Enterprise Strategy Group™
by TechTarget

The State of Data Loss Prevention

Current Struggles and Future Expectations

Research by Enterprise Strategy Group, commissioned by MIND
and distributed under license from TechTarget, Inc.

Research Objectives

Enterprises need data loss prevention (DLP) solutions to secure sensitive information from unauthorized access, leakage, and theft. DLP solutions are essential for enabling productivity and innovation with appropriate security guardrails, safeguarding intellectual property, preserving customer trust, and meeting regulatory compliance obligations. DLP technology is widely deployed, but enterprises have faced ongoing struggles in deploying, evolving, and maintaining DLP solutions. Enterprise environments are more complex, and data stores are growing. Maintaining and evolving DLP rules, as well as wading through the significant false-positive alerts generated by existing solutions, are a few of the struggles facing enterprise security teams today.

To gain further insight into these trends, TechTarget's Enterprise Strategy Group surveyed 100 senior cybersecurity and IT decision-makers at organizations in the United States who are involved with or responsible for their organization's deployed DLP technologies.

This study sought to:

Assess the volume and growth of data that enterprises need to secure.

Explore attributes or features that are most important for solving enterprise DLP challenges.

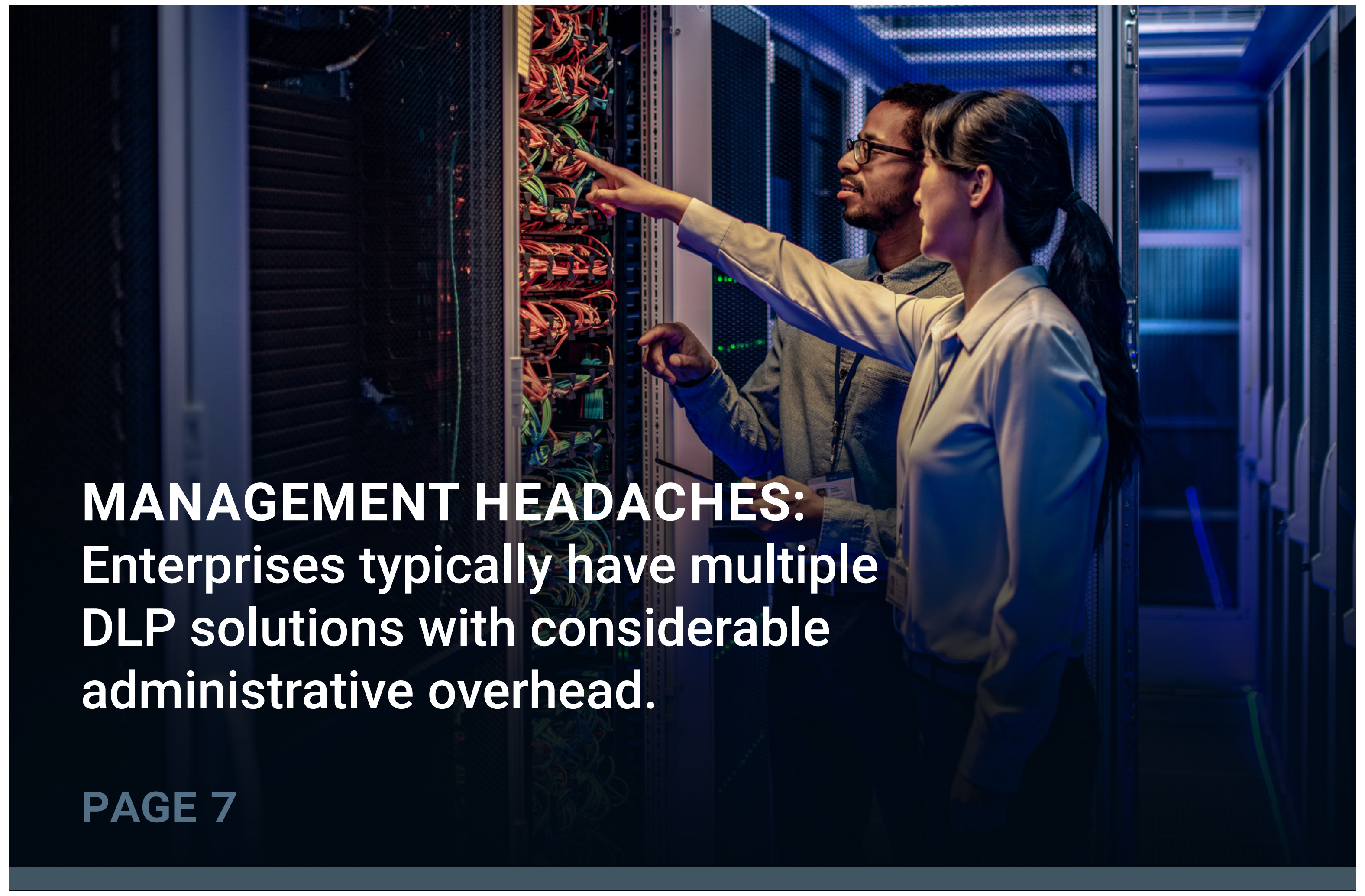
Understand the satisfaction and dissatisfaction with existing approaches to DLP.

Determine future requirements and plans to secure sensitive information against data loss.

Key Findings

DATA EXPLOSION:
Sensitive data lives everywhere, both on premises and in the cloud, with proliferating data sources.

PAGE 4



MANAGEMENT HEADACHES:
Enterprises typically have multiple DLP solutions with considerable administrative overhead.

PAGE 7

DATA LEAKS CONTINUE:
Data losses are still pervasive and have widespread impact.

PAGE 11

DLP INNOVATION OPPORTUNITIES:
Top DLP priorities are reducing alert noise, gaining context awareness, and determining risk severity.

PAGE 14

INTENTIONS AND PLANS:
Enterprises are primed to adopt innovations that streamline workflows, overcome alert noise, and remediate incidents.

PAGE 18

BACK TO CONTENTS

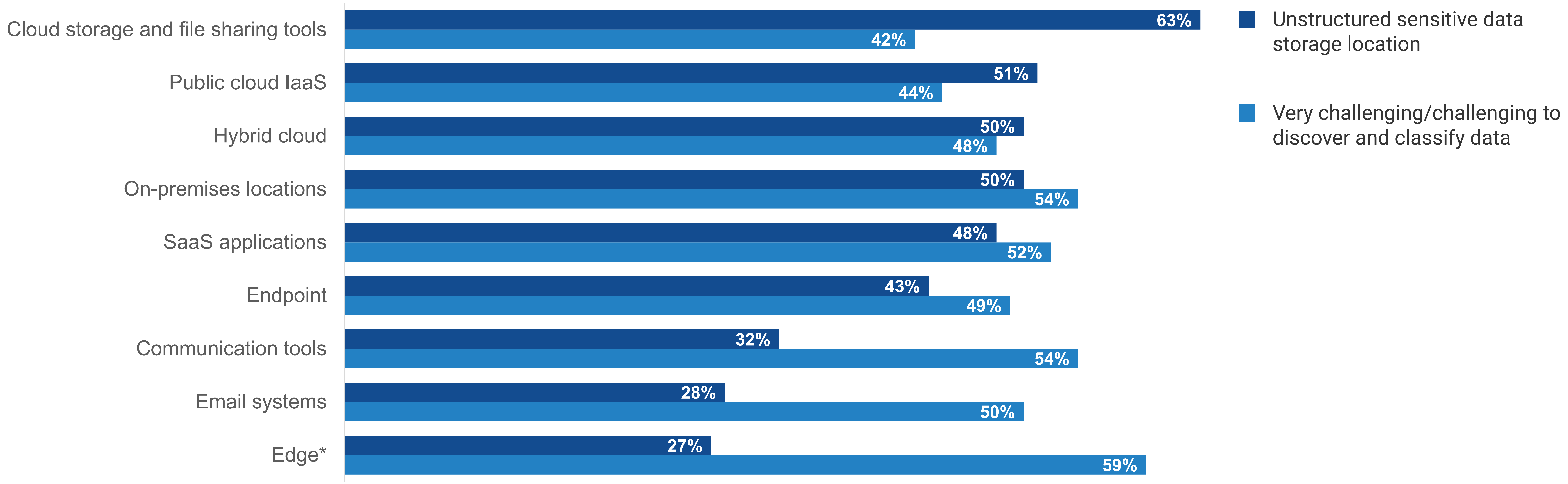
DATA EXPLOSION:

Sensitive data lives everywhere, both on premises and in the cloud, with proliferating data sources.

Sensitive Data Lives Everywhere, and Half Say It’s Challenging to Discover and Classify

While sensitive data is distributed throughout an enterprise, organizations store a disproportionate amount of unstructured sensitive data in cloud storage.

Where Unstructured Sensitive Data Resides



*Directional data (N size is 27)

Less than half (46%) of **unstructured sensitive data has been discovered**, and less than two-thirds (58%) of **discovered unstructured sensitive data has been classified.**

Organizations Struggle to Discover and Classify Unstructured Sensitive Data

Unstructured sensitive data is expected to grow 45% annually (doubling every 2.2 years).

Only 26.7% of unstructured sensitive data has been both discovered and classified.

Discovery and Classification of Unstructured Sensitive Data

46%
Percentage of unstructured sensitive data that has been *discovered.*

58%
Percentage of discovered unstructured sensitive data that has been *classified.*

26.7%
Percentage of unstructured sensitive data that has been discovered and classified.

BACK TO CONTENTS

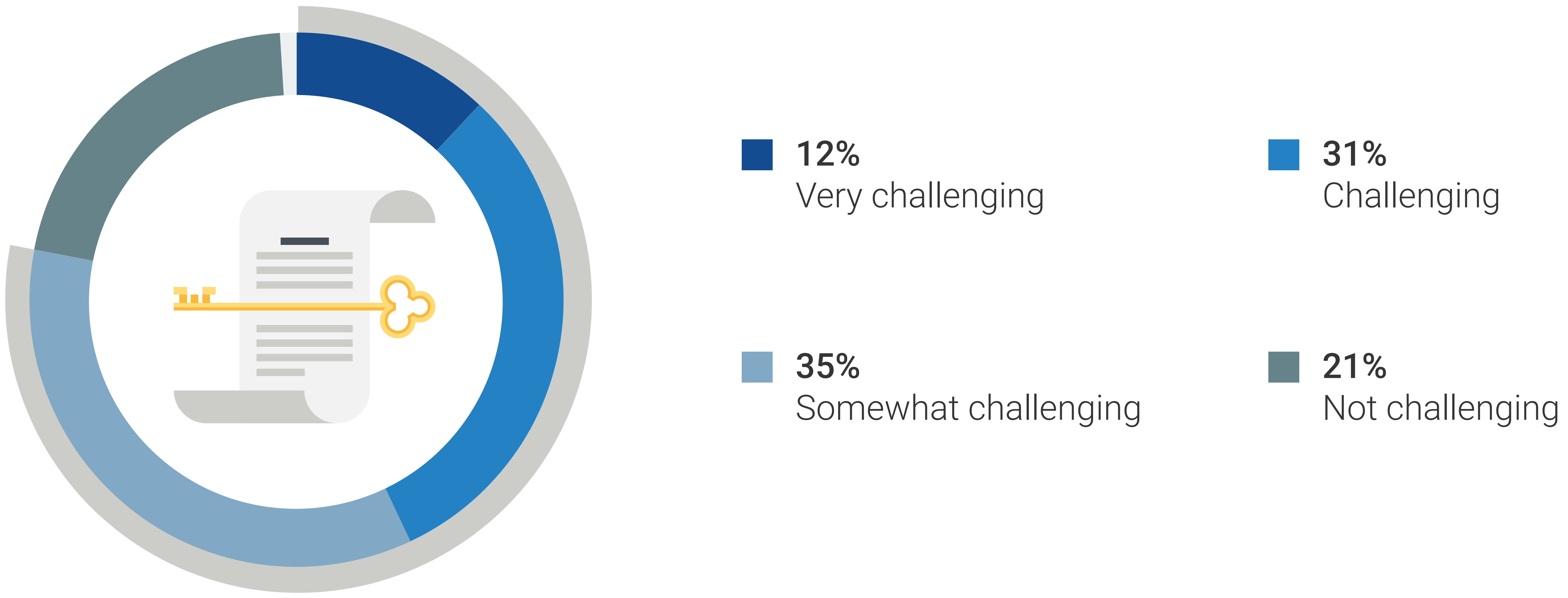
MANAGEMENT HEADACHES:

Enterprises typically have multiple DLP solutions with considerable administrative overhead.

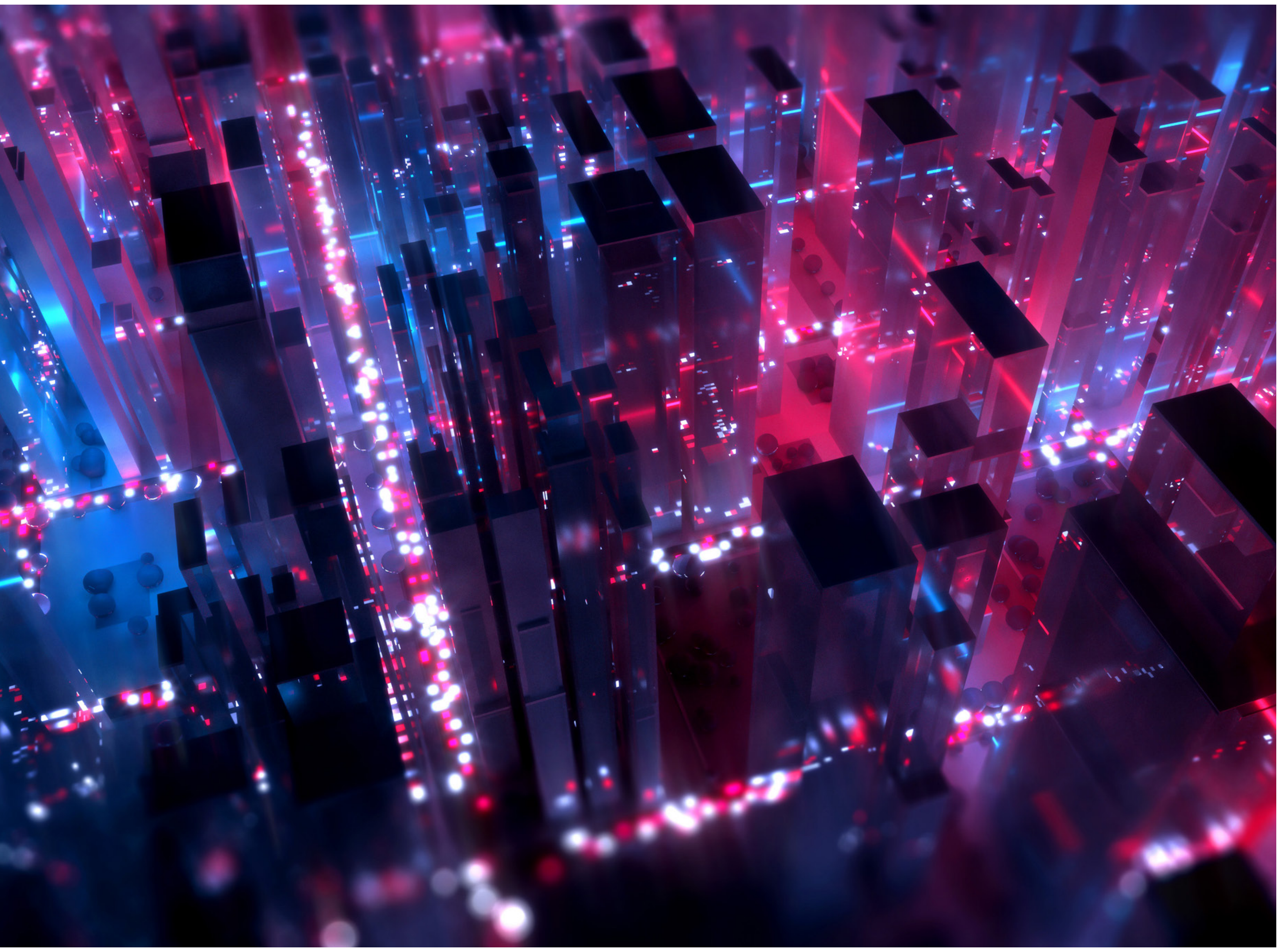
Administering and Maintaining Existing DLP Technology Solutions and Policies Is Challenging for Most Organizations

DLP consumes considerable security resources while data continues to leak. Practitioners are not satisfied with existing approaches to solving the DLP challenge.

Views on Administrating and Maintaining Existing DLP Technology Solutions and Policies



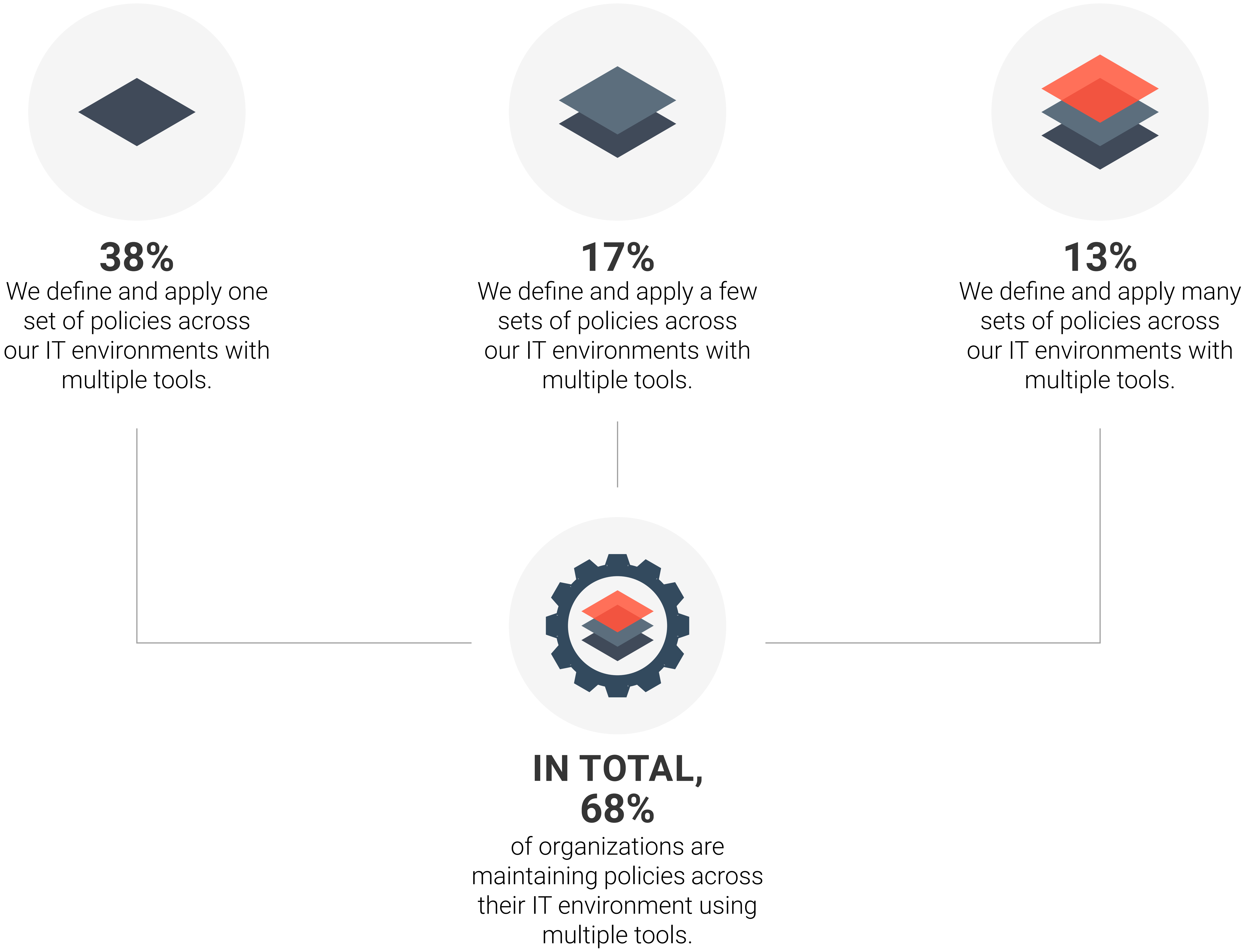
78% of organizations indicated that it is **challenging to administer and maintain existing DLP technology solutions and policies.**



Organizations Have a Variety of Approaches to DLP Policies, With a Plurality Having One Set of Policies Deployed Using Multiple Tools

Overall, 94% of organizations use 2 or more tools with DLP capabilities. On average, organizations are using 3.3 tools with DLP capabilities. While many tools include DLP functionality, multiple tools can result in swiveling between consoles to administer and maintain different solutions.

Description of DLP Policies Deployed Across IT Environments



38%
We define and apply one set of policies across our IT environments with multiple tools.

17%
We define and apply a few sets of policies across our IT environments with multiple tools.

13%
We define and apply many sets of policies across our IT environments with multiple tools.

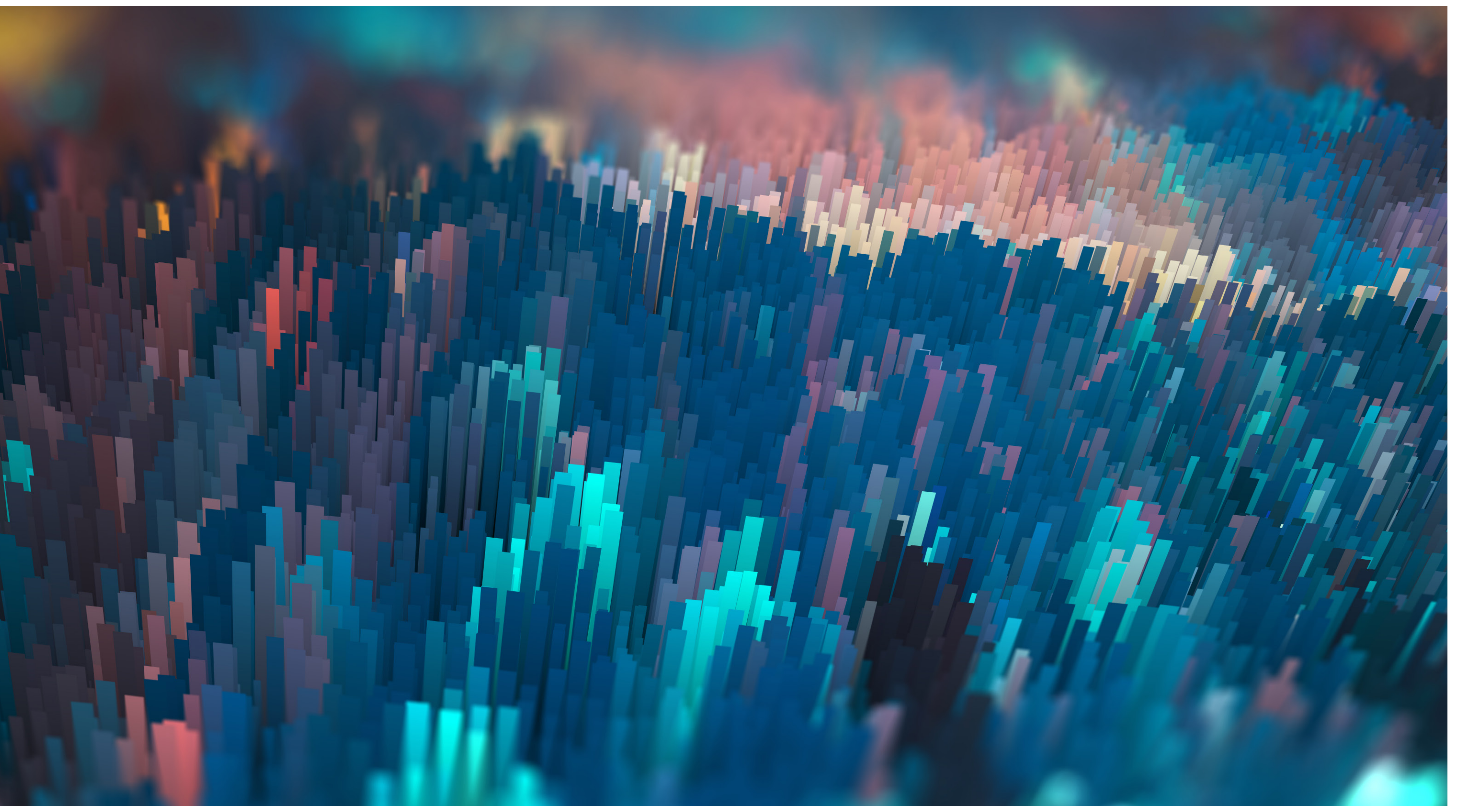
IN TOTAL, 68%
of organizations are maintaining policies across their IT environment using multiple tools.

BACK TO CONTENTS

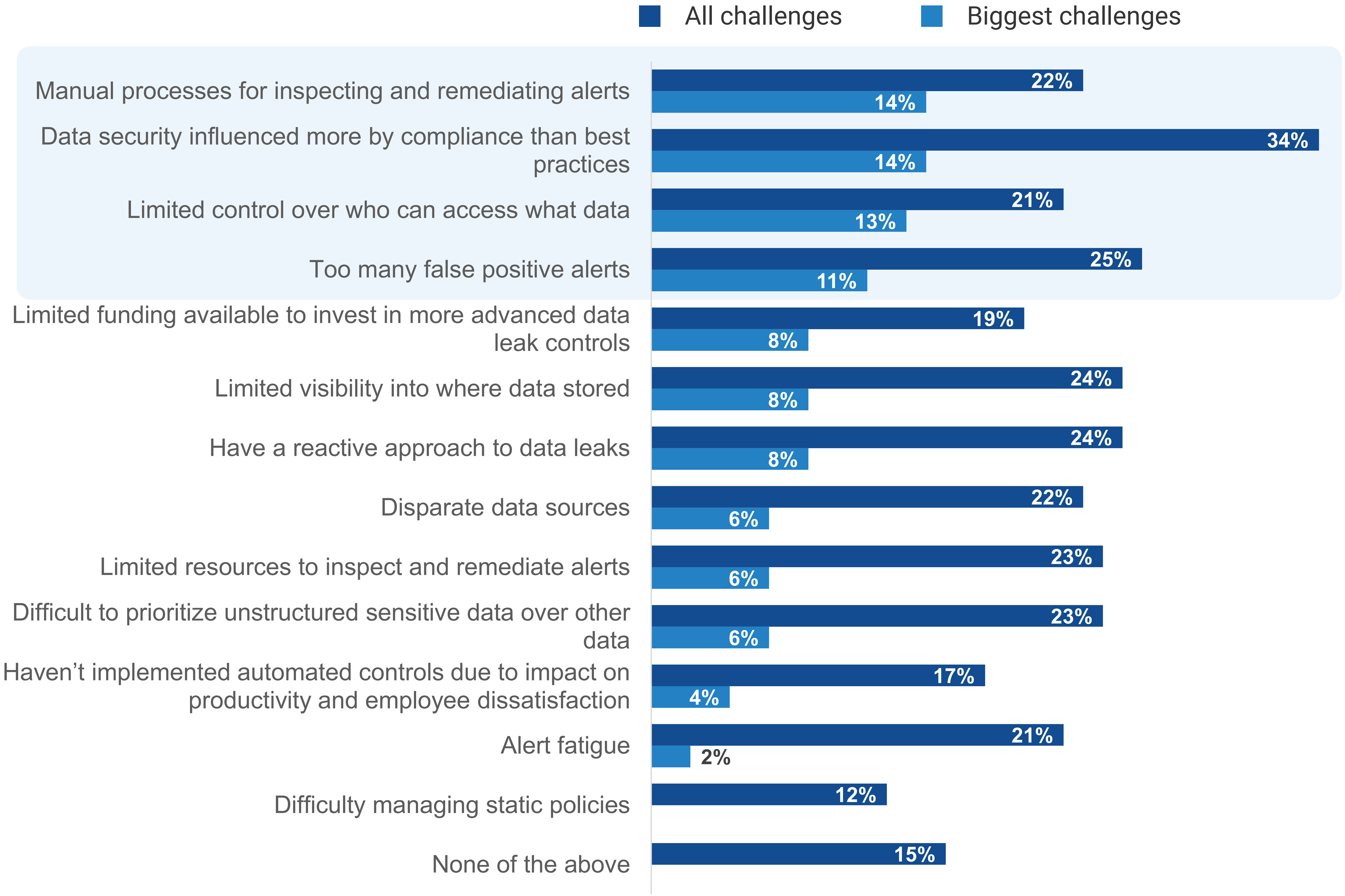
DLP Challenges: Process, Tick Box Compliance, and Lack of Control Are Biggest Pain Points

DLP is difficult to operate, creates volumes of false positives, and requires considerable manual work. It frequently becomes a compliance exercise rather than improving security. There is an opportunity to flip that script.

Most of the security team challenges can be addressed by improved DLP technology, possibly in conjunction with adjacent technology (i.e., data security posture management).



Challenges Organization Have Experienced With Controls in Place for Preventing Data Loss



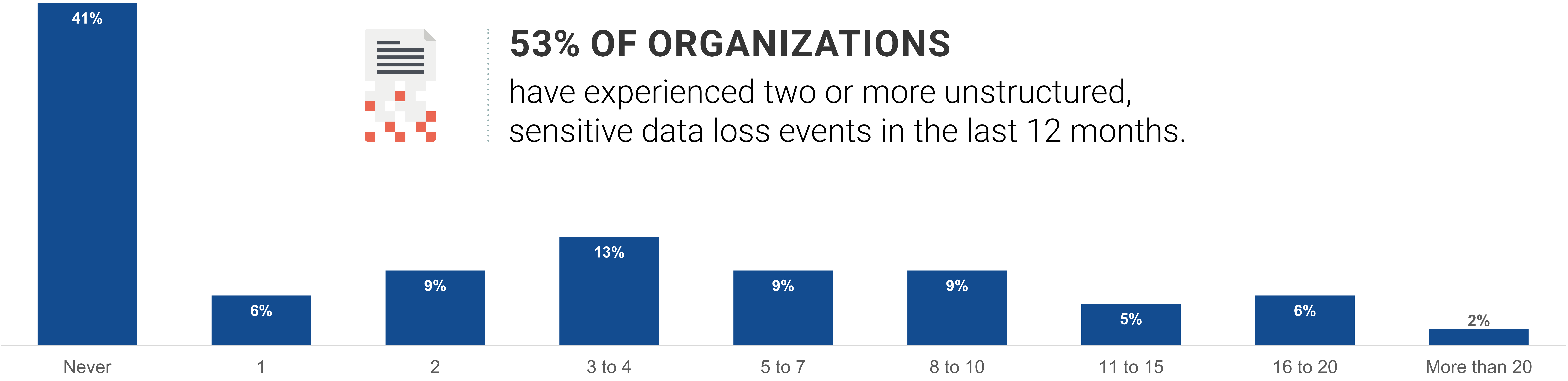
DATA LEAKS CONTINUE:

Data losses are still pervasive and have widespread impact.

Data Loss Is Pervasive: On Average, Organizations Have Experienced 4.2 Unstructured, Sensitive Data Loss Events Over the Past 12 Months

Over half of organizations (53%) have experienced two or more unstructured, sensitive data loss events in the last 12 months. Data loss occurs despite practically all organizations having multiple tools, consistent policies, and strong solution integration and security visibility.

Unstructured Sensitive Data Loss Events Experienced by Organizations Over the Past 12 Months



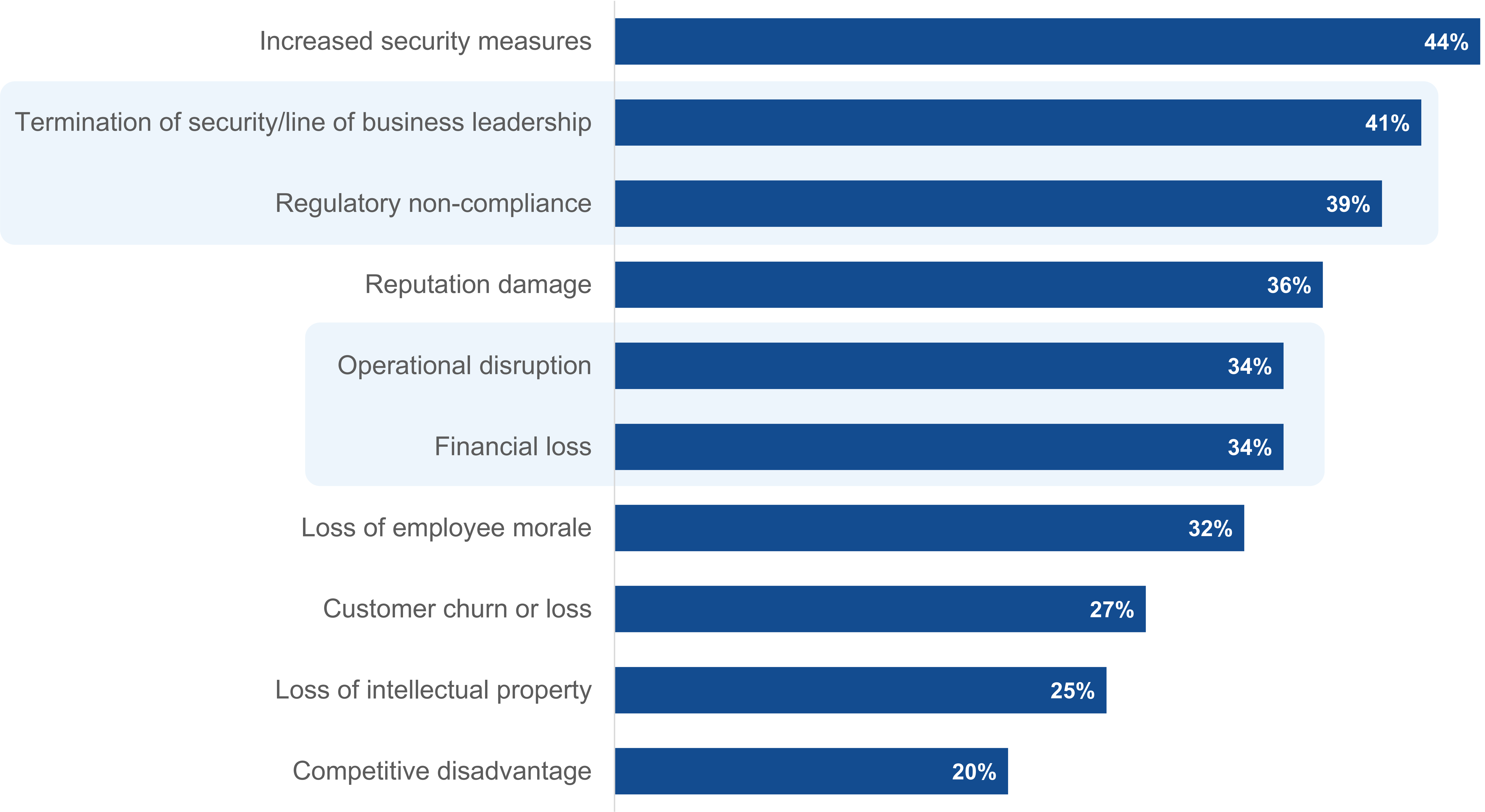
53% OF ORGANIZATIONS

have experienced two or more unstructured, sensitive data loss events in the last 12 months.

Business Impact of an Unstructured Data Loss Event Is Widespread

As security requirements become more stringent, executive heads may roll following a data loss event. Top business impact concerns also include regulatory fines and reputational damage.

Business Impact of Unstructured Sensitive Data Loss Event



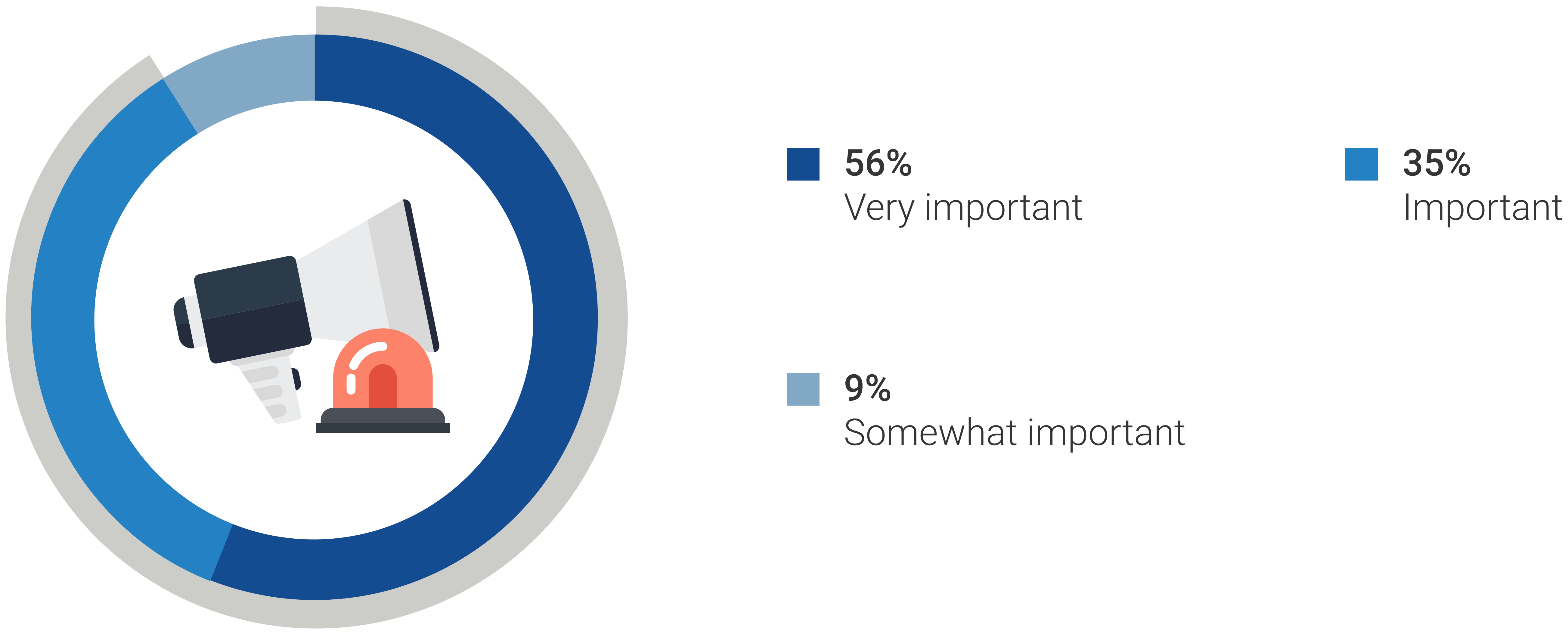
DLP INNOVATION OPPORTUNITIES:

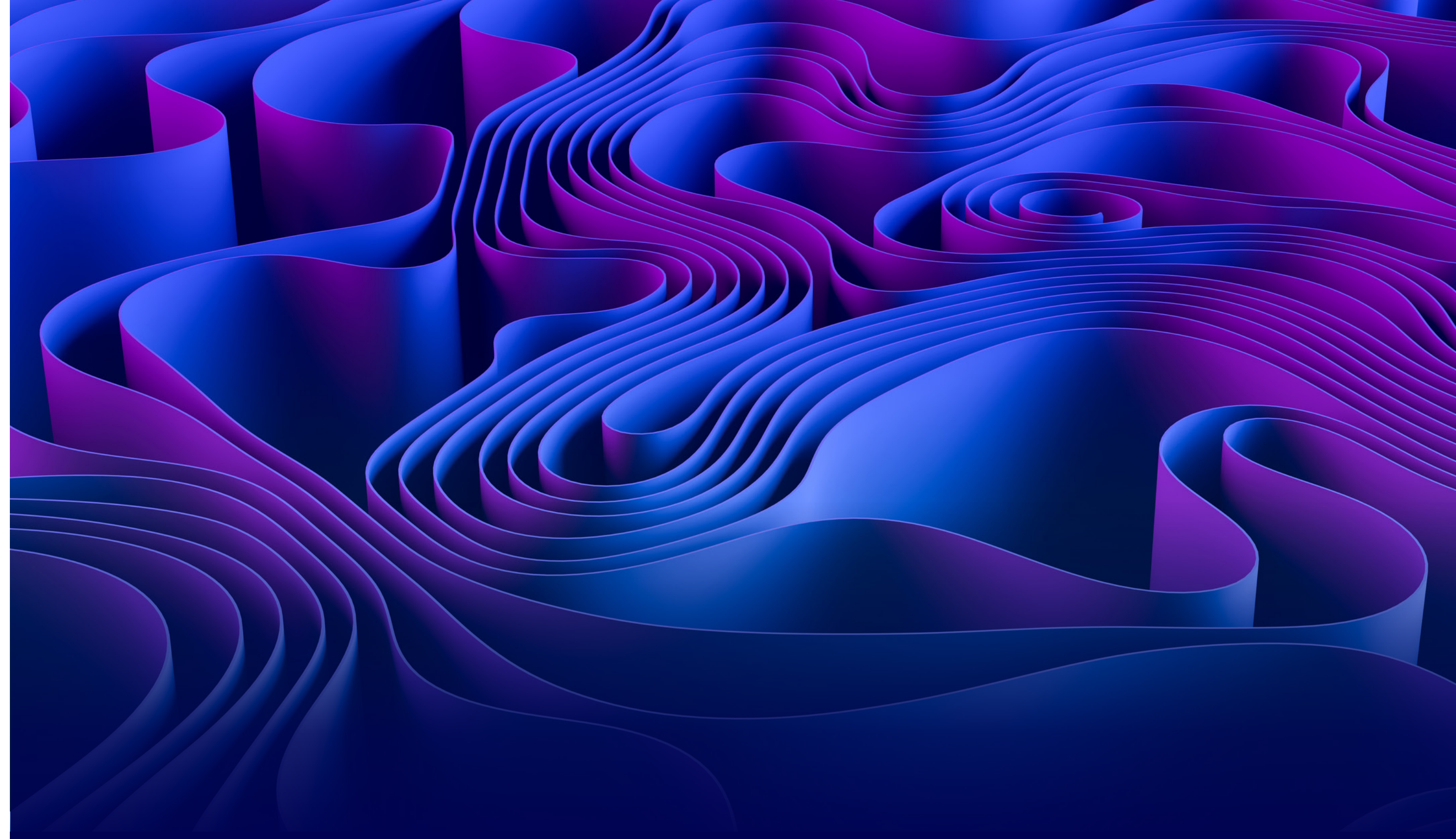
Top DLP priorities are reducing alert noise, gaining context awareness, and determining risk severity.

A Top Priority: Reducing Alert Noise Pollution

Almost all organizations said it is important to reduce alert noise produced from their current DLP controls. Reducing alert noise improves security while enabling practitioners to focus on what matters, be more productive, and enjoy better job satisfaction.

Importance of Reducing DLP Alert Noise





91%

of organizations said it is important to **reduce alert noise produced from their current DLP controls.**

DLP Is Noisy and Wastes Time: Understanding the Math

Of the total number of DLP alerts that are generated, 8% are remediated, non-false-positive DLP alerts. 92% of alerts are either deferred/left for inspection after 24 hours or are false positives/not remediated.

DLP Alerts (Averages)

65%

of DLP alerts are inspected within 24 hours.

For example: If 100 DLP alerts are generated, 65 (65%) are inspected within 24 hours.

60%

of the inspected DLP alerts are remediated.

For example: Of the 65 DLP alerts that are inspected within 24 hours, 39 (60%) are remediated.

47%

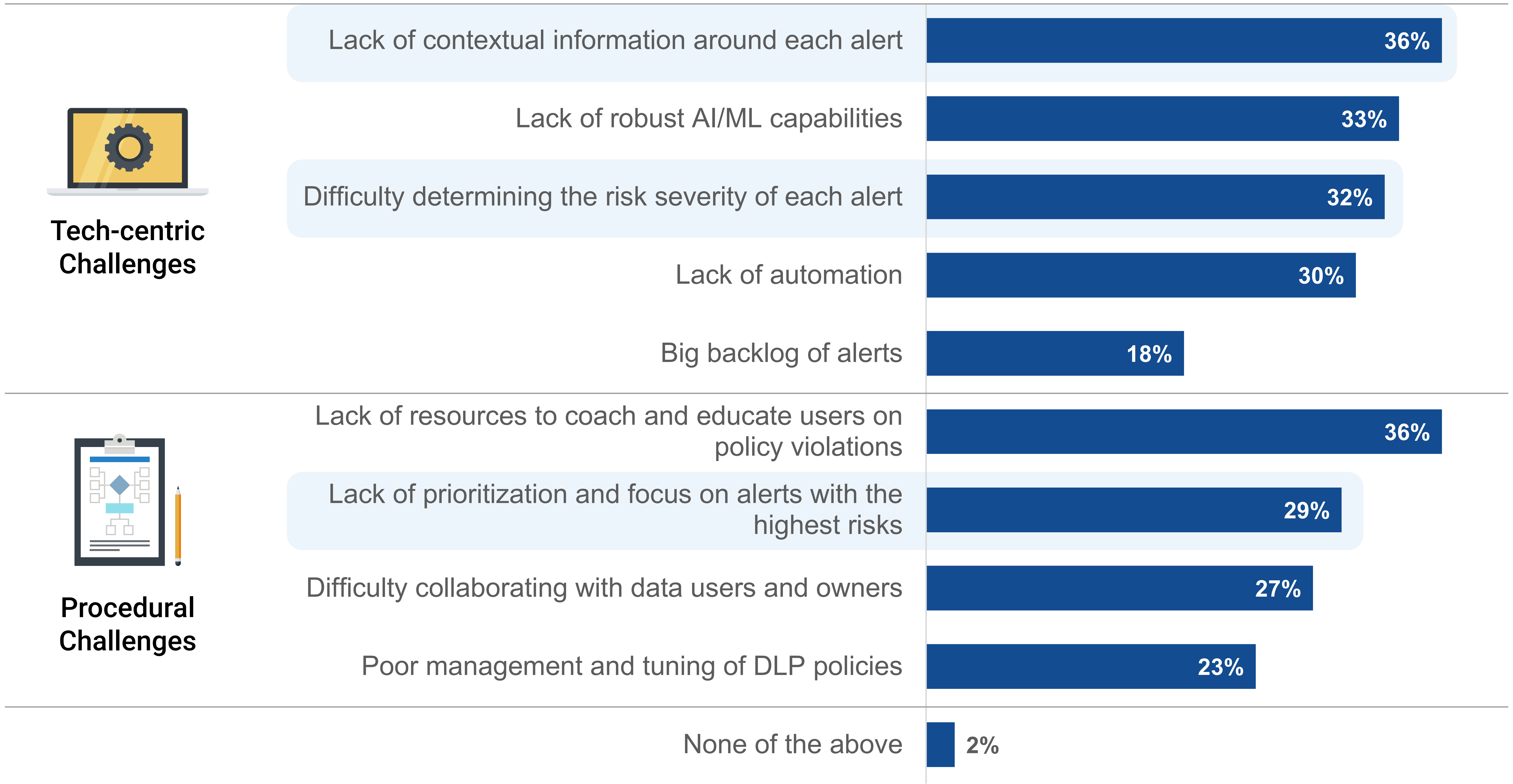
of DLP alerts that are inspected within 24 hours are false positives.

For example: Of the 65 DLP alerts that are inspected within 24 hours, 31 (47%) are false positives.

DLP Alert Remediation Challenges: Technology and Processes

Many technology-centric challenges lend themselves to technology disruption, and procedural challenges can be solved with new solution approaches. When an organization faces a deluge of false positive alerts, even the best procedures will do little to improve the situation. The lack of context and evaluating risk severity for each DLP alert are especially challenging for security teams.

Issues Preventing Prompt DLP Alert Remediation



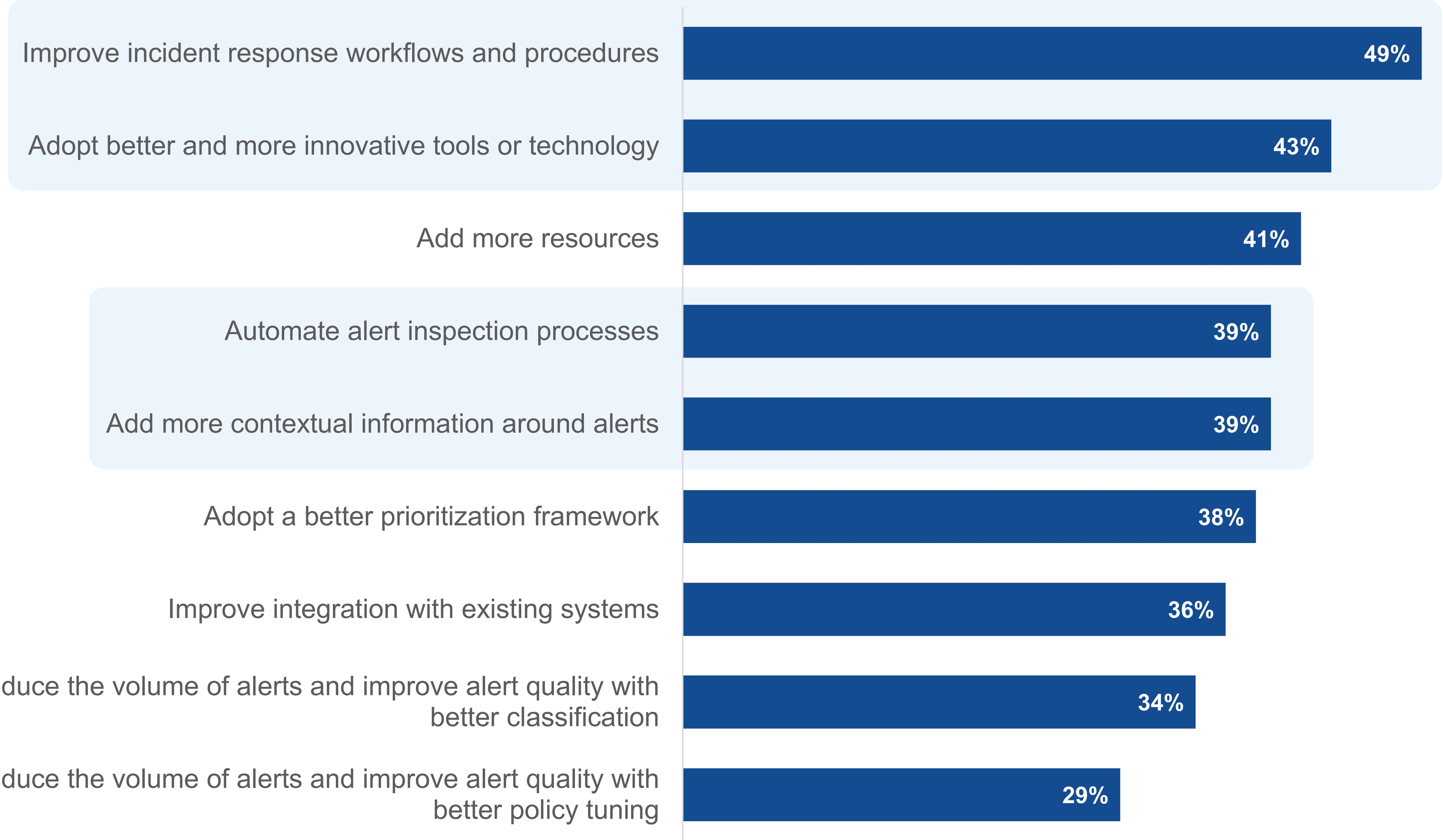
INTENTIONS AND PLANS:

Enterprises are primed to adopt innovations that streamline workflows, overcome alert noise, and remediate incidents.

Future-ready DLP Strategy: Optimizing Alert Investigations and Integrating Cutting-edge Tools and More Resources

A majority of organizations (60%) described innovation in the DLP category as excellent and are looking forward to innovative solutions for incident response workflows, automation, and additional contextual information.

Solutions for Accelerating DLP Alert Investigation



Investment Plans to Remediate DLP Issues More Effectively and Efficiently

Enterprises want solutions that provide context around DLP alerts and automate remediation actions to quickly and efficiently scale DLP event resolution. An “easy button” that helps implement DLP policies and prioritize alerts, combined with guardrails to help educate users on policy violations, can boost security team productivity and effectiveness.

Plans for Accelerating DLP Alert Remediation

44%

Help to prioritize and focus on alerts with the highest risks

43%

Adopt solutions with robust AI/ML capabilities

41%

Alert users of policy violations with collaboration tools

39%

Improve creation, administration and tuning of DLP policies

39%

Identify ways to reduce alert backlog

39%

Provide near real-time end user policy coaching in response to potential DLP policy violations

35%

Help to determine the risk severity of each alert

35%

Provide more contextual information around each alert

28%

Automate remediation processes

MIND

ABOUT

MIND is on a mission to help organizations thrive in a digital world by protecting their most sensitive information. MIND is the first-ever data security platform that puts DLP and insider risk management (IRM) programs on autopilot to automatically protect sensitive information, mitigate risk, and preserve brand reputation.

At the core of the platform is MIND AI, which autonomously monitors billions of data events 24x7 in real time, dramatically reduces false positives and noisy alerts, and effectively streamlines headcount needed. MIND AI is made of hundreds of tailored algorithms and a proprietary AI engine to classify and categorize sensitive data and understand context-aware business views to determine risk severity and take automated prevention and remediation actions. MIND enables businesses to mind what really matters—their most sensitive data.

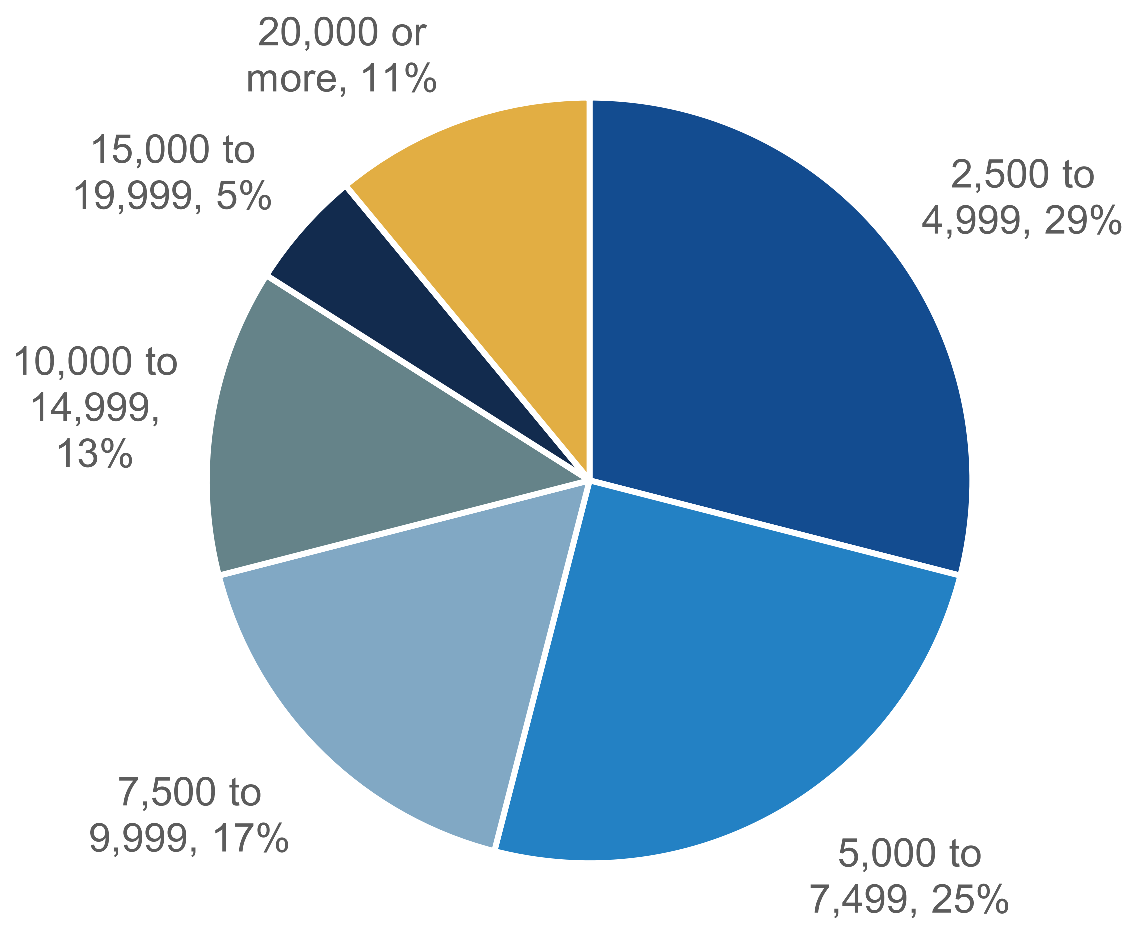
Learn more →

RESEARCH METHODOLOGY AND DEMOGRAPHICS

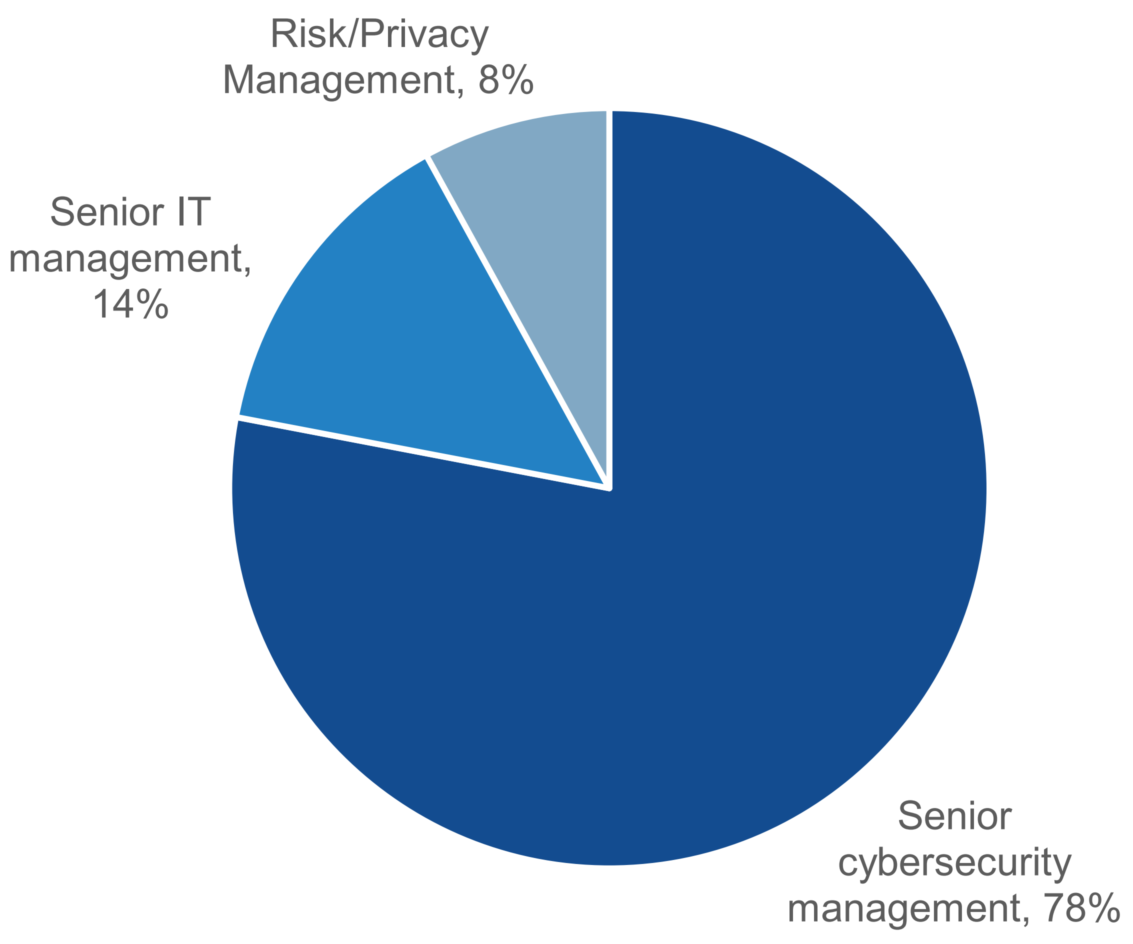
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of senior cybersecurity and IT decision-makers from private- and public-sector organizations in the United States in July of 2024. To qualify for this survey, respondents were required to be knowledgeable about their organization's deployed DLP technologies. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 100 senior cybersecurity and IT decision-makers.

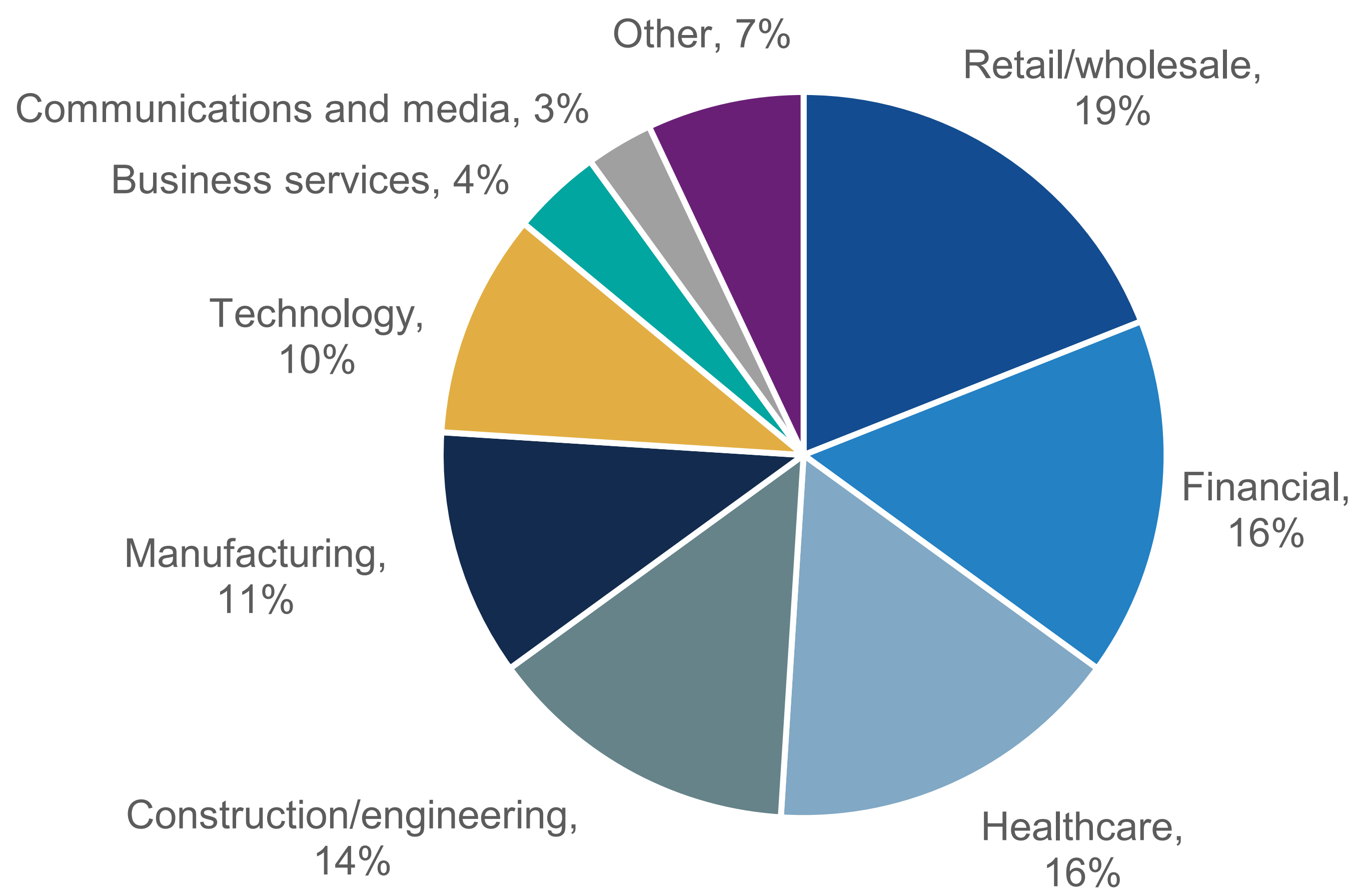
Respondents by Number of Employees



Respondents by Job Title



Respondents by Industry



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise
Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.