VOLUME II

DATA EXPOSURE REPORT 2021

Cut the Cord: DLP and CASB solutions don't combat today's Insider Risk

Research Conducted by Ponemon Institute for Code42
Published March 2021

CODE42

Ponemon INSTITUTE

Part 1
Introduction

Remote and hybrid work demand technologies that make it easy to collaborate and move files across the organization—exponentially increasing Insider Risk. Security teams' traditional response is to block data movement using conventional Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) tools that are rooted in identify, classify and block tenets known for disrupting employees' legitimate work, but these tools run counter to what business leaders and employees expect. Security leaders know they need a more nuanced strategy than simply looking at good versus bad actions. And they know their teams will never actually reduce risk while living in the forced "maintenance mode" of policy-based tools. A new approach to data protection is long overdue.

The research in The Code42 2021 Data Exposure Report on Insider Risk, Volume II highlights the frustrations security teams face with the industry's inability to mitigate today's growing Insider Risk. It serves as a wakeup call for vendors and organizations to create a more effective, proactive strategy for addressing Insider Risk. To craft this report, Code42 worked with Ponemon Institute in October of 2020 on a survey of U.S.-based IT security leaders and business decision makers. This report represents a deeper dive into the responses provided by existing users of policy-based tools, like DLP and CASB. Over the coming months, Code42 will release additional reports, each diving deeper and revealing insights into specific topics outlined in Volume I.

Executive Summary

The study finds that the data protection problem is getting worse every year despite massive investments in technology and process. Security leaders are frustrated with the industry's inability to address the growing risk proactively and are developing a more nuanced approach to securing data from risks that come from the way employees work today.

DLP is not an effective strategy for stopping Insider Risk and the problem is getting worse.

76%

KEY FINDING:
More than three-quarters of organizations have suffered a data breach despite having a DLP solution in place.

Current Insider Risk strategies do not align with digital transformation and the evolving nature of cloud-based work.

58%

KEY FINDING:
More than half of organizations continue to use a network DLP solution to mitigate Insider Risk despite the acknowledgement that the network perimeter has dissolved amid today's highly-distributed, multi-cloud world.

The failure of policy-based tools is forcing security teams to fly blind in their efforts to combat Insider Risks.

1 IN 2

KEY FINDING:
More than half of security professionals continue to rely on DLP and CASB solutions that do not provide visibility into untrusted destinations such as private email or private cloud environments, even if a network alert is triggered.

Part 2

DLP is not an effective tool for stopping Insider Risk, and the problem is getting worse.

Despite a massive investment in DLP and CASB solutions, organizations around the world continue to be hit with devastating data breach events—and there's no reason to think that current strategies will turn the tide.

6 IN 10

IT security leaders expect Insider Risk to increase significantly in 2021

of respondents said they had suffered one or more data breaches involving the loss or theft of sensitive information in the last year with a DLP solution in place at the time of the event

There's no doubt that massive changes in 2020 are making the enterprise more difficult to secure. Nearly six in 10 (59%) IT security leaders expect Insider Risk to increase significantly in 2021 while their **employees are 85% more likely to leak files today than they were pre-COVID**. Interestingly, the presence of a DLP solution doesn't matter. Employees at organizations with a DLP solution in place are just as likely to exfiltrate data--the increase in both populations is mirrored.

Data around actual insider threat events bear this out. **More than three-quarters (76%) of respondents** said they had suffered one or more data breaches involving the loss or theft of sensitive information in the last year with a DLP solution in place at the time of the event. This is up from **69%** in our 2019 report. The research also shows that organizations are no less likely to suffer a breach with a DLP solution in place, as the general responding population suffered a breach at the same rate as those with a DLP.

It's clear that few people inside the organization—from the security team to line of business leaders—have faith that existing DLP solutions are able to meet today's challenges for mitigating insider Risk.

Part 3

Current Insider Risk strategies do not align with digital transformation and the evolving nature of cloud-based work.

Despite changes in the way we work and access data, organizations continue to rely on outdated, ineffectual network or endpoint DLP solutions that inhibit—rather than enable—employee and security productivity.

Nearly six in ten security professionals use a network DLP to mitigate Insider Risk, but the network has essentially dissolved in today's highly-distributed cloud-based world. For a network DLP to work properly, employees would have to be in the office or connect via VPN. That just isn't a realistic situation today, and there's no reason to think we'll ever go back to "normal" working conditions.

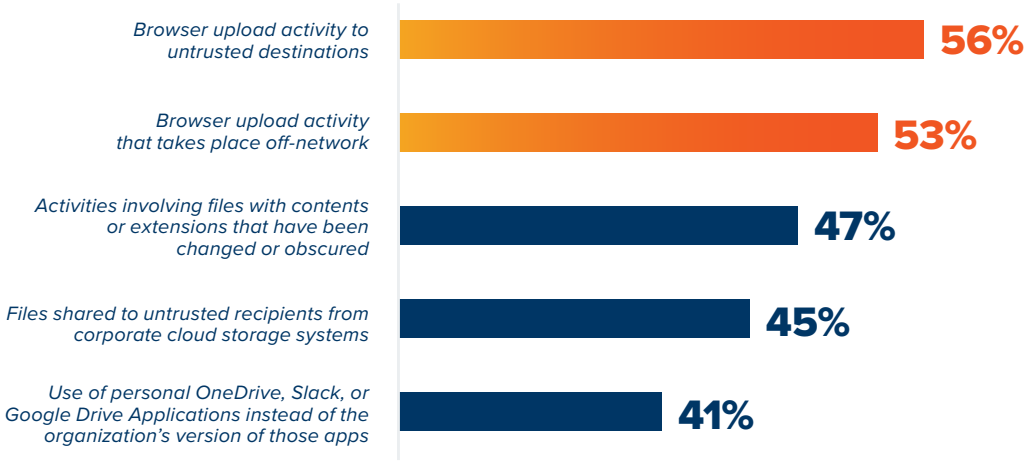
6 IN 10

security professionals rely on a network DLP to mitigate Insider Risk, despite remote work increases and VPN reticence.

A network-based solution just isn't suited for stopping Insider Risk today. According to our survey, 63% of workers use unauthorized applications daily or weekly to share files with colleagues, while **security leaders ranked browser upload activity that takes place off network and browser activity to untrusted domains as their most critical Insider Risk concerns.** Neither would be detected by network DLP solutions.

Most concerning data exfiltration risks

According to security leaders



Even if they did work, DLP solutions do not align with today's collaborative work culture. **Half (51%) of security professionals** receive daily or weekly complaints about IT mistakenly blocking legitimate employee file activity. This can slow critical workflows, pit employees versus security and create a lot of manual work for the team that has to spend time managing policy exceptions.

1 IN 2

security professionals receive daily or weekly complaints about IT mistakenly blocking legitimate employee file activity.

It's not surprising that a Forrester study in 2020 found that **77% of companies have their DLP solutions in monitor-only mode and have not fully deployed the tool.** According to our survey, legacy DLP solutions are difficult to configure and deploy, sap critical resources and expertise and disrupt legitimate work.

of companies have their DLP solutions in monitor-only mode and have not fully deployed the tool.

** Sourced from Forrester Report, Yesterday's Solutions Won't Solve Tomorrow's Data Security Issues, June 2020*

Part 4

The failure of policy-based tools is forcing security teams to fly blind in their efforts to combat Insider Risk.

Security teams using traditional security solutions do not have visibility into the events that lead to data exfiltration—preventing them from understanding the damage already done and from stopping future threats.

It's clear that data exfiltration is happening—and it's happening a lot. In our February 2020 Data Exposure Report, we found that **two-thirds (63%) of employees** who admit to taking data with them to a new job are repeat offenders. This is critical because 59% of departing employees move to a competitor in the same industry.

Serious risks go unnoticed because more than half (55%) of security professionals say they do not have visibility into risky file movement unless a specific event has triggered an alert or rule. This is a big problem. An employee who puts in their two-week notice likely already exfiltrated the data and files they need in their new job before they tendered their resignation, and security teams have no way of knowing the extent to which sensitive information has been compromised. In fact, **72% of the time, security professionals do not have the necessary context to know if they should close or pursue an investigation.**

Part 5
Conclusion

Enterprise security teams know that Insider Risk is a growing problem for their organizations—yet many continue to rely on policy-based tools like DLP and CASB. This severely handicaps security teams—preventing them from mitigating file exposure and exfiltration risks without disrupting employee productivity and collaboration. The problem will continue to frustrate security leaders until they admit that they'll never be able to categorize or predict every data risk.

Recognize the extent of the problem.

The world is changing, and security teams need to adapt to today's challenges while preparing for the future. This requires a new way to assess and prioritize risk, proactively mitigate or manage that risk and secure a new collaboration culture without putting data or the ability of employees to innovate and collaborate at risk.

Find the right tool for the job.

It's clear that existing solutions are not suited for meeting today's data security challenges. Security teams need to identify tools they can put in place to enable business transformation in a cloud-based world.

Put everything in context.

Security leaders need to give their teams modern Insider Risk mitigation tools that allow them to proactively prioritize the riskiest activity, streamline the investigation and response workflows for those risks, and improve risk posture over time.

Part 6
Methodology

The research for this report was conducted by Ponemon Institute. The survey was completed by 623 IT security leaders and 586 business decision makers from the U.S. All respondents were familiar with their organizations' approach to securing sensitive information.

CODE42

About Code42

Code42 is the leader in Insider Risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak and theft as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce Insider Risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's Insider Risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NewView Capital and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com.

Ponemon INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Contact Us

Code42.com

twitter.com/Code42

linkedin.com/company/code-42-software-inc

US: +1 844 333 4242

©2021 Code42 Software, Inc. All rights reserved. Code42 and the Code42 logo are registered trademarks or trademarks of Code42 Software, Inc. in the United States and/or other countries. All other marks are properties of their respective owners.

CODE42

(RP2103248-R8)