



# Adaptive Enterprise Data Loss Prevention in an Emerging Digital-First World

June 2023

Author:

**Ralf Helkenberg**, Research Manager,  
European Privacy and Data Security

IDC #EUR150557623

An IDC InfoBrief, Sponsored by

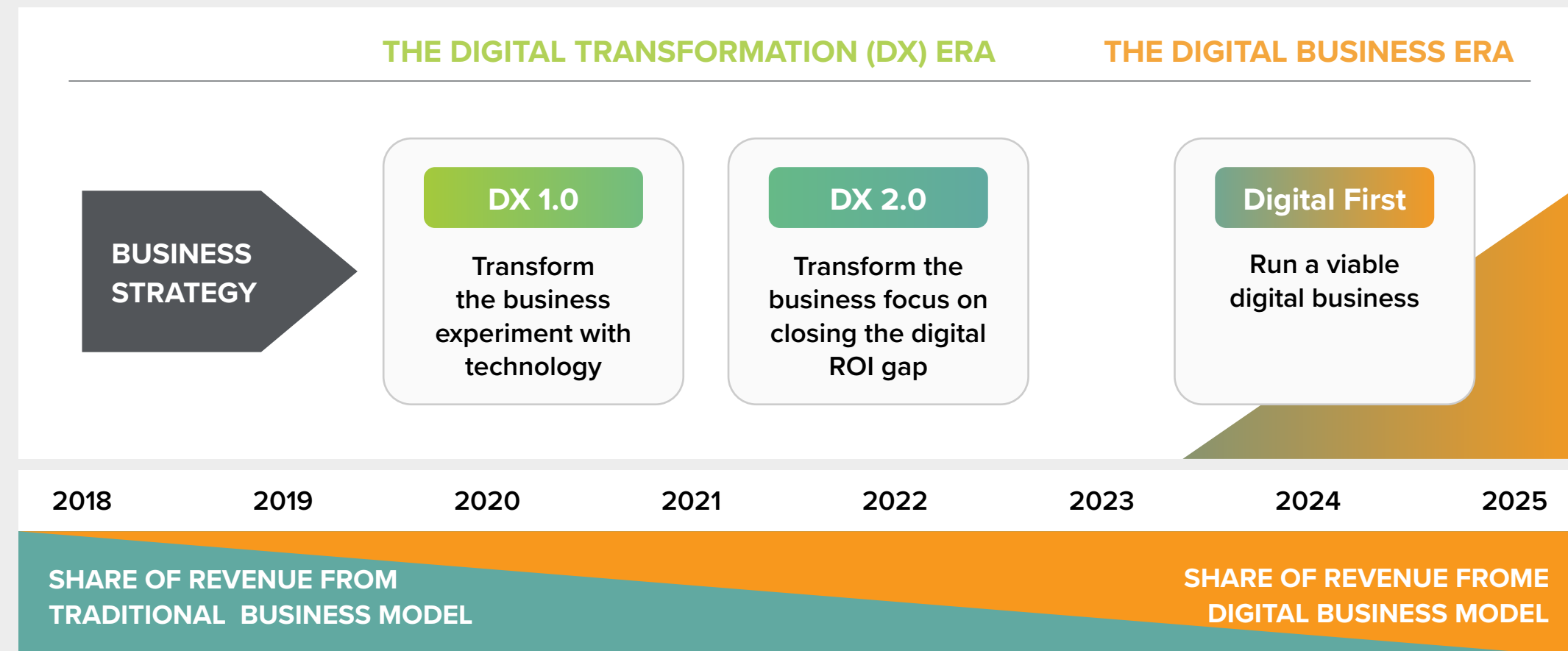




# Modern Data Protection in a Digital-First World

## Data protection for the digital first enterprise

According to IDC research, businesses are adopting a digital-first approach, shifting from iterative transformation to becoming a sustainable digital business. As a result, there is a growing trend toward modernizing IT infrastructure to support hybrid and multicloud architectures, AI and Big Data analytics platforms, and distributed data infrastructure models.



Source: IDC's Worldwide Digital Transformation Spending Guide

Delivering on the digital-first promise has expanded the attack surface that organizations need to protect and monitor for cyber risks. The evolving threat landscape and shift to cloud are putting enterprise data at an ever-growing risk of being compromised and maliciously exploited.

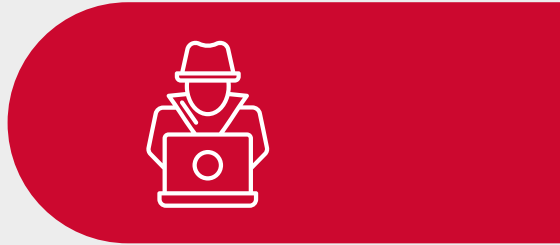
## Data loss prevention critical to modern data protection

Data loss prevention (DLP) provides a comprehensive and proactive approach to data protection. Benefits of modern DLP include:

- Improved visibility and control over the data estate
- Protection of sensitive data: reduce the risk of sensitive data loss, theft, or accidental disclosure
- User behavior monitoring and risk profiling to detect and mitigate against insider threats, intentional or unintentional
- Support zero trust: make informed decisions about access control and user privileges with sensitive data
- Smarter incident management at scale: prioritize and delegate responses based on incident severity and risk
- Support compliance with global regulations and industry standards
- Avoid data breaches and associated costs: legal fees, regulatory fines, and reputational damage

### Adaptive DLP for the modern enterprise

Many enterprises already have foundational DLP capabilities. The challenge lies in advancing and scaling these capabilities. This IDC InfoBrief explains how a modern enterprise DLP solution must not only consistently discover and safeguard sensitive data but also seamlessly scale and adapt to meet rapidly changing business needs and cyber risk without compromising on performance and effectiveness.



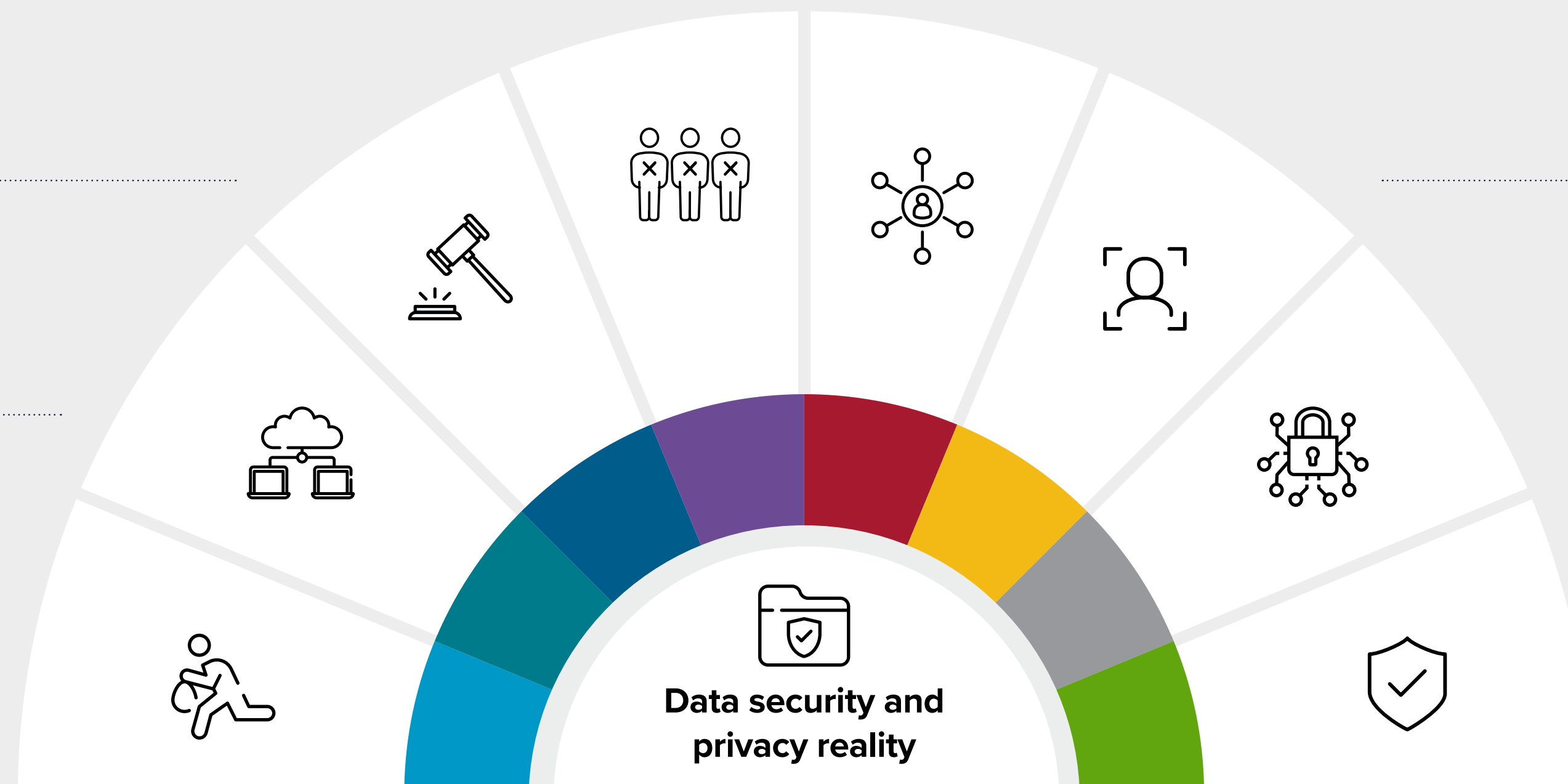
# Cyber Risk Professionals Face a Range of External, Operational, and Technical Challenges to Protect Their Enterprise From Cyberthreats and Data Breaches

Scarcity of qualified information security and privacy professionals

Navigating the regulatory compliance landscape

Digital transformation and hybrid work expanding the attack surface

Keeping pace with a growing and evolving cyberthreat landscape



Maintaining visibility and control over data spread across multiple platforms and locations

Identifying and stopping insider threats

Complexity of managing disparate security technologies

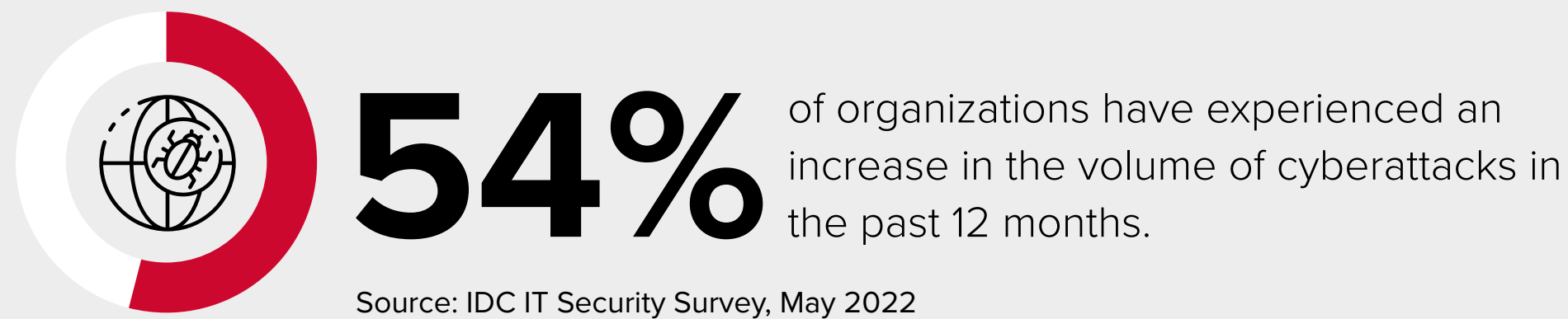
Digital trust climbing up the corporate agenda



# Data Exfiltration: The New Face of Ransomware

## The evolving cyberthreat landscape

Cyberattacks are growing in volume, variety, complexity, and precision:



## Cloud as an attack vector



Cloud attacks

The rapid shift of business-critical workloads and applications to the cloud has seen a rise in cloud-based data loss attacks, and supply chains are emerging as a new vector of attack as attackers seek to exploit vulnerabilities in a third-party supplier to compromise an extended network of customers and partners.

## Data exfiltration and loss is a growing risk

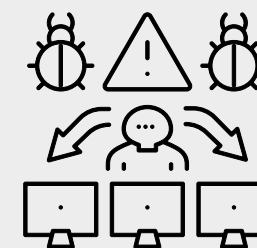


Data extortion

Ransomware groups are turning to data exfiltration missions to extort victims by threatening to release confidential information or sell it to unscrupulous third parties.



## The growing occurrence of insider threats



Insider threat

Data loss is increasingly caused by malicious insiders, compromised privileged accounts, or accidental data sharing by employees. The shift to hybrid working has made it harder to keep track of risky employee behavior actions without adequate cybersecurity monitoring.

**2022**

Cybersecurity threats

**CEO VIEW:  
Number 1  
business risk**

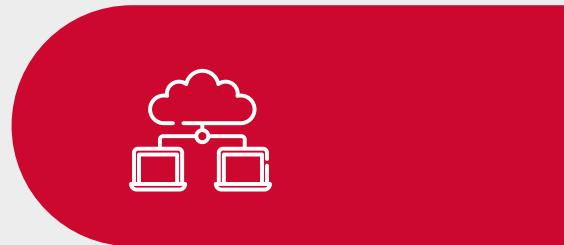
**2024**

Cybersecurity threats



## Cyber resilience is a strategic imperative

CEOs see cybersecurity threats as the main business risk over the next two years. The growing business cost and disruptive nature of cyberattacks and data breaches are requiring organizations to raise their security posture and strengthen their cyber resilience.



# Cloud Accelerators and Road Bumps

## Cloud adoption is accelerating

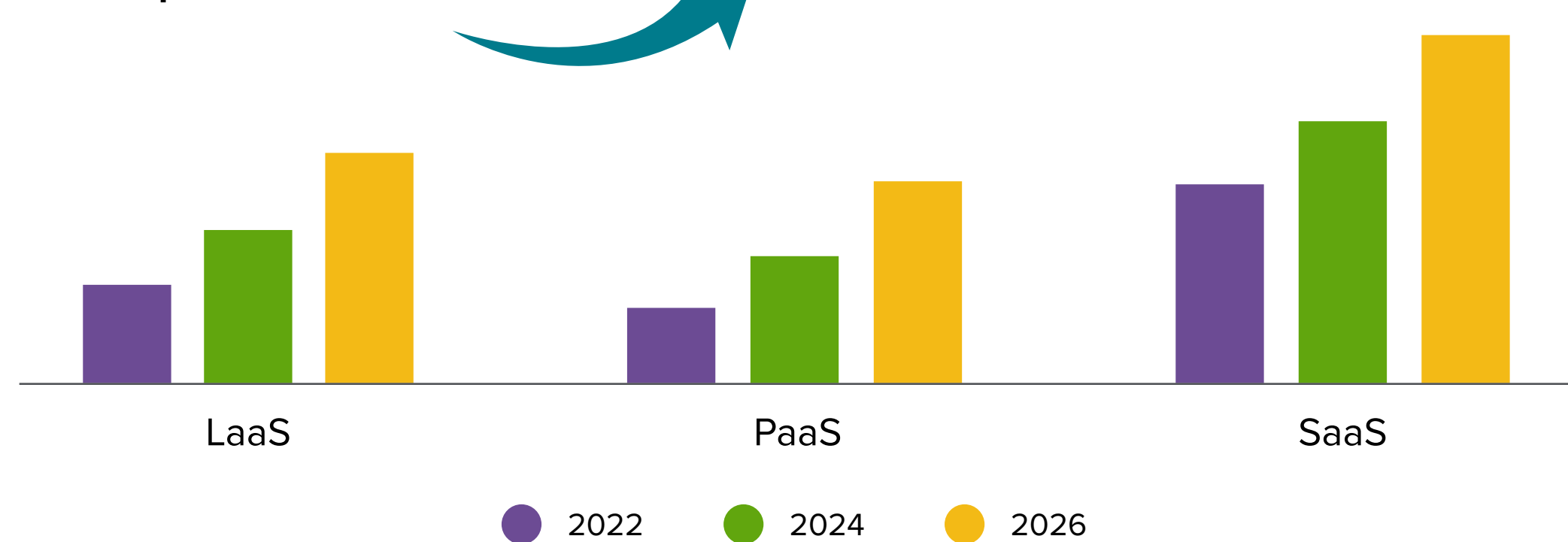


Cloud in all its permutations is playing an ever-greater role as organizations pivot to a digital-first economy. Cloud represented 39% of worldwide IT spending in 2022.

Shared (public) cloud as a service for infrastructure, platforms, and various software-as-a-service (SaaS) offerings continue to be the largest and fastest-increasing engines of growth for the whole cloud market, with spending forecast to grow at a CAGR of 20% by 2026.

## Public cloud as a service

Cloud spend: 20% CAGR to 2026



## Cloud trust concerns



Public clouds are typically multi-tenant environments sharing the same infrastructure. This gives rise to data security and privacy compliance concerns and is a key inhibitor to moving sensitive data into the public cloud, particularly in Europe.

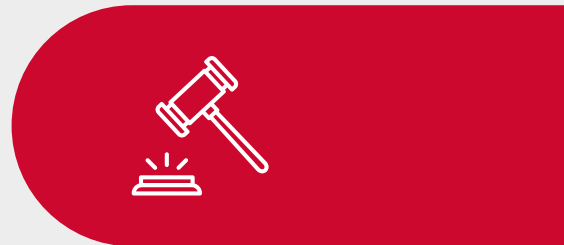
### 2022: top trust concerns impacting cloud strategy

- 1 Security of data
- 2 Privacy compliance
- 3 Data sovereignty

Source: IDC IT Security Survey, May 2022

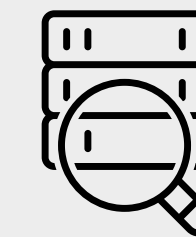
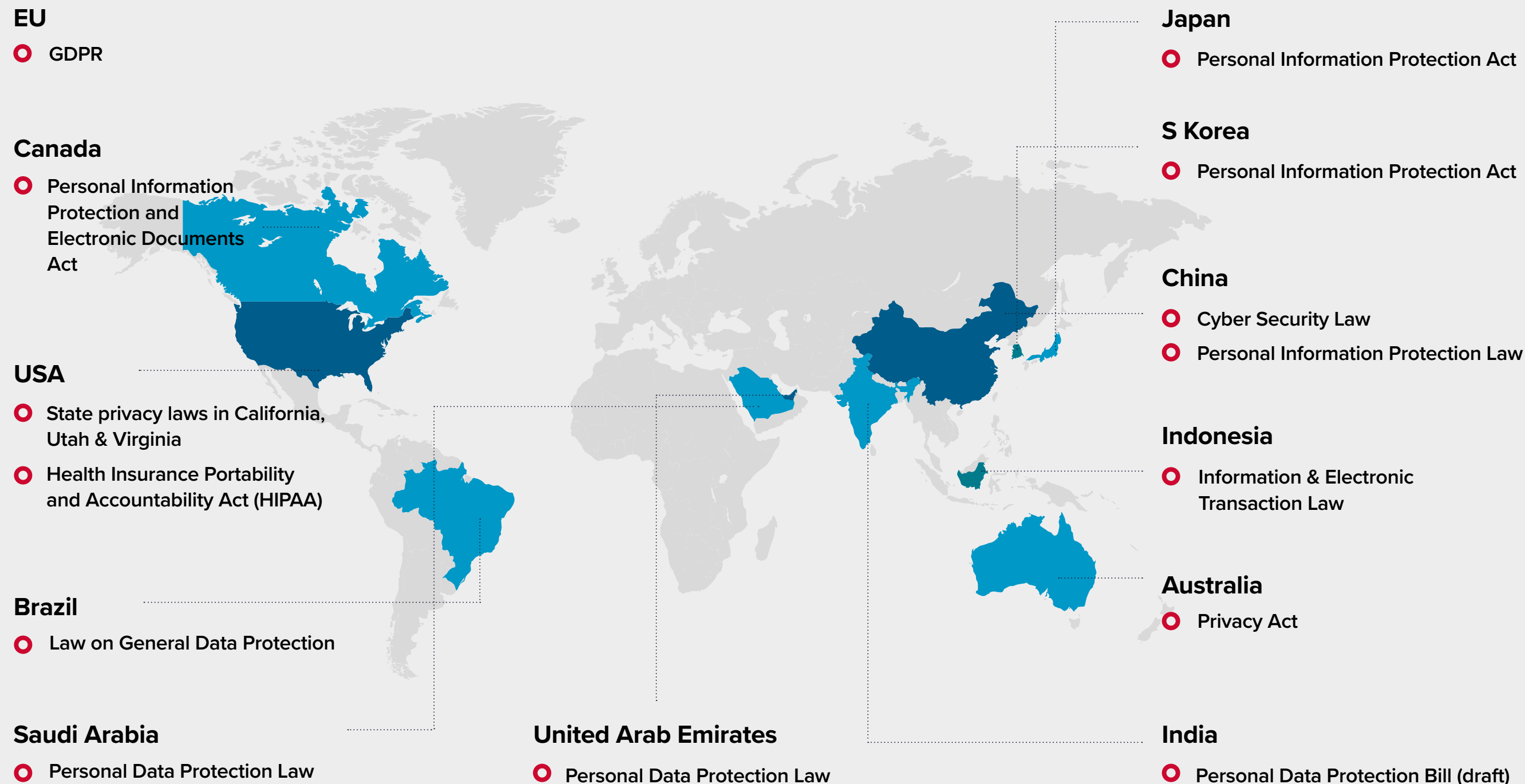
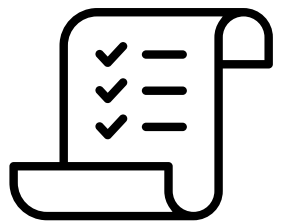
DLP plays a critical role in supporting data security and compliance in the cloud by providing organizations with greater visibility and protection from potential exposure of sensitive data in cloud-based data storage and applications.





# A Fast-Moving Regulatory Landscape Is Pushing Enterprises to Comply With New Data Protection Standards

Data protection regulations are expanding around the world as governments and regulators seek to strengthen data security and privacy protections and hold organizations accountable for how they handle sensitive data. This trend is set to continue as data-driven technologies advance and individuals become more aware of the value of their personal data.



## High-speed data discovery and scanning

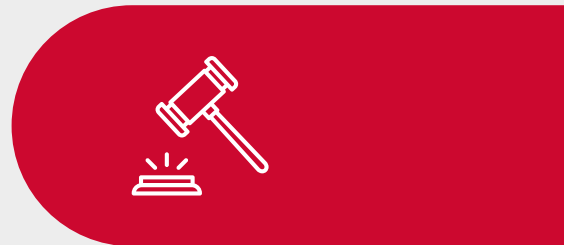
High-speed data scanning is essential to achieve regulatory compliance in data environments, increase efficiency to identify and classify sensitive data, and generate up-to-date reports on data protection and compliance risks.



## Regulatory templates

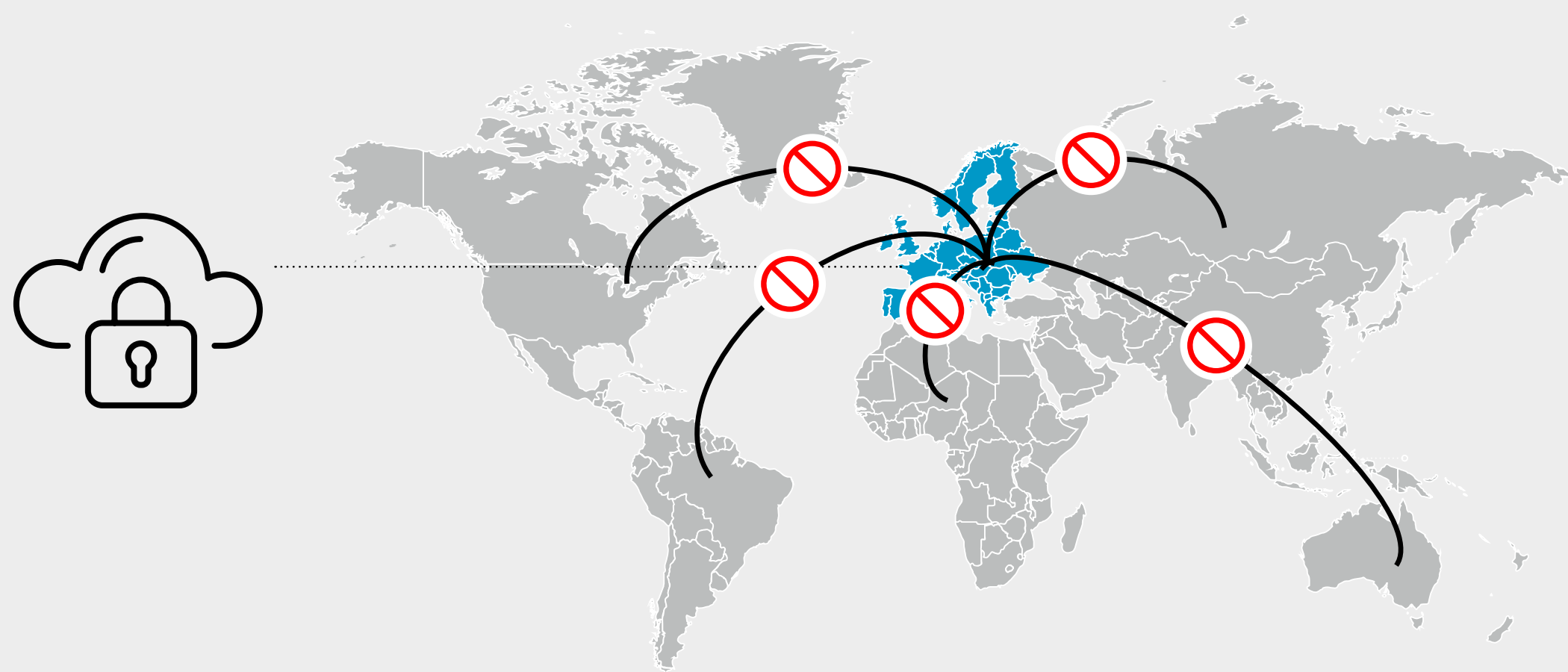
A library of preconfigured regulatory templates provides a fast, accurate, and consistent way to configure policies and rules that meet national, regional, and industry-specific regulatory requirements.

# The Rise of Data Sovereignty



## Cloud adoption is accelerating

Countries are taking more sovereignty measures to control the data generated in their jurisdictions, from rules that certain types of data must be stored in-country to conditions on transborder data flows.



### Data sovereignty

This is the concept that data is subject to the laws and governance structures within the country it is collected or pertains to and cannot be accessed by foreign governments.



The growing extraterritorial application of data governance laws is subjecting organizations to greater tension between allowing digital innovation to accelerate and ensuring data and IT infrastructures comply with regulations and guidelines. The data sovereignty implications extend to the cloud environment given that organizations are moving their services and data to platforms managed by international providers.



### How enterprise data loss prevention can support data sovereignty requirements:

- Apply data controls in hybrid mode: cloud for secure data processing flexibility and on premises to meet data location compliance requirements
- Monitor the location of data and provide alerts when data is moved to a location that is not authorized
- Ensure data is only accessed from within the authorized country
- Encrypt data to protect it from unauthorized access, even if it is transmitted outside of the authorized country
- Provide compliance reports on data storage and processing

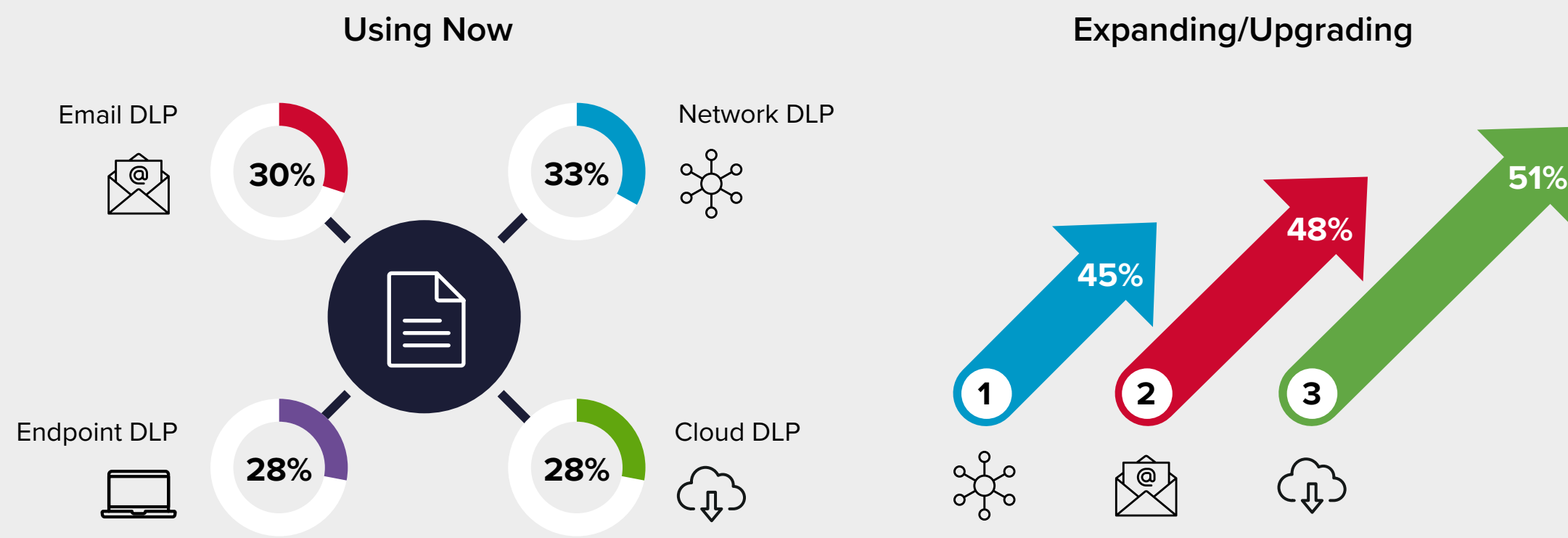


# Data Loss Prevention Renaissance

## Data protection through a single pane of glass

IDC believes enterprises need a single pane of glass to locate, classify, protect, govern access, and prevent data loss across the data estate. Working from the same data inventory and activity information provides a more comprehensive risk picture and strengthens the security posture against data exposure, loss, and theft.

## DLP renaissance

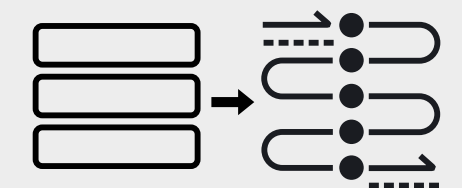


Source: IDC IT Security Survey, May 2022







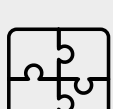
IDC research highlights a renaissance in data loss prevention. In a 2022 security survey, respondents cited network and email as the main use cases for DLP, with over 45% looking to expand or upgrade their DLP coverage, primarily across email and cloud environments.

## Risk adaptive data loss prevention

Modern data loss prevention has shifted from a static model to a dynamic approach that leverages data and security context to enable the proper protection controls based on changing conditions, incidents, and violations unique to an enterprise.



DLP capabilities are expanding to meet the evolving needs of the modern enterprise and alleviate security team workload in terms of:

-  **Scalability:** from handling large and growing volumes of data and users to ease of scaling new protections and updates across the enterprise
-  **Smart intelligence:** Machine Learning (ML) algorithms adapt to new data patterns and learn from previous incidents and user behavior to determine data risk, policy, and controls
-  **User-centricity:** enrichment of data risk with user behavior analytics to enable flexible context-driven policies that provide risk-appropriate access to apps and data
-  **Workflow automation:** detect and classify sensitive data automatically, apply policies to that data, and trigger alerts or actions based on policy violations
-  **Effectiveness:** consistent policy enforcement across channels (endpoint, network, storage, and cloud) delivered by a single DLP engine
-  **Cloud focus:** extend visibility and sensitive data policies to sanctioned and unsanctioned cloud applications and web traffic
-  **Security integration:** strong security integration capabilities including data backup, encryption, digital rights management, endpoint protection, and cloud app (CASB) and workload protection (CNAPP)





# Know Your Data: Expand Visibility With Intelligent Data Discovery and Classification

Whether it's to satisfy auditing requirements, compliance, or just corporate security policies, it's important to understand where your most sensitive data is flowing and how it's being used.

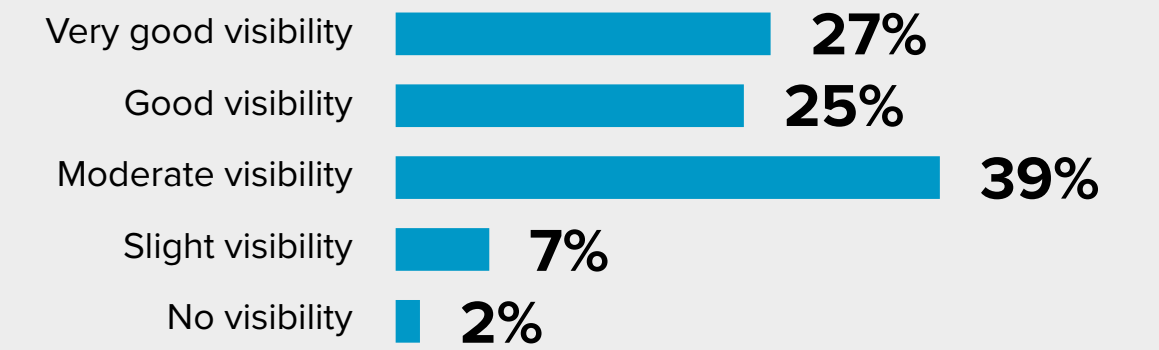
## Data discovery and classification in seven steps

1	<b>Data sources</b>	Identify all data sources; this includes databases, file systems, cloud storage, and applications
2	<b>Classification schema</b>	Define the criteria for classifying data, such as its sensitivity, confidentiality, integrity, availability, and compliance requirements
3	<b>Data Categorization</b>	Categorize the data based on business or regulatory requirements
4	<b>Data discovery</b>	Discover and catalog data held across environments
5	<b>Data classification</b>	Automatically apply classification labels to data
6	<b>Data protection</b>	Apply the appropriate security controls, such as access controls, encryption, and monitoring, to protect the data
7	<b>Monitor and update</b>	Data environments is dynamic and requires monitoring for changes or policy violations

## Data sprawl

Data in organizations is exponentially growing and widely distributed across environments. While some data is neatly structured, much lies unstructured. Data protection regulations require organizations to take a holistic view of their data, but data visibility is a blind spot for many.

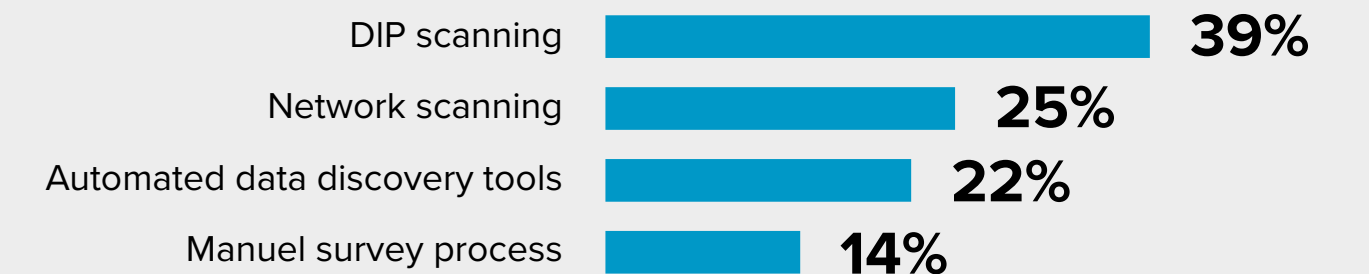
**Q. To what extent does your organization have visibility into regulated and sensitive data for privacy and security purposes?**



## In-depth discovery with high-speed scanning

Manual data discovery is resource and time intensive and fails to scale for distributed data environments comprising terabytes or even petabytes of data. High-speed automated data scanning is important in modern DLP, enabling DLP to quickly and efficiently scan large volumes of data, making it easier to scale to meet the needs of large enterprises. Advanced ML scanning technologies can understand both the content and context of the data.

**Q. What is the primary approach to locating sensitive data assets within your organization?**

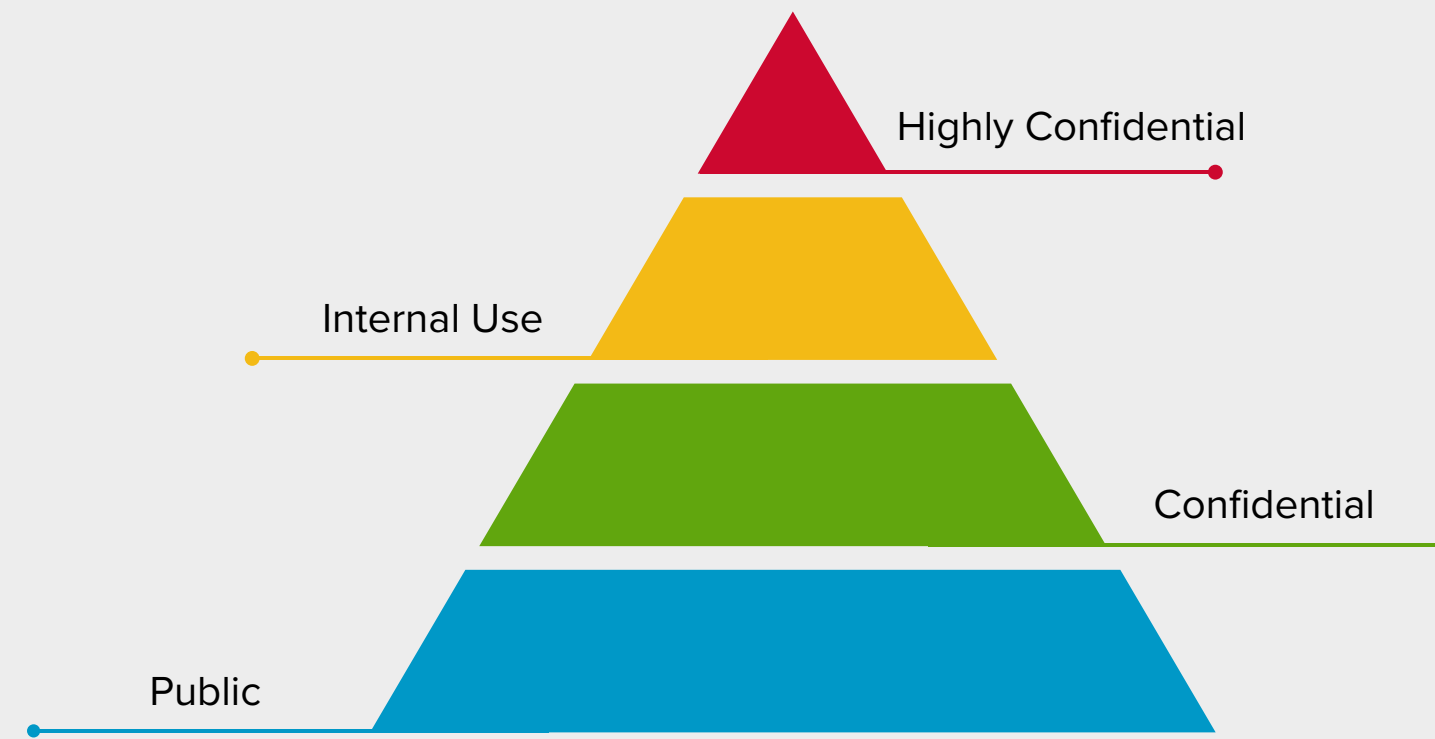




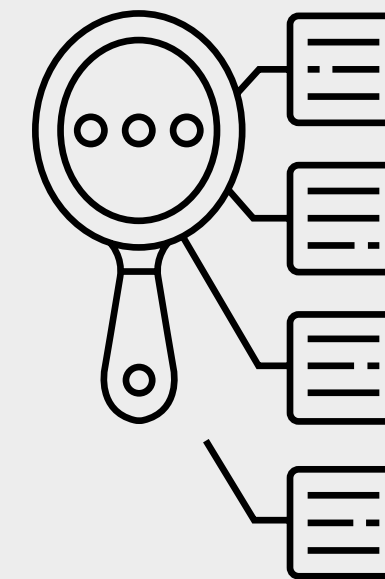


# ML-Powered Intelligent Data Classification

Data classification helps enterprises to prioritize data protection efforts and resources more effectively based on the sensitivity of the data.

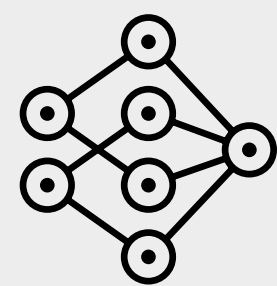


## Common technical approaches to data classification in data loss prevention



- Rule-based classification** is a simple and effective approach but may be limited in its ability to classify data that does not fit pre-defined rules.
- Pattern matching** for regular expressions can be more flexible but can also generate false positives or miss sensitive data that does not fit pre-defined patterns.
- Exact data match** detects specific data values to enhance detection accuracy and reduce false positives.
- Machine learning algorithms** analyze patterns and relationships in data to identify and classify sensitive information at scale.

## Benefits of machine learning in data classification



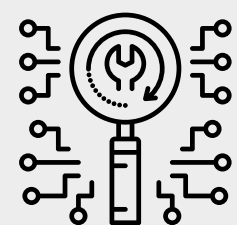
**Faster classification:** classify large amounts of data faster than with manual processes. Ensures that sensitive data is identified more consistently.

**Continuous learning and improvement:** learn from user actions and feedback to continuously improve the accuracy of data classification.

**Adaptability to new data types and patterns:** can be trained to recognize new data types and patterns, making them more adaptable to changing data environments. This reduces the need for manual updates to classification rules.

**Reduced manual intervention:** automate many of the tasks involved in data classification and enable security professionals to focus on higher-level tasks.

## A blended approach to machine learning is more powerful



Modern enterprise DLP supplements pattern and exact data match classification with advanced content detection and machine-learning capabilities. A technical hybrid approach improves the accuracy of data classification, reduces false positives, and scales better to handle large and complex data sets.





# Data Protection for Multicloud IaaS Environments

## Protect data at rest across cloud database storage repositories

Securing cloud data stores is a growing enterprise concern, as the amount of data stored in the cloud continues to grow exponentially.

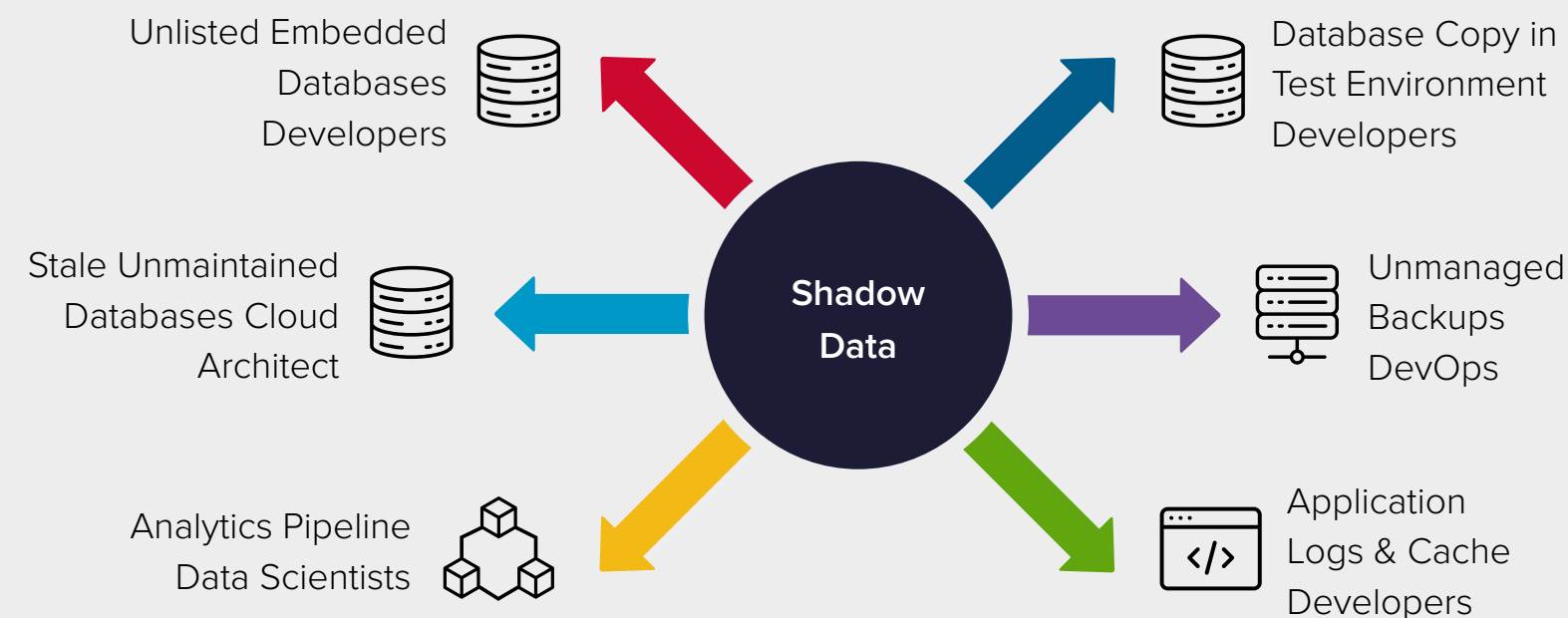
**What types of app security challenge are you most concerned about as part of the shift to public cloud platforms?**



Organizations, especially those with a cloud-first approach, are transitioning to distributed cloud-native applications based on microservices, containers, and serverless functions across platforms and locations. These environments are usually paired with a decentralized data architecture in which cloud workloads and databases can be spun up or shifted around within minutes.

## Securing shadow data in the cloud

Cloud services are the biggest contributor to the accumulation of shadow data — data that is beyond the view of data security teams. Examples of shadow data in the public IaaS environments include:



Point solutions from the cloud service providers do not in many cases support multicloud environments and are often limited in coverage and functionality.

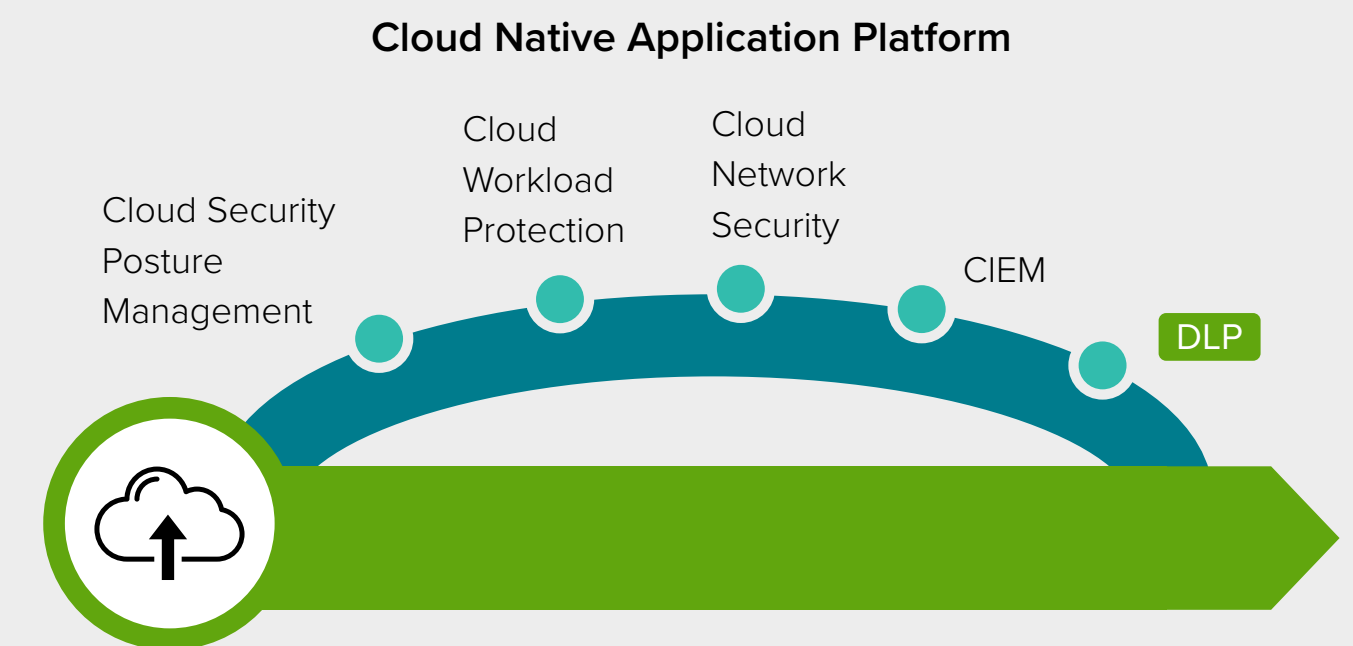


Poorly designed DLP and CASB integrations introduce operational complexity: from extra effort replicating on-prem policies to the cloud, to different management consoles and latency in synchronizing policies.



A cloud-native application protection platform (CNAPP) helps secure and protect cloud-native applications across development and production.

Integration with CNAPP is essential for cloud DLP, and should seamlessly extend the same curated data classification and protection policies on endpoints, networks, and datacenters to cloud database, storage, and Kubernetes environments.







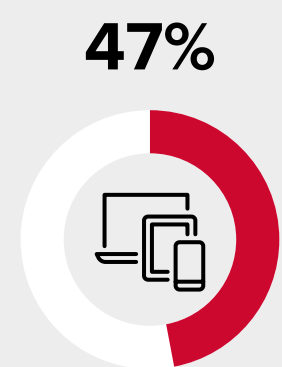
# Enterprise DLP Capabilities in the Modern Anywhere Office

Users expect a convenient work-from-anywhere experience. However, the shift to hybrid and remote work models has broadened the enterprise attack surface and the risk of data loss and exfiltration across endpoints and SaaS applications. Enterprises need to balance the protection of sensitive data across multiple channels with employee productivity.

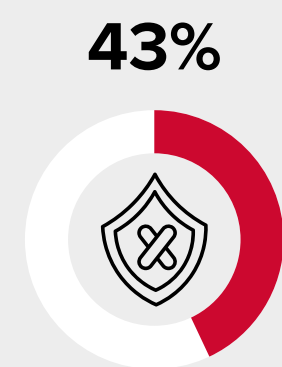


## Protecting endpoint data

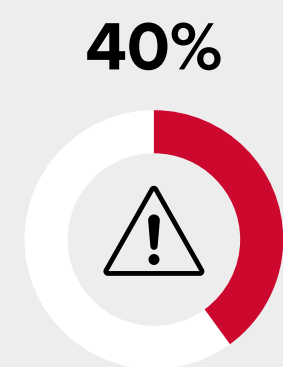
Hybrid and remote work is driving growth in endpoints that need to be managed. Sensitive information access on unmanaged devices is the top security concern.



Sensitive information accessed or saved on unmanaged devices



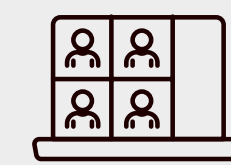
Communication over unsecure and unmanaged network



Greater risk of lateral movement from threat actors

## Endpoint DLP needs to be flexible enough to:

- Quickly adapt policies to a changing security risk environment
- Work across device types and configurations, both inside and outside the corporate network
- Provide granular visibility of workspace activity, including attempts to move sensitive data between endpoints and cloud services
- Effectively handle remote management at scale, such as updates and policy enforcement
- Support bring your own device (BYOD)
- Deploy a range of data protection controls: encryption, file quarantining, and digital rights management



## Data collaboration is in real time

IDC research highlights a growing preference for online-first collaboration tools such as chat, whiteboard, and online conference rooms. DLP approaches need to be adaptive to data flowing through collaboration tools where users communicate with short and unstructured messages leveraging more screen captures rather than traditional files to quickly convey ideas and information.



## Comprehensive data protection against shadow IT

DLP solutions and CASBs are complementary technologies that can work together to detect and protect against intrusions, threats, and data loss in cloud applications (SaaS). Integration should allow seamless extension of DLP policies and controls over sanctioned and unsanctioned cloud apps and continuously monitor the environment on a single console.



## Zero trust

Modern DLP solutions are becoming part of a zero-trust data protection fabric that incorporates real-time security posture assessments combined with least-privileged access for data, devices, and identities. Integration of DLP with other SASE technologies is an important step for advancing effective zero-trust implementations.






# Smart Data Loss Prevention for Email


Email security goes beyond protecting employees against sophisticated inbound email threats. Modern adaptive email data loss prevention offers real-time email protection from accidental or malicious leakage of sensitive data with fully customizable response actions.

### Data Classification of Email Messages



**62%** of survey respondents classify general email messages as either very or extremely sensitive.






### Likelihood of Email Leakage



**52%** of survey respondents report that email leakage of sensitive data is likely or very likely in their organisation

Source: IDC Data Security Survey 2021

### Common Email Errors Encountered by Data Protection Authorities

-  Email sent incorrect recipient due to human error
-  Email sent to incorrect recipient due to the message service predicting the recipient's email address based on the first characters entered
-  Attaching an incorrect document or hyperlink to an email
-  Forwarding an email chain to an unintended/unauthorised recipient
-  Email sent to multiple recipients using the "to" or "Cc" fields instead of the "Bcc" field

### Smart DLP protection for outbound email



Misdirected emails are a common source of data breaches. Advanced content-aware DLP capabilities in email security environments are therefore a must, but such protection shouldn't involve a tradeoff between secure communications, effortless configuration, and user experience.

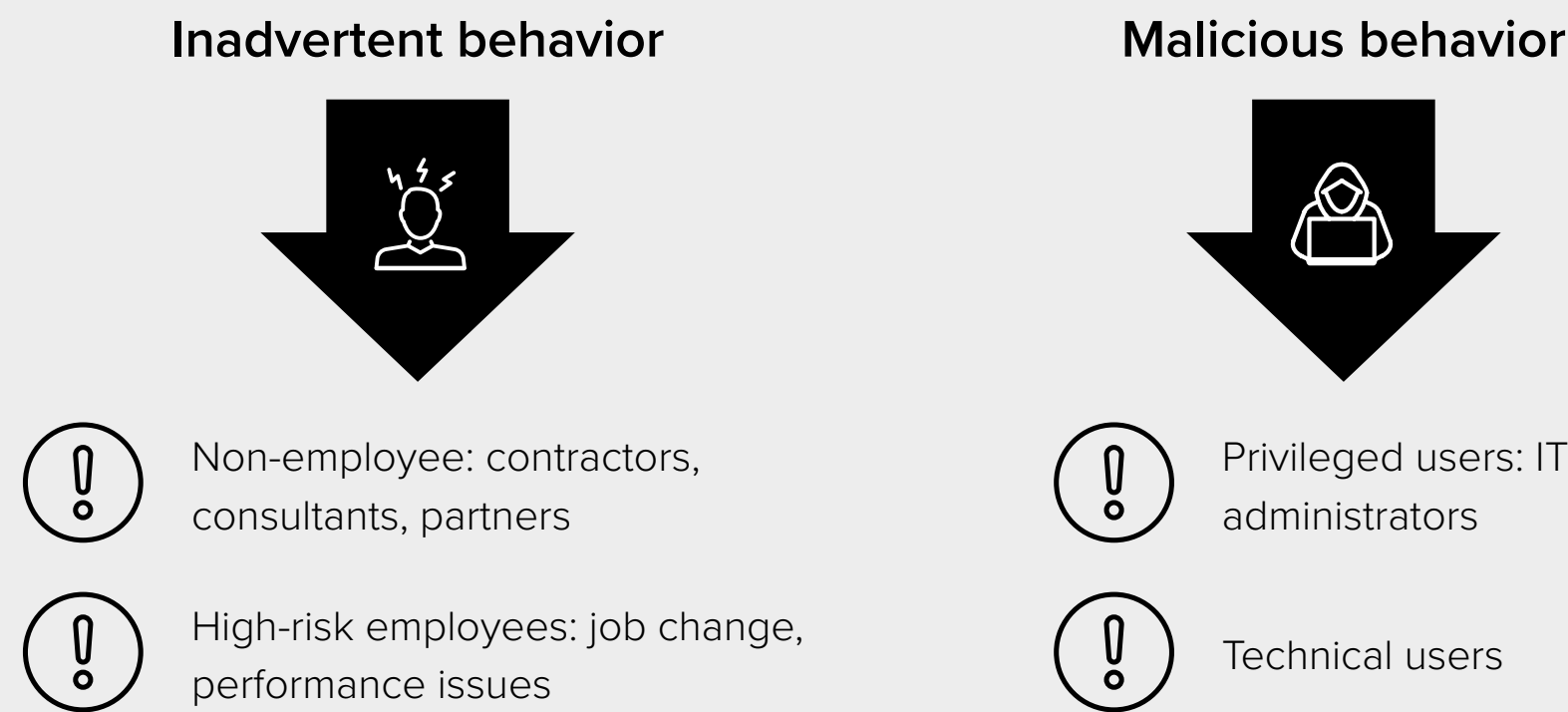
By overlaying ML-powered user behavior analytics, adaptive email DLP can identify patterns in user activity that are indicative of data exfiltration and take appropriate response actions to mitigate those threats such as message blocking, redirection, encryption, and quarantining.





# Insider Threat Management: User-Centric Visibility and Protection

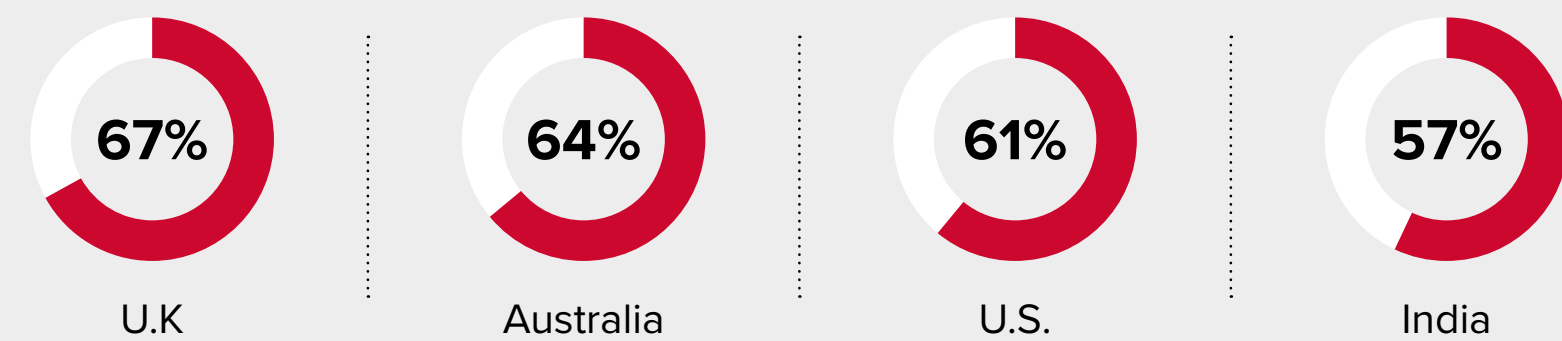
## Integrating the right tools into DLP can help to expedite the detection and management of insider risks



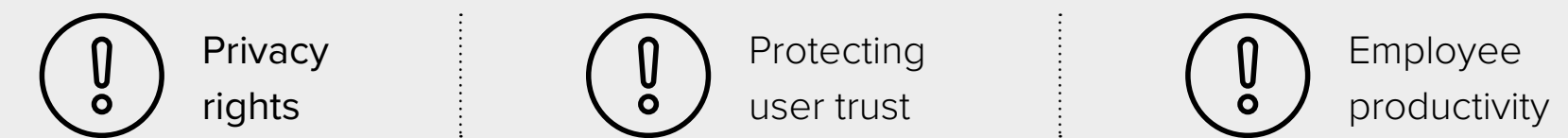
## Insider risk management is a high priority

**40%** of surveyed organizations experience up to three serious incidents of IP leakage/loss a year. Insider risk management is therefore a high priority for the C-suite.

### Q. How much of a priority is managing insider risk to senior management?



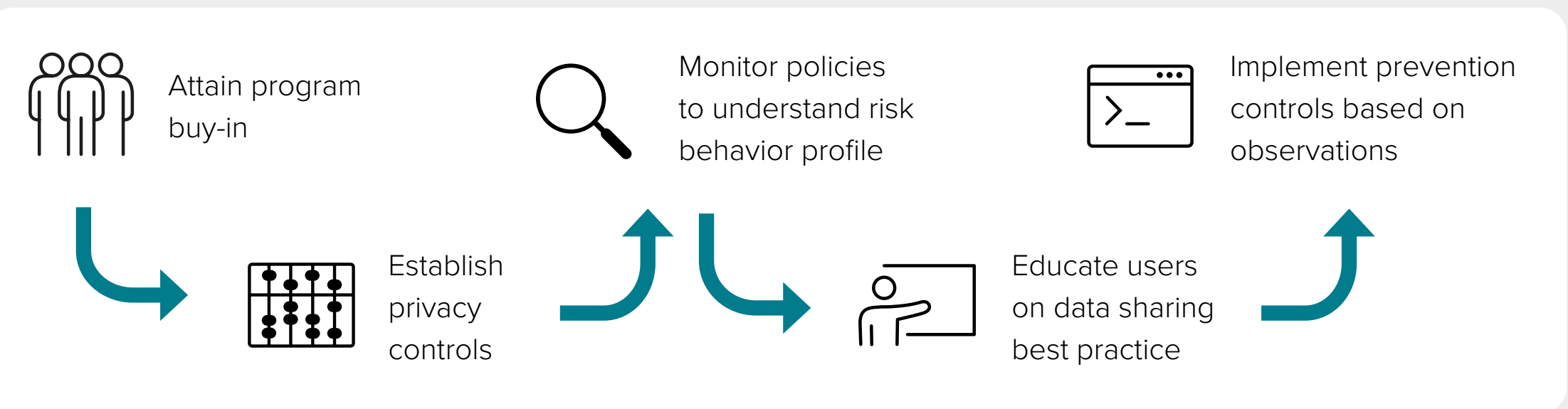
## Business concerns about insider risk management programs



## Balance protection and productivity

Enriching DLP information with user behavior analytics can provide a more accurate assessment of user intent around sensitive data, uncover broader behavior risks, and reduce the number of false positives. Convergence with insider risk management and user and entity behavior analytics (UEBA) fits well with the desire for a more user-centric approach by behavior modelling users to baseline normal activity and assigning appropriate policies and controls to high-risk users.

## Best approach to insider risk management

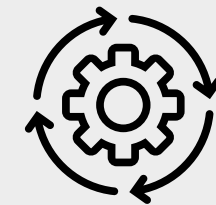






# Recommendations for Scaling Your Enterprise DLP Program

## Operational considerations



**Develop a comprehensive DLP strategy:** Before scaling your DLP program, have a solid DLP strategy that outlines your organization's data protection goals, governance policies, and regulatory requirements.

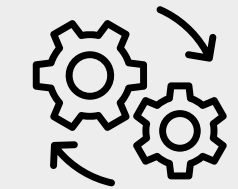
**Work closely with other departments:** Collaboration with data, IT, legal, and privacy and compliance teams is essential when scaling DLP. Ensure that all relevant line of business departments are involved in DLP planning and implementation.

**Educate employees:** Employee awareness and training are crucial for successful DLP implementation. Educate employees on data security best practices, data classification, and how to identify and report potential security incidents.

**A risk-based approach:** Identify high-risk areas and data types. You can then strategically prioritize the application of advanced DLP controls to achieve the greatest impact.

**Monitor your DLP program:** As you scale, continuously monitor and evaluate your DLP program to ensure that it remains effective and meets your organization's evolving needs.

## Technical considerations



**Centralized management:** A unified view that allows security teams to monitor and manage DLP policies and incidents across multiple systems and data sources at scale from a single interface.

**Scalability:** As the volume of data and number of users increases, your DLP needs to be able to scale to meet these demands. This means that organizations need to consider the scalability of your DLP solutions, both in terms of hardware and software.

**Performance:** DLP needs to be able to scan and analyze data quickly and efficiently, without impacting system performance or user productivity. This means that you need to consider the speed of scanning and analysis needed, and the impact on network bandwidth.

**User-centric:** Enrichment of data risk with user behavior analytics to enable flexible context-driven policies that provide risk-appropriate access to apps and data and detect and identify patterns in user activity that are indicative of critical data loss.

**Automation:** Streamline DLP processes including data discovery, classification, policy enforcement, incident response, and reporting through native orchestration capabilities to reduce the burden on IT and security teams.

**Productivity:** System can handle incidents at scale through a single unified view of incidents, consolidated with contextual reports, and alleviate incident response team workload through flexible remediation capabilities including delegating incidents to data owners for review.

**Customization:** Consider to what extent customization is needed to meet the specific needs of the organization, including policies, rules, and workflows, and whether the DLP solution has the appropriate capabilities.

**Integration:** Interoperability with other security technologies needs to be considered to ensure that they work seamlessly and effectively together.



# Message from the Sponsor

Symantec DLP is here to help you protect your sensitive data everywhere.

Managing an effective data security program demands careful thought and reliable technology. We partnered with IDC to share its research on the key issues facing enterprises, including cloud migration, compliance, machine learning, and user risk.

We help the largest organizations navigate this complexity. Our solution provides highly accurate protection and reliability at scale and simplifies the workload of DLP administrators and incident responders. Please get in touch if you would like more information:

**[www.broadcom.com/dlp](http://www.broadcom.com/dlp)**





# About IDC



International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

## **IDC UK**

5th Floor, Ealing Cross,  
85 Uxbridge Road  
London  
W5 5TH, United Kingdom  
44.208.987.7100  
Twitter: @IDC  
idc-community.com  
www.idc.com

## **Corporate Headquarters**

140 Kendrick Street,  
Building B, Needham,  
MA 02494 USA  
508.872.8200  
www.idc.com

## **Copyright Notice**

---

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or [permissions@idc.com](mailto:permissions@idc.com). Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit [www.idc.com](http://www.idc.com). For more information on IDC Custom Solutions, visit [http://www.idc.com/prodserv/custom\\_solutions/index.jsp](http://www.idc.com/prodserv/custom_solutions/index.jsp).

Corporate Headquarters: 140 Kendrick Street, Building B, Needham, MA 02494 USA P. 508.872.8200 [www.idc.com](http://www.idc.com)

© 2023 IDC. Reproduction is forbidden unless authorized. All rights reserved.