

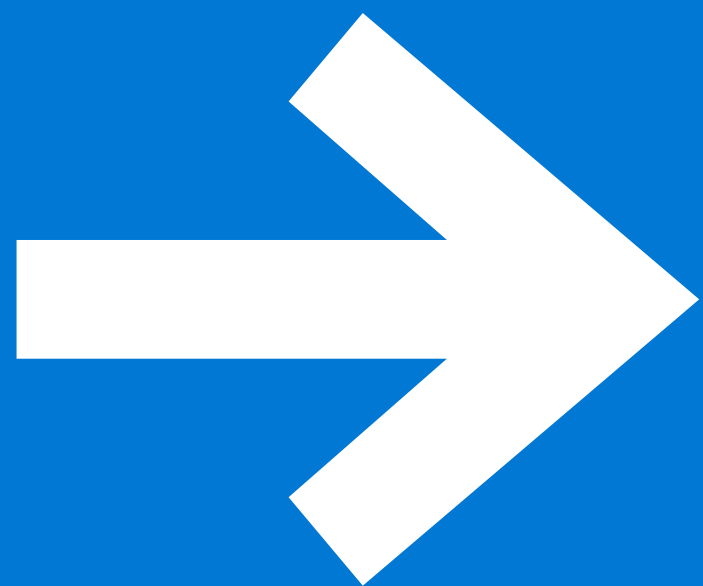


4 steps for achieving a forward-thinking compliance strategy

Get integrated tools that help you intelligently assess risk, govern and protect sensitive data, identify and take action on insider risks, and effectively respond to regulations.



Introduction



A growing and evolving set of laws and regulations, including GDPR and CCPA, is holding organizations more accountable for protecting customer data. As data increases exponentially—and gets shared beyond the corporate firewall more widely—it's more challenging than ever for organizations to meet their compliance obligations.

Microsoft 365 compliance solutions are built in, providing integrated, intelligent tools to reduce your risks. These tools can help you better assess risk, govern and protect sensitive and business-critical data, and respond to regulatory requests with intelligence and efficiency.

Learn how Microsoft 365 can help on your compliance journey:

4 steps for achieving a forward-thinking compliance strategy



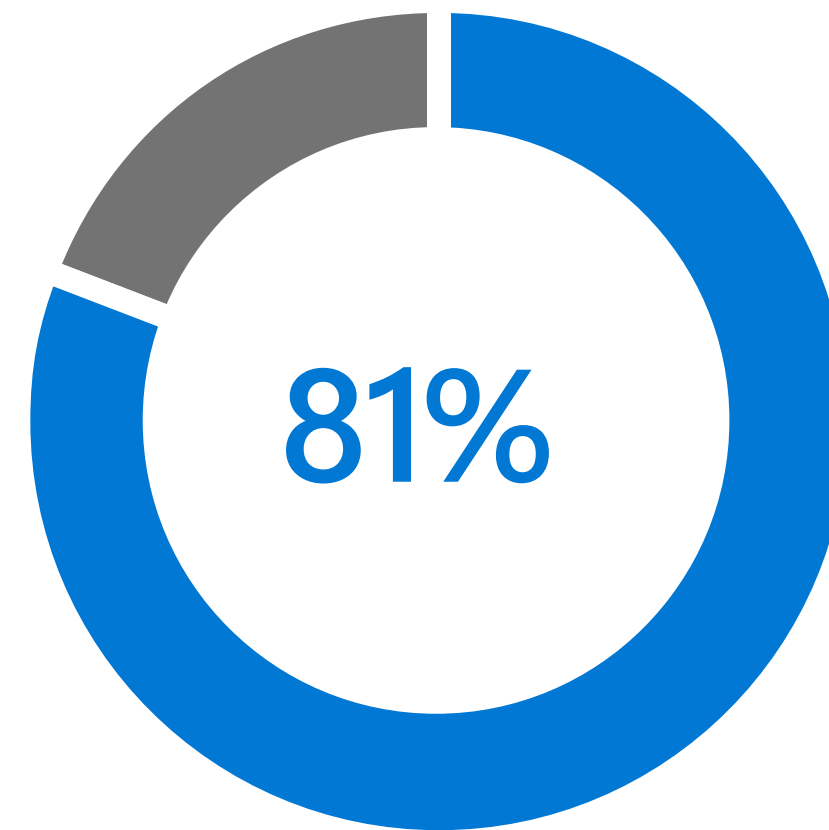
1. Protect and govern data wherever it lives

Improve compliance by detecting critical data wherever it resides, keeping control of data wherever it travels, and classifying, labeling, and protecting data.



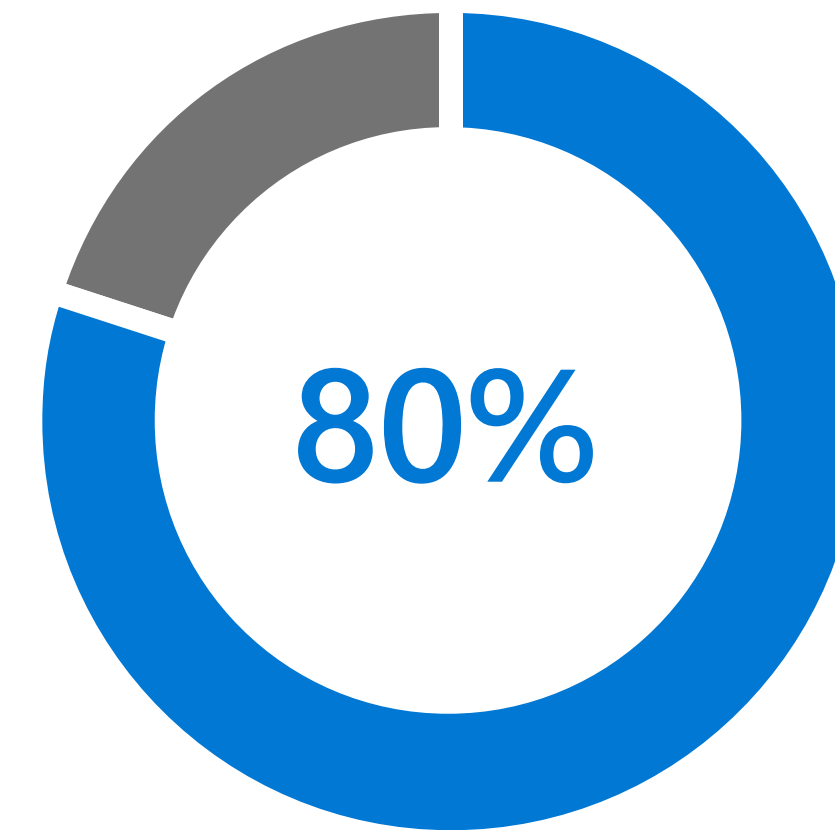
Enabling a hybrid digital environment has dramatically increased productivity and collaboration across organizations, yet managing and monitoring data growth across endpoints has remained a challenge. In the modern workplace, there are very few limits to where corporate data may travel.

While mobility and cloud services have helped users become more productive and collaborative, securing and monitoring the data has become harder. You need to protect sensitive information anywhere, anytime.



81% of breaches involve stolen or weak credentials.¹

¹ Verizon Data Breach Report, 2017



80% of all corporate data generated is “dark”—i.e., unstructured and not utilized in other ways. This will rise to 93% by 2020.²

² IBM, The Future of Cognitive Computing



Reduce risk and harness your organization's dark data with information protection and governance

Get a handle on the data and complexity in your environment with a simple interface that helps you discover, classify, protect, and govern data across end points.

Start with discovery of sensitive information (and data that has exceeded its useful life) across on-prem, file shares, cloud locations, and more. Then set comprehensive policies to protect and govern your most important data throughout its lifecycle.



Take a unified approach to identify, classify, and label your sensitive data.



Automatically apply policy-based actions.



Use proactive monitoring to identify risks.





Get broad coverage across locations and applications.


1. Protect and govern data wherever it lives

Use encryption that helps meet your compliance needs

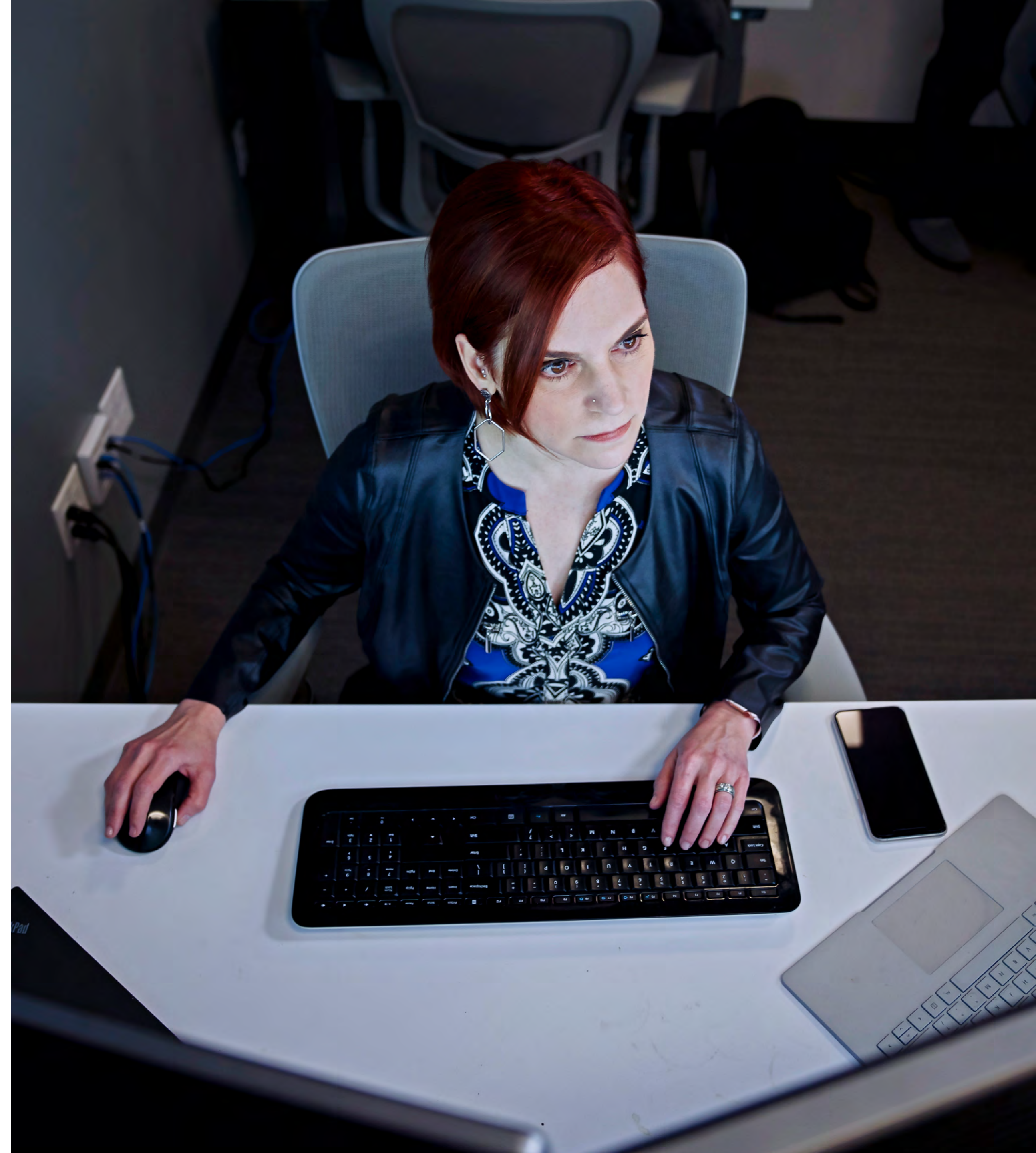
Microsoft follows stringent industry standards for encryption and uses some of the strongest encryption protocols.

 Meets rigorous industry standards.

 Data is encrypted by default at-rest and in-transit.

 Additional customer controls for added protection and control.

 Option to manage and control your own encryption keys to help meet compliance needs.



Increase visibility and control privileged access to your data that's logged and auditable

Customer Lockbox and privileged access management in Office 365 can help you put appropriate limits on access, with greater oversight and audit trails.

Customer Lockbox enables you to control access to your Office 365 data by Microsoft service engineers during service operations, while privileged access management enables you to control privileged access by your tenant admins. Both features enable organizations to enforce:



Zero standing access

This means that there is not standing access to data, and when access is required it is at the bare minimum.



Just in time and just enough access

When access is granted, access is scoped for a specific duration of time, and for the specific task or activity.



Privileged workflow

All access requests go through a privileged access workflow, with requests requiring approvals and having significant oversight.



Logging and auditing

Review and audit privileged access requests, approvals, and other related information.

Customer story

EMCOR



Enabling Customer Lockbox is a must for EMCOR because it helps us meet our customers' requirement that we control access to their data.

Peter Baker
Senior Director of IT, EMCOR Group



Customer story

Shell Oil



Data Governance in Office 365 really enables us to automate and give that power back into the business.

Vivek Bhatt

Technical Design Authority, Shell Oil



Chapter resources

Learn more about the tools that can help you protect and govern data.



In this interactive guide, you'll see how advanced data governance in Office 365 can help you retain or delete sensitive information as needed, easily classify content across Office 365 services, and define policies to ensure compliance.



Microsoft uses some of the strongest encryption protocols in the industry to provide a barrier against unauthorized access to customer data.



In this interactive guide, you'll see how privileged access management in Office 365 can help you increase visibility into your environment, isolate the use of privileged accounts to prevent unauthorized admin activity, and gain insights into how administrative accounts are being used.



Privileged Access Management in Office 365 enables organizations to enforce Zero Standing Access for any user (admin) within the customer's tenant.





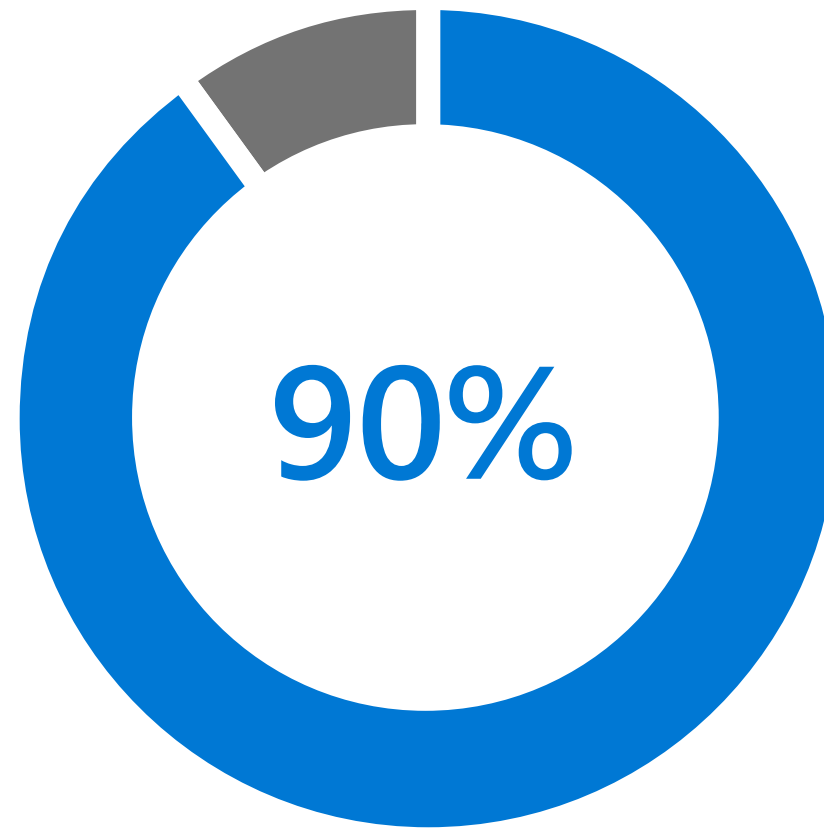
2. Identify and take action on critical insider risks

Quickly and intelligently identify the risks from inside your organization, and take immediate steps to take action on them.

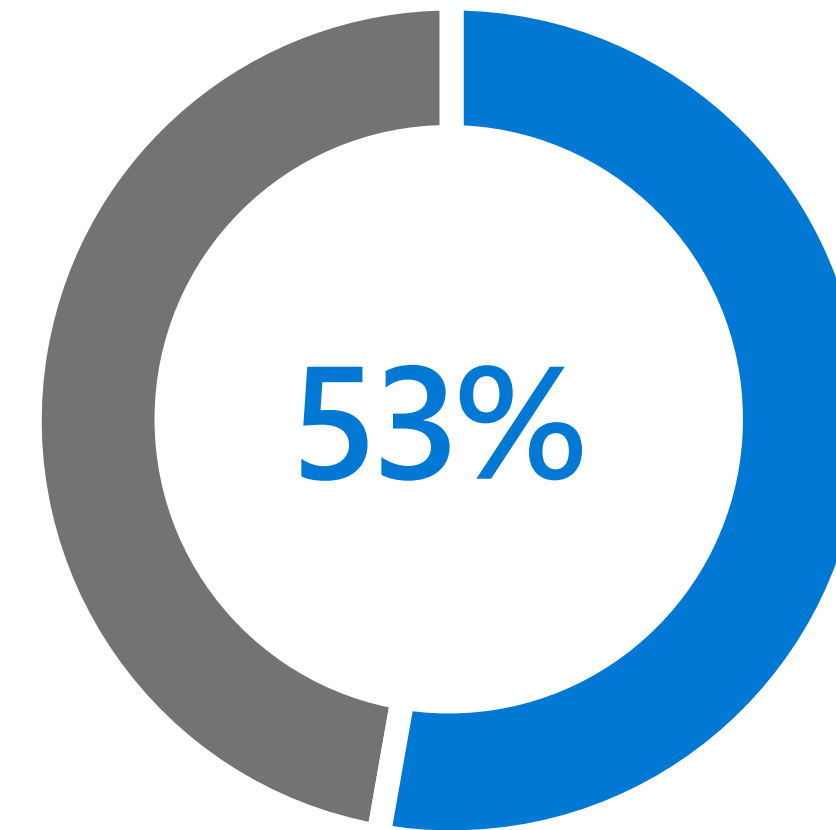


One of the largest concerns within an organization today is insiders inadvertently or maliciously violating internal policies such as IP theft, leakage, or data harassment.

In addition, as employees leave the company, change roles, or move between compliance boundaries, data governance needs to be strictly monitored through controlled access.



90% of companies feel they are vulnerable to insider risks.³



53% of companies confirmed insider attacks against their organization in the last 12 months.³

³ Cybersecurity Insiders, [Insider threat risks 2018](#)

Establish a program to protect against and detect insider threats

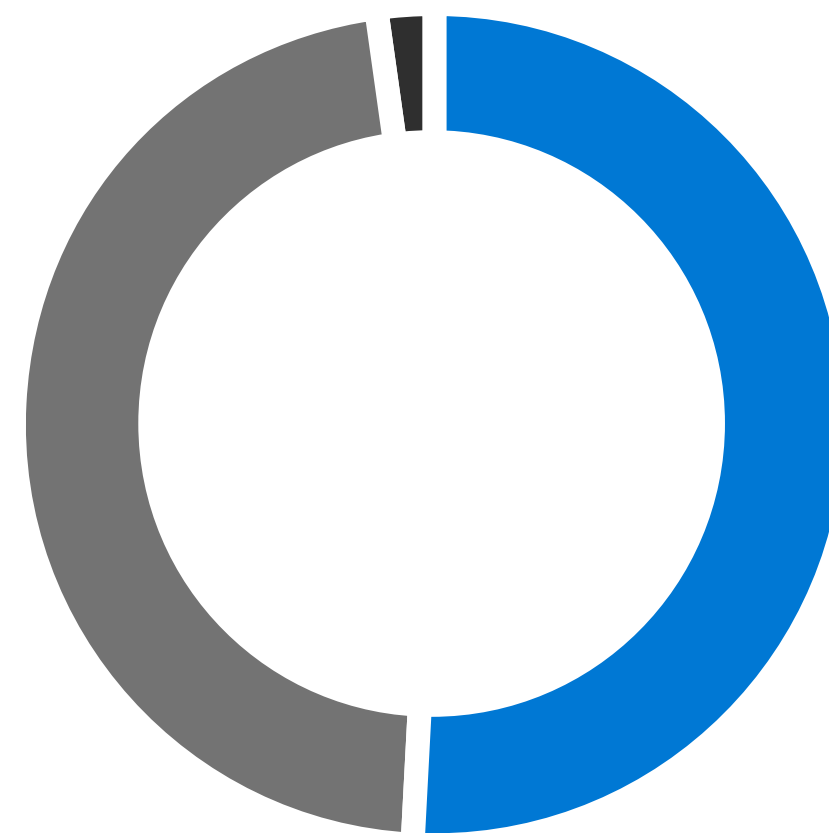
Correlate multiple signals, from activities to communications, to view and manage alerts on potential insider risks and take remediation actions.

Proactively monitor and address data access governance issues when employees leave, change roles, or move between compliance boundaries.

Scan company-managed email, chats, and social accounts to ensure compliance with corporate code-of-conduct policies and external regulations.

ITDMs are equally concerned about malicious and accidental risks

What type of insider threats are you most concerned about?



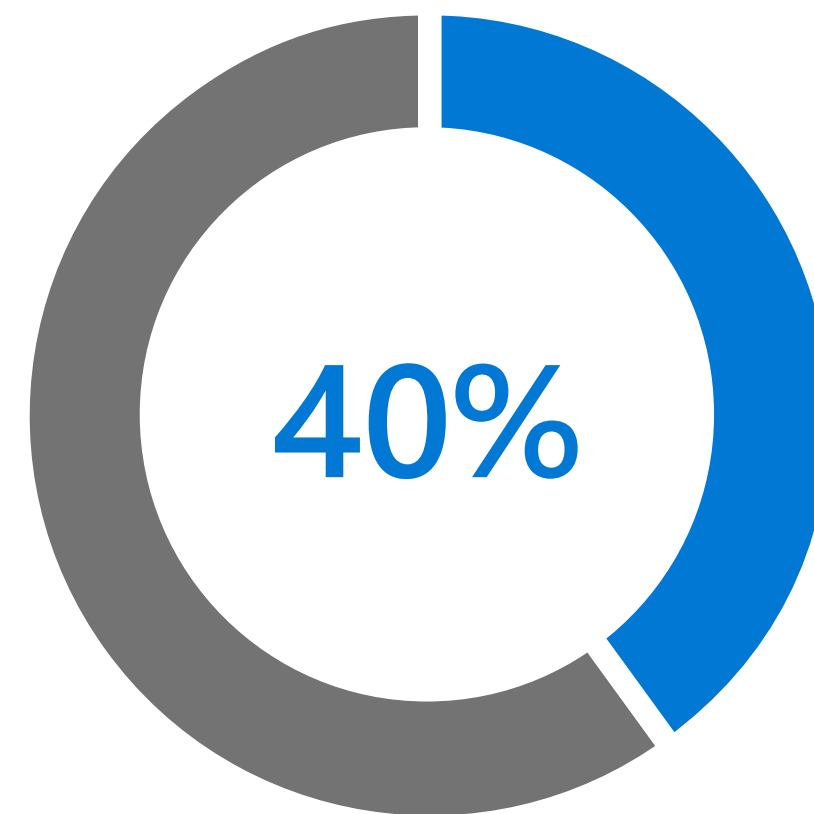
- 51% accidental/unintentional insider
- 47% malicious/deliberate insider
- 2% not sure

Use technology to create controls against insider risk

Establish privacy controls for user anonymity, exploring content, and managing how information related to policy violations is shared within your organization.

Access just-in-time granular control over privileged admin access to sensitive data or critical configuration settings.

Create flexible controls over external recipients' access to encrypted emails including the ability to revoke message and apply expiration dates.



40% of global information workers ignore or go around their company's security policy because they believe it's more efficient for getting work done.⁴

⁴ Forrester, [Harden your human firewall](#)

Chapter resources

Learn more about the tools that can help you identify and take action on critical insider risks.



In this interactive guide, you'll see how advanced data governance in Office 365 can help you retain or delete sensitive information as needed, easily classify content across Office 365 services, and define policies to ensure compliance.



Microsoft uses some of the strongest encryption protocols in the industry to provide a barrier against unauthorized access to customer data.





3. Quickly investigate and respond with relevant data

Collect and process content, intelligently analyze unstructured data, and make better decisions to reduce the amount of data for review.



With the explosion of data in most modern organizations, finding the data you need when you need it is more challenging than ever.

Whether you're handling litigation, internal investigation, or a regulatory request or policy obligation, you need to be able to find relevant content, refine that content, and then prepare that content to be handed off to the requesting body in an efficient and effective way.

Find the information you need, when you need it, effectively and efficiently

Microsoft 365 provides rich, built-in, suite-wide tools for search and discovery, to reduce your risk and exposure of multiple copies of data in multiple places.



Reduce risk with archiving and holds on data in place.



Reduce cost with advanced analytics.



Review and annotate prior to export.



Handle situations beyond litigation, including DSRs, investigations, and more.

20x ↗

rise in average data per custodian.

85x ↘

reduction in the cost per custodian with eDiscovery.

3. Quickly investigate and respond with relevant data

Support continuous compliance with comprehensive audit logs

Microsoft cloud services provide audit information and reports to help you more effectively manage user experience, mitigate risk, and fulfill compliance obligations.

Auditing and reporting features help track user and administrative activity, such as changes made to Exchange Online and SharePoint Online tenant configuration settings, and changes made by users to documents and other items.



Set comprehensive coverage across Office 365 services.



Get a unified audit log search and alert experience.



Create alerts based on organization-specific criteria.



Audit logs and alerts give you comprehensive coverage:



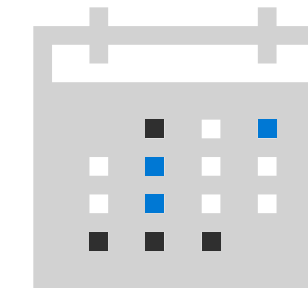
15+

Microsoft 365
services



90+

operations



250+

billion events
per month



Customer story

Discovery Communications

Discovery Communications creates some of the most compelling and recognizable content on television today. Discovery was intrigued with all the key workloads in the Office 365 E5 suite but found security through Advanced eDiscovery and ATP to be worth the price alone.



Chapter resources

Learn more about the tools that can help you quickly investigate and respond with relevant data.



In this interactive guide, you'll see how Advanced eDiscovery builds on existing eDiscovery capabilities in Office 365 to help you efficiently collect and process content, intelligently analyze unstructured data, and make better decisions to reduce the amount of data for review.



4 steps for achieving a forward-thinking compliance strategy



4. Simplify compliance and reduce risk

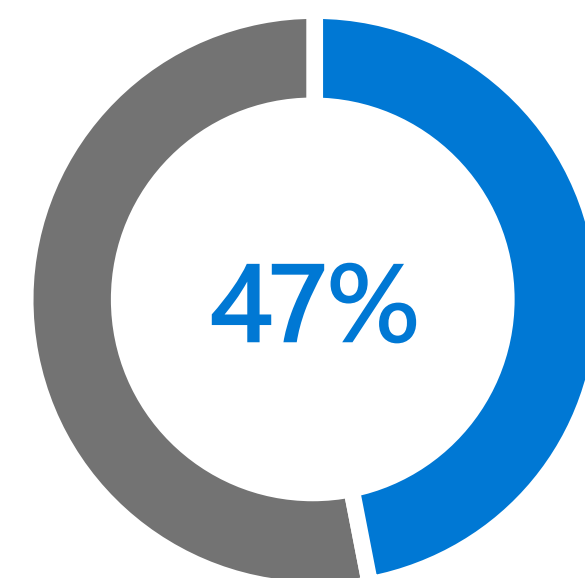
Simplify your compliance journey with ongoing risk assessments, actionable insights, and streamlined compliance workflow.





Managing compliance is complicated, and organizations face many different challenges:

- Multiple standards that are constantly evolving
- Shifting regulatory landscape
- Variations by industry and country



47% of executives were unsure what data compliance standards applied to their organizations.⁵

Compliance regulations are often difficult to navigate, especially for multinational organizations. The requirements can be complex to interpret, difficult to track, and labor-intensive to implement—and the challenge is even greater for regulated industries such as healthcare and financial services.

Not only are there numerous standards and regulations, but they are constantly changing, making it difficult and expensive to keep abreast of international electronic data handling laws. Microsoft 365 can make all of this easier.




⁵ Microsoft GDPR survey—November 2017

Shared responsibility in the cloud
















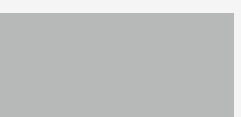


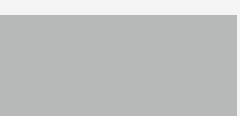
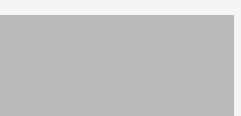
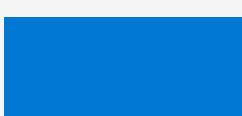







When your IT is only on-premises, you have complete responsibility to protect your data and implement any controls needed to be compliant with applicable regulatory standards. When you use cloud services, you can lessen your burden—sometimes considerably—because the cloud represents a shared responsibility between you and your cloud service provider.

For example, if you use SaaS like Microsoft 365 or Office 365, Microsoft helps you take care of the majority of the controls, including physical infrastructure and networking.

Shared responsibility model:

-  **Customer management of risk**
Data classification and data accountability
-  **Shared management of risk**
Identity & access management
End point devices
-  **Provider management of risk**
Physical networking

 Cloud Customer  Cloud Provider

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & data accountability				
Client & end-point protection				
Identity & access management				
Application-level controls				
Network controls				
Host infrastructure				
Physical security				

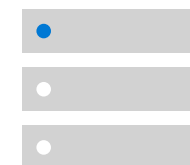
Manage compliance, all in one place

Assess and implement data protection controls, all in the same place. When you take actions, you can see your scores improve in real time.



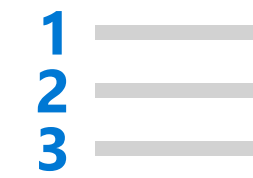
Ongoing risk assessment

Continuously assess, improve, and monitor your compliance effectiveness with a risk-based score that automatically detects implemented controls.



Simplified compliance

Use built-in workflow management tools to assign, track, and record compliance activities and evidence across internal teams.



Actionable insights

Connect regulatory requirements with technology solutions and provide recommended actions with guidance to implement and test controls.



Customer story

Abrona

See how Dutch healthcare organization Abrona is using Microsoft technologies such as Compliance Manager and Azure Information Protection to prepare for GDPR.



Chapter resources

Learn more about the tools that can help you simplify compliance and reduce risk.



In this interactive guide, you'll see how Compliance Manager can help you perform ongoing risk assessments of your organization's Microsoft cloud services usage, gain actionable insights, and simplify compliance by streamlining processes to meet complex obligations—all from one place.



In this whitepaper you'll learn about data protection compliance challenges, the importance of control frameworks, the concept of shared responsibilities and key capabilities of Service Trust Portal and Compliance Manager.





Get started

©2020 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.