Microsoft Security

Protecting Your Data End-to-End

How to strengthen and simplify information protection and data loss prevention

Contents

Introduction

Data management challenges and an increasingly remote workforce call for an intelligent approach to safeguarding data across the enterprise

Protecting and preventing the loss of sensitive information have long been priorities for enterprise IT and security teams. Now, however, with people, devices and applications extending well beyond the confines of the traditional office, CIOs and CISOs are rethinking their approach to information protection and the tools they need to secure sensitive data and prevent its misuse.

Consider that even before the sudden work-from-home shift in early 2020, **64%** of executives and office workers said many employees were already working outside the office at least one day a week, according to the PwC 2020 Remote Work Survey. Executives expect the trend to continue in the months ahead, with 89% saying that many or most employees will not return to the office for the foreseeable future. Nearly three-quarters of workers **(72%)** said they'd like a permanent option to work away from the office at least two days a week, with nearly one-third **(32%)** saying they prefer to never go back to their office, versus **18%** prior to 2020.

As data extends well beyond on-premises infrastructure into multi-cloud and hybrid cloud environments, IT and security teams are looking for ways to better manage the entire data life cycle – from when data is created to when it is retired or deleted. A key piece of these efforts is to reduce risk without compromising user productivity across this expanded IT landscape.

The ability to integrate these activities into an end-to-end solution can help to close those gaps and reduce risk.

This end-to-end approach involves three key steps: **identifying your data, classifying it and deploying tools and policies to safeguard it**. The goal is to help ensure all information is protected, however and wherever it's used.

Organisations have a variety of technology and tools at their disposal for managing and protecting data at different stages of the life cycle. While these tools provide flexibility, they also add significant complexity. A recent IDG study found that organisations use an average of nearly five different data management systems for activities such as classification, e-discovery and records management. This patchwork of tools can leave unexpected and critical gaps that lead to data leakage.

Know your data

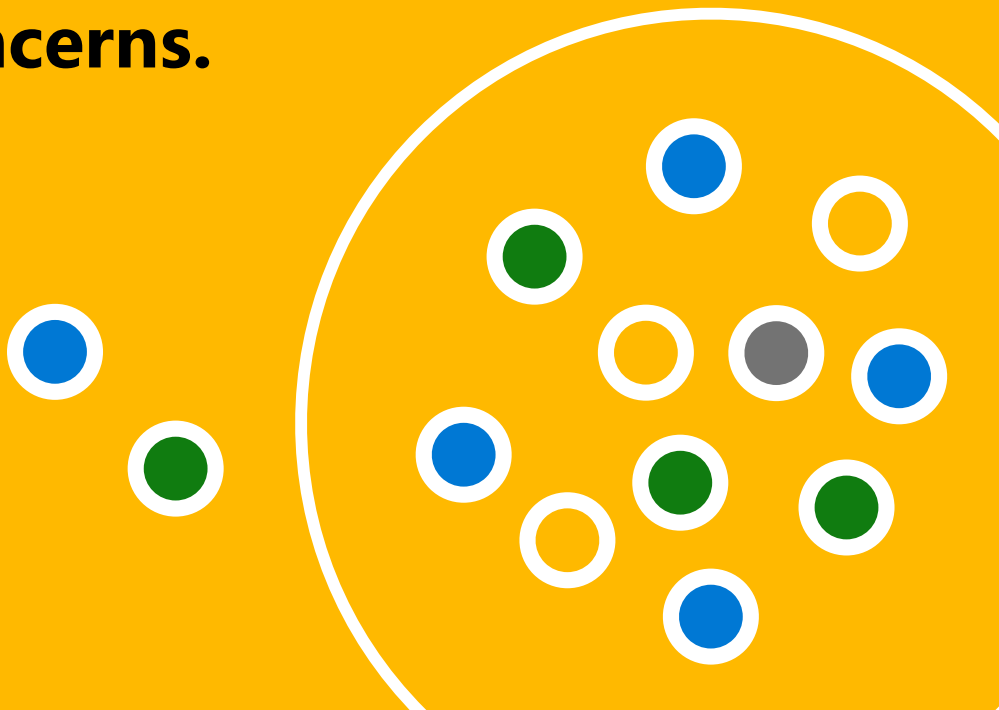
An integrated approach offers more flexibility in identifying and classifying data.

If you don't know where all of your data lives, what kind of data it is or how it's being used and shared, it's impossible to apply the right levels of protections or policies to it. Two-thirds of organisations in the IDG study acknowledged they don't have the skills, resources, technology or process to classify or delete 'dark' data – information that's collected but not put to use.

The challenge will only grow. The amount of enterprise data is roughly doubling every two to three years, and data is captured and stored in a wide array of locations and environments, from on-premises and cloud storage to a multitude of servers, desktops, laptops and mobile and smart devices.

Artificial intelligence (AI) and machine learning (ML) technologies are playing an emerging and critically important role in helping IT and security teams get their arms around this challenge. AI/ML algorithms can be trained to recognise sensitive data, such as email addresses, health data, credit card numbers or intellectual property, and then classify it automatically to define what level of protection the data requires. AL and ML can increase classification accuracy and can even be used to retroactively review data that previously had been manually classified.

Depending on their use case, organisations can start with classification, then build data loss prevention (DLP) policies around categories. Or, they can begin with DLP policy-setting to then shape data classification. Either way, this flexibility enables an organisation to more quickly address data protection concerns.



Protect your data

Protective measures such as encryption and watermarking can further protect data at rest, in transit and in use.

With data properly classified, organisations can apply a variety of policies and risk mitigation solutions to help ensure it is not accidentally or intentionally misused or accessed by unauthorised entities.

To protect data as it travels around the organisation, data classification cannot be confined to discrete documents. Instead, classifications – and policies – must follow the data. For example, if a marketing employee copies credit card numbers from a Microsoft Word document into an Excel spreadsheet, the classification and assigned policies should automatically apply to both the old and newly created documents.

To be effective, labelling and protection policies must span the entire digital estate – on-premises repositories, OS-native applications, cloud-based repositories and Software-as-a-Service (SaaS) apps. Traditional approaches involve considerable manual work to classify all this data, which runs the risk of errors or inadvertently overlooking critical data.

Ensuring data is correctly classified is critical to the success of a data classification initiative, and anything else that will leverage that data classification in the future. It should be done right from the start. An integrated solution helps administrators manage these policies centrally and ensures they are applied across all systems.

Prevent data loss

Identifying and classifying data are prerequisites to mitigating actions that might lead to accidental sharing of sensitive data outside of the organisation.

This is where DLP solutions come into play. They enforce policy to prevent employees from intentionally or inadvertently sharing, exposing or transferring sensitive data without authorisation.

Intelligent DLP solutions use context to find a balance between blocking high-risk actions and providing flexibility of choice. For example, individuals may be presented with an option to continue when a justified business use is required, while still providing information about the potential risks and applicable policies. The goal is to ensure that sensitive data is used as intended, and in the process also train users to better understand the risks to sensitive data.

Let's revisit the example of the marketing employee who copied credit card numbers from Word into Excel. If the individual then tried to download the spreadsheet file onto a flash drive or upload it to a share storage folder in the cloud, DLP policy would identify this activity as being out of compliance with stated policy and prevent these actions from completing.

A DLP solution is critical for protecting intellectual property and other critical business data, as well as to help achieve compliance with regulations such as the General Data Protection Regulation (GDPR), Health Information Portability and Accountability Act (HIPAA) and the California Consumer Privacy Act (CCPA).

In addition, a comprehensive approach to DLP enforces policies consistently across the organisation, reducing potential exploitation of 'weakest link' points in the data life cycle.

Look for built-in versus bolt-on solutions

Importantly, intelligent information protection provides peace of mind that sensitive information has the proper safeguards wherever it resides.

A ‘bolt-on’ approach to information protection, in which different solutions manage discrete parts of the data life cycle, can leave critical gaps that expose data to unauthorised use or leakage across different business units or outside of the organisation. Increasingly, organisations are looking for an integrated, end-to-end solution that brings together data discovery, classification and DLP across the environments that their information workers interact with every day – such as email, file storage, collaboration and other platforms.

A ‘built-in’ approach makes it easier to centrally manage and enforce information protection policies across the enterprise and also reduces training time for users, since policy enforcement experiences such as notifications occur in a familiar way natively within the application.

End-to-end: information protection plus data loss prevention

Microsoft Information Protection and Microsoft Endpoint Data Loss Prevention offer built-in automation and intelligence to protect sensitive information and help organisations meet compliance requirements.

These capabilities have now been extended to the endpoint with Endpoint Data Loss Prevention. Organisations can get a complete, end-to-end system that protects information no matter where it may reside without putting up barriers that interfere with employees' daily work. It automatically identifies and classifies data to protect against accidental or intentional loss without the need for an additional agent.

Learn more about Microsoft Information Protection >

See how to get started with Microsoft Endpoint Data Loss Prevention >

Microsoft