The Sensitive Data Report

A Global Survey of Executives, Security, and IT Professionals.

February 2023

dimensional research | Sponsored by: KOLIDE

Introduction

Sensitive data is slipping through the cracks

You might call it an open secret.

In 2023, companies are investing heavily in Zero Trust security to control access to their assets on the cloud. Sophisticated authentication protocols work to keep bad actors from breaking into SaaS applications and accessing the critical data stored there.

But what about when sensitive data leaves the cloud and is downloaded onto employee devices? That's something most companies aren't prepared to address, even though it's happening all the time.

What do we mean by "sensitive data"?

There's no universal definition. Data privacy laws like GDPR and CPRA regulate the personally identifiable information of customers and employees. Many compliance standards emphasize operationally critical data that would impact a business' ability to function. A company might consider anything that could damage its position or help its competitors to be sensitive.

In the real world, all three definitions are valid. Businesses need to protect the employee records maintained by HR, the GitHub credentials the developer uses to access the production environment, and the contracts drawn up by the sales rep.

For the purposes of this study, we're using the broadest definition of sensitive data: any data asset that a company is legally obligated or economically incentivized to protect.

Employees download sensitive data at almost every company

It's important to recognize that **the mere practice of downloading sensitive data is not inherently problematic**.

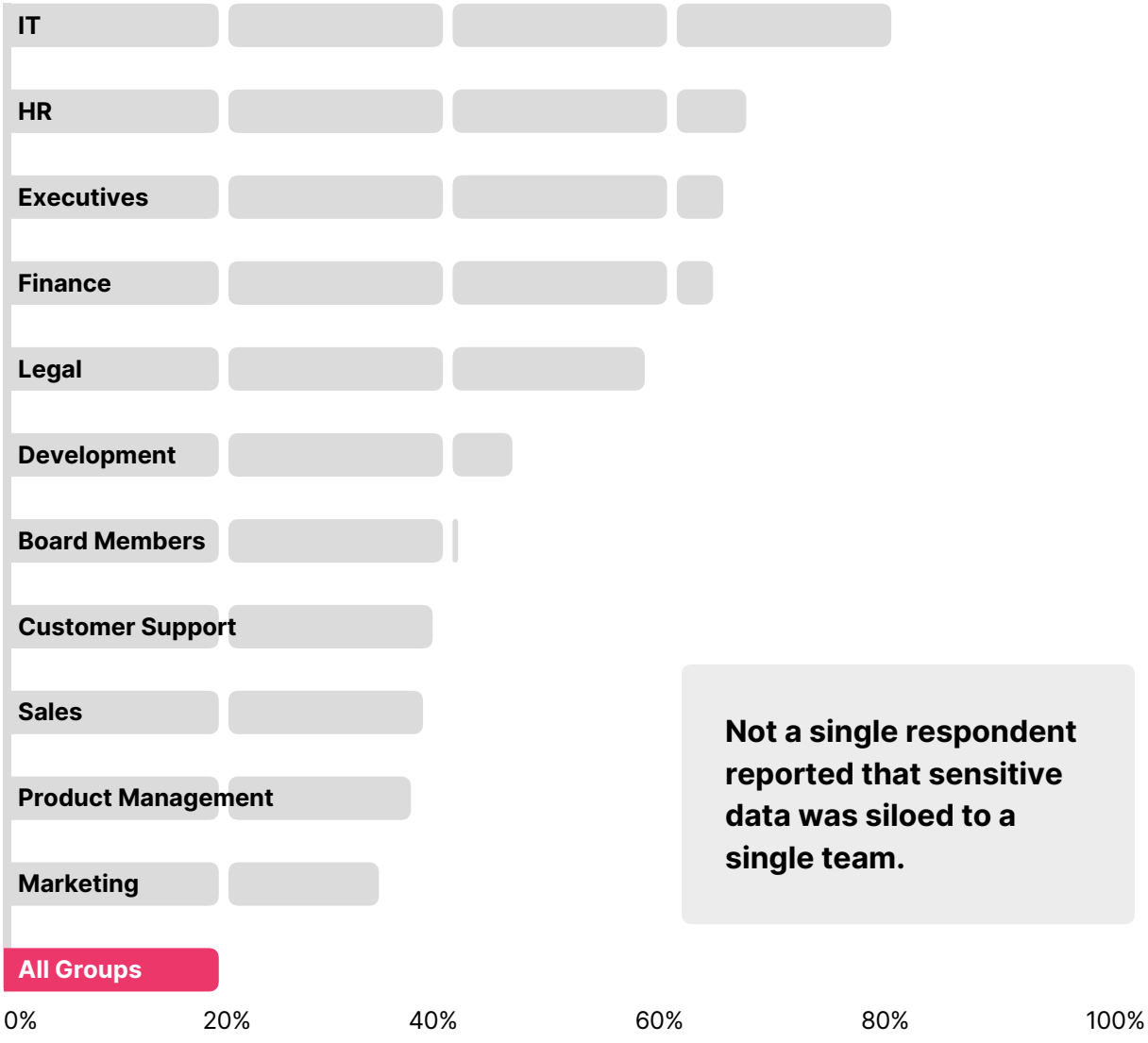
83% of companies have employees who download sensitive company data.

In fact, in most companies, it's not even against the rules. Only 21% of respondents report that their organization prohibits downloading sensitive data. And only 46% report that they prohibit downloads onto personal devices.

This speaks to the fact that employees have valid reasons for downloading data onto their devices. Simply banning downloads (at least onto managed devices) isn't a viable strategy. But it becomes a problem when companies have no visibility into how long sensitive data has been on a device, or whether that device is in compliance with security policies.

Systemic Exposure

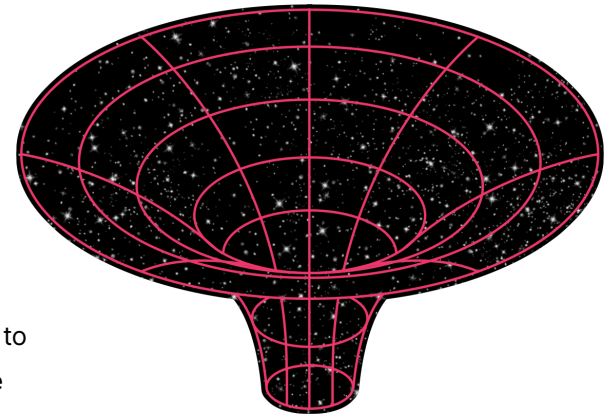
In most companies, multiple teams access sensitive data.
In some companies, **all teams** access sensitive data.



Not a single respondent reported that sensitive data was siloed to a single team.

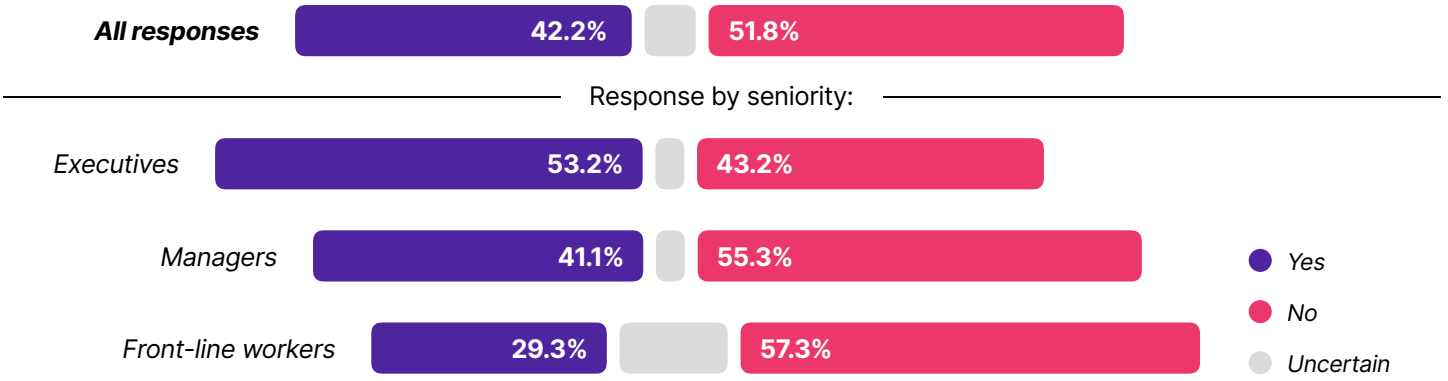
The number of teams with access to data is highly correlated to a company's size. Only 17.8% of companies with under 1000 employees reported that all teams accessed sensitive data, but it was 27.6% for companies with 5-10k employees, and 34.3% in companies with over 10k employees. A large headcount can present data security challenges for both young, rapidly-growing companies, and for established enterprises saddled with legacy technology and policies.

Once sensitive data is downloaded, it might as well be in a black hole



Fewer than half (42%) of the companies we surveyed have a solution to proactively locate sensitive data on an employee device, meaning the majority have little idea where data is and who has it.

"We can detect sensitive data on employee devices."



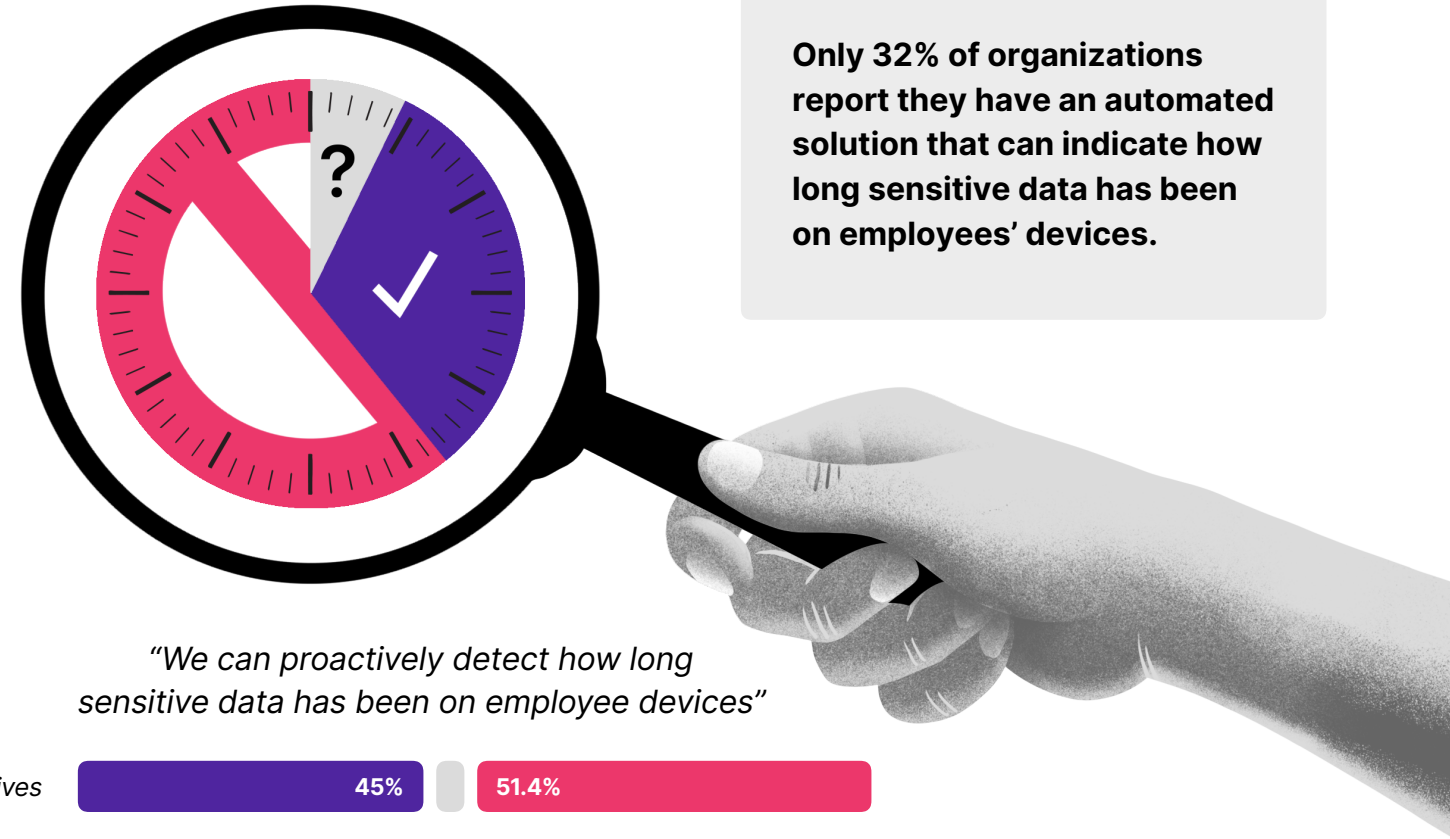
Estimates vary wildly with seniority:

But even 42% might be a generous estimate, since a company's capabilities for detecting sensitive data vary a lot depending on who you ask. In our survey, 45% of executives said they could locate sensitive data, compared to 29.1% of managers, and only 18.3% of front-line workers.

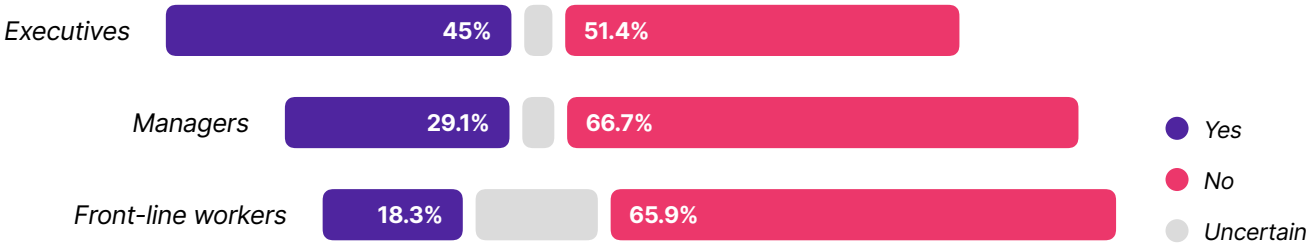
The view from the C-suite vs. the ground

One of the strongest trends we found is that the farther down you go in the org chart, the more pessimistic (or realistic) the answers become about how well the company can monitor sensitive data.

Only 32% of organizations report they have an automated solution that can indicate how long sensitive data has been on employees' devices.



"We can proactively detect how long sensitive data has been on employee devices"



Further examples of this trend:

• When asked if devices in violation of sensitive data policies would automatically be prevented from accessing sensitive data, 45% of executives said yes, compared with 37.9% of managers, and 26% of front-line workers.

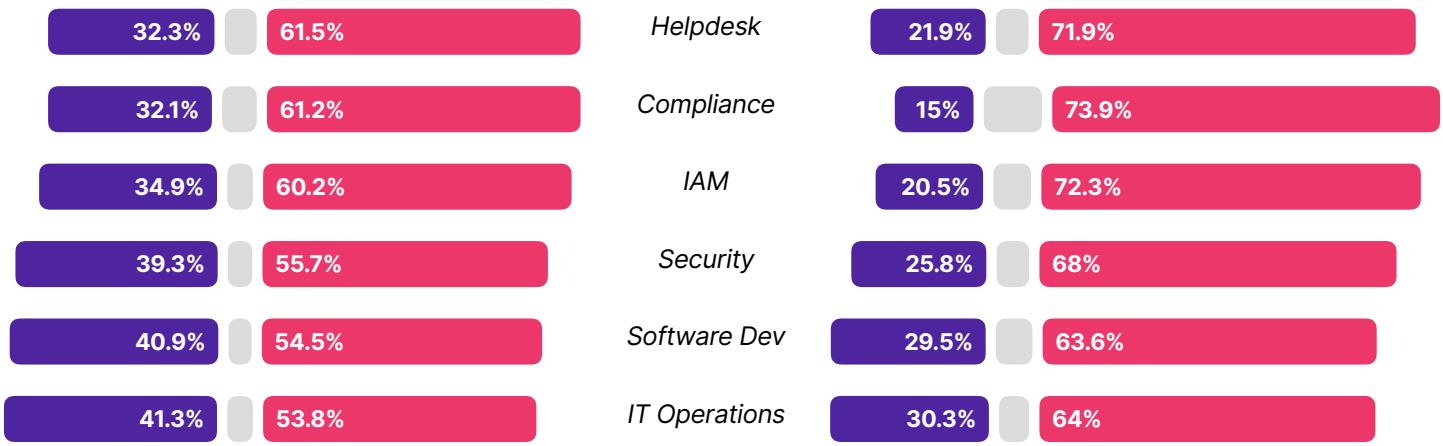
• When asked if their organization had a solution that could automatically inform employees when they violated sensitive data policies, 57.3% of executives said yes, compared to 44.9% of managers, and 33.3% of front-line workers.

Assessments vary by role as well as seniority

In particular, respondents involved with helpdesk, compliance, and identity and access management (IAM) tend to offer the darkest assessments.

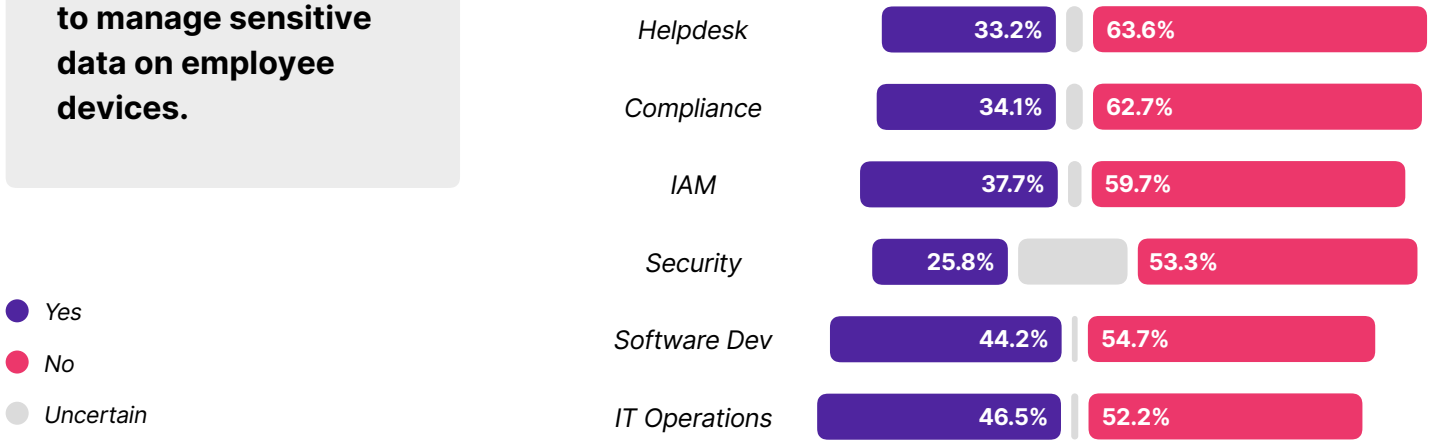
*Does your organization have a solution that can **proactively locate** your company's sensitive data on employee's devices?*

*Does your organization have an automated solution that can **indicate how long** sensitive data has been on employees' devices?*



Workers who interact with end users report not having the means to manage sensitive data on employee devices.

*Does your organization have an automated solution that specifically **detects if** any of your company's **policies** for handling sensitive data **are being violated**?*



Employees are fallible but trying their best

Across the board, most respondents agreed that end users try to obey policies, even though they make mistakes. After that, answers were nearly evenly split between "employees are ignorant of policies" and "employees knowingly violate policies." (9% answered that their employees always follow sensitive data policies, which is, for lack of a better word, *sweet*.)

8.9% *Employees always follow sensitive data policies.*

52.1% *Employees are aware of and try to follow our policies but inadvertently break them.*

19.5% *Employees are generally ignorant of our policies and act based on what they think is "safe".*

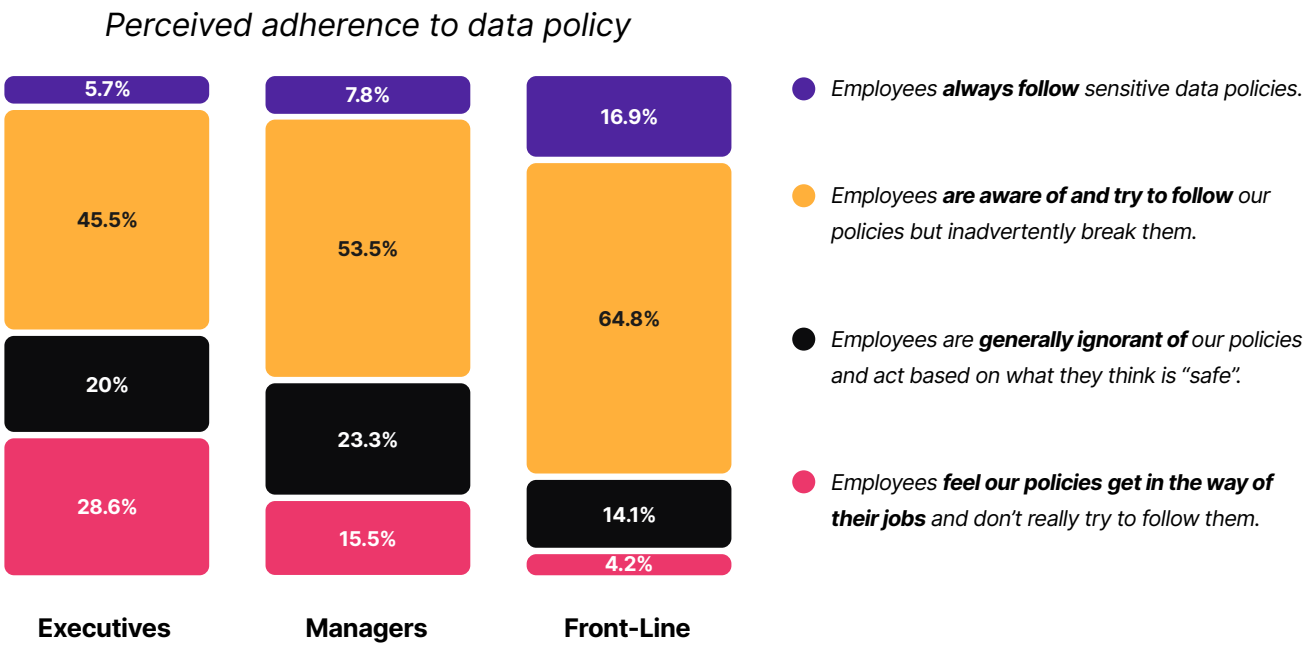
16.9% *Employees feel our policies get in the way of their jobs and don't really try to follow them.*

2.6% *Prefer not to say.*

Executives are suspicious of workers

But executives, who were so confident in their technological capabilities, had the poorest opinions of their employees. 28% of executives claimed their workers didn't really try to follow policies.

Only 16% of managers and 4% of front-line workers took this dim view.



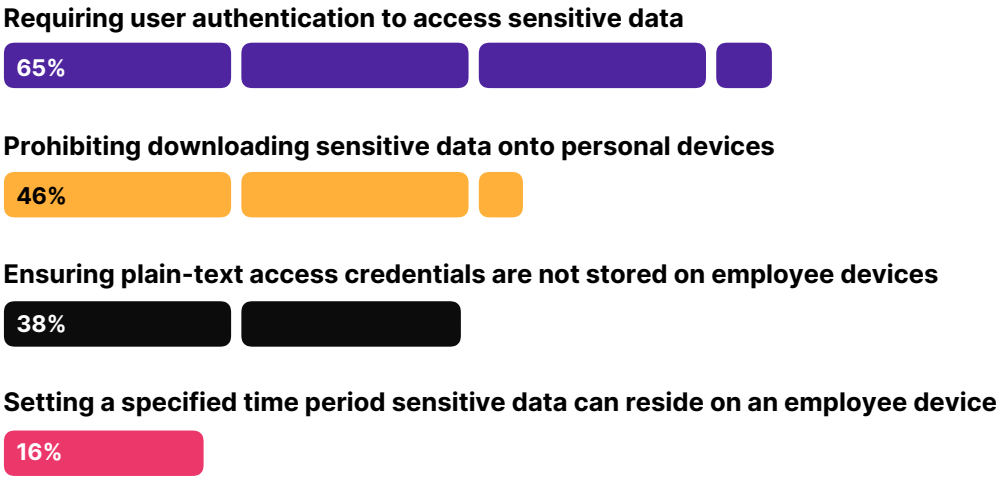
This was one of the survey's most dramatic and surprising findings.

It may indicate that executives have been sold on a version of Zero Trust security that overemphasizes the danger of malicious insider threats (as opposed to human error), and which relies on surveillance and punitive measures to police employees.

Sensitive data policies lean on authentication, but ignore devices

When we asked respondents about the policies they have in place to protect data, it became clear that authentication was the low-hanging fruit, while everything else was out of reach.

Which of the following policies for handling sensitive data have been established at your company?



In another question about authentication, 70% reported that they used a single sign-on (SSO) solution to manage access to all or some applications that manage sensitive data.

But while access to cloud apps is under control, it's a different story once data is on an employee device. Even though 46% report that they have a policy prohibiting employees from downloading data onto their personal devices, only 34% report they can track violations of that policy with an automated solution. This gap in device security undermines the entire system, since even cloud apps aren't safe if plain-text access credentials are sitting on employee devices.

The majority of companies surveyed don't employ practical sensitive data policies and 84% allow sensitive data to reside on employee devices forever.

Conclusion

This research reveals major disconnects between the people who set a company's compliance and security policies and the people responsible for implementing them.

So who's right? Execs or front-line workers?

The data can't answer that question, and in reality, there is no universal answer. However, we can draw two conclusions with confidence:

1. More communication is needed between executives and front-line IT/helpdesk/compliance workers, and between these teams and the workforce at large.

Open dialogue is the only way to establish an accurate picture of an organization's security posture and clear up the confusion between groups. This conclusion holds true whether you believe an organization's tools aren't capable of protecting sensitive data, or that they're merely being misused. All parties, including end users, need a clear understanding of what policies exist and how they're being enforced. In cases where employees aren't complying with sensitive data policies, leaders should be asking "why?" before assigning blame and issuing punitive policies.

2. Organizations need to establish better policies regarding sensitive data and invest in tools to enforce them.

Even if you believe the C-Suite's optimistic assessment of security, the results of this research are sobering. To recap: only one-fifth of companies (21%) even have a policy about how long sensitive data can remain on an employee's device. And more than half (53%) can't prevent employees in violation of policies from accessing more sensitive data. To be clear, employees don't usually download sensitive data out of recklessness or malice—they're just trying to do their jobs. But they make human mistakes, and most organizations have no effective way to account for this inevitable fact.

We'll close by saying that companies can't really be blamed for these shortcomings. Historically, there haven't been tools that could automatically identify violations related to sensitive data retention or enforce them by communicating directly with end users.

As you might have guessed, **that's what we're trying to change**.

Methodology

Who we surveyed

Below is a detailed breakdown of survey participant's various demographic information.

Total participants: 344

Participants by industry

Technology (software)	25%
Financial Services	11%
Education	9%
Manufacturing	8%
Services	7%
Government	7%
Healthcare	6%
Technology (other)	5%
Telecommunications	3%
Retail	3%
Non-Profit	3%
Other	2%
Transportation	2%
Energy & Utilities	2%
Food & Beverage	2%
Pharmaceutical	1%
Hospitality & Entertainment	1%
Media & Advertising	1%
Insurance	1%
Life Sciences	1%

Participants by job duties

IT Operations	79%
Security	73%
Identity and Access Management	50%
Compliance	40%
Helpdesk	29%
Software Development	26%

Participants by company size

50-1000 Employees	60.5%
1,000-5,000 Employees	20.4%
5,000-10,000 Employees	8.7%
> 10,000 Employees	10.5%

Participants by location

US or Canada	71%
Europe	17%
Asia	5%
Oceania	3%
Mexico, Central & South America	2%
Middle East and Africa	2%

Participants by seniority

Executives	33.2%
Managers	42.2%
Front-Line Workers	24.6%

KOLIDE

About Kolide

Kolide is a device security and compliance company that **believes two things:**

1. Organizations have the right and obligation to protect their sensitive data and assets.

2. Employees need to have agency over their devices in order to do their jobs effectively.

Kolide's cross-platform solution reconciles these two ideas–it helps IT and security teams achieve total compliance, and it does so by working *with* end users.

The premise is simple: **if an employee's device is out of compliance, it can't access your apps.**

With Kolide, organizations can set and enforce policies across their fleet, and solve problems that are beyond the capabilities of MDM or SSO solutions.

Kolide's automated tool lets admins:

- Enforce OS and browser updates so vulnerable devices aren't accessing data
- Run queries to detect sensitive data
- Flag devices that have violated sensitive data policies–whether by leaving data unencrypted, keeping it too long, or downloading data they shouldn't have
- Draw from Kolide's library of Checks or build their own
- Do a lot of other cool things that won't fit on this page

Kolide makes device compliance part of the authentication process. Our tool notifies users about compliance issues when they log into their cloud apps and blocks unsecure devices from logging in. But instead of sending users to IT, Kolide educates them and provides remediation instructions, so they can get their device secure and continue logging in. This unique approach decreases the need for intrusive tools, reduces IT workload, and enables organizations to solve previously unsolvable compliance issues. It's time to replace open secrets with Honest Security.

To learn more visit: kolide.com