOR A HOLISTIC INSIDER RISK SECURITY PROGRAM?

However, this sentiment is contradicted by the Insider Risk factors these companies currently monitor—many of which are data-related.

WHAT TYPES OF DATA, THREAT VECTORS, AND USERS DO YOU CURRENTLY MONITOR FOR INSIDER RISK?

Insider Risk can't stop at endpoints. The data moving across, through, and out of the IT environment contributes most to Insider Risk in today's remote workforce. To distinguish between everyday collaboration and Insider Risk, it's important to monitor file, vector, and user activity, and correlate indicators of risk across these three variables.

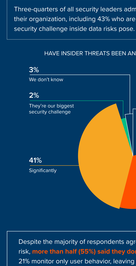
What first comes to mind when security leaders think about Insider Risk? "A tool that monitors and mitigates inside threats as soon as they occur."

- A director of security in the education industry

Not all Insider Risk is malicious—but all threats need a response

66% of security leaders respond to an insider threat by sending the employee an email, and 56% bring the action to the attention of the employee's manager. Only 17% of detected insider threats are brought to the attention of the legal team.

HOW DO YOU CURRENTLY RESPOND TO OR MITIGATE INSIDER THREATS?



For security leaders considering an insider threat security tool, it's most important the software be SaaS-based, detect data exfiltration risks, and is simple to use.

WHAT FEATURES WOULD YOU LOOK FOR IN AN INSIDER RISK SECURITY TOOL?

In a time where collaboration and remote work is the norm, data breaches are happening everyday. Old-school classify and block data loss protection approaches may have worked for compliance, but they're failing to prevent sensitive data from leaving the organization.

Security teams need technology that reduces the noise, recognizes the real risks to sensitive information and provides the much needed context to remediate before any damage is done. They need Insider Risk Detection & Response.

Learn more at Code42.com.

Respondent breakdown

GEOGRAPHY

TITLE

COMPANY SIZE

Insights powered by PULSE