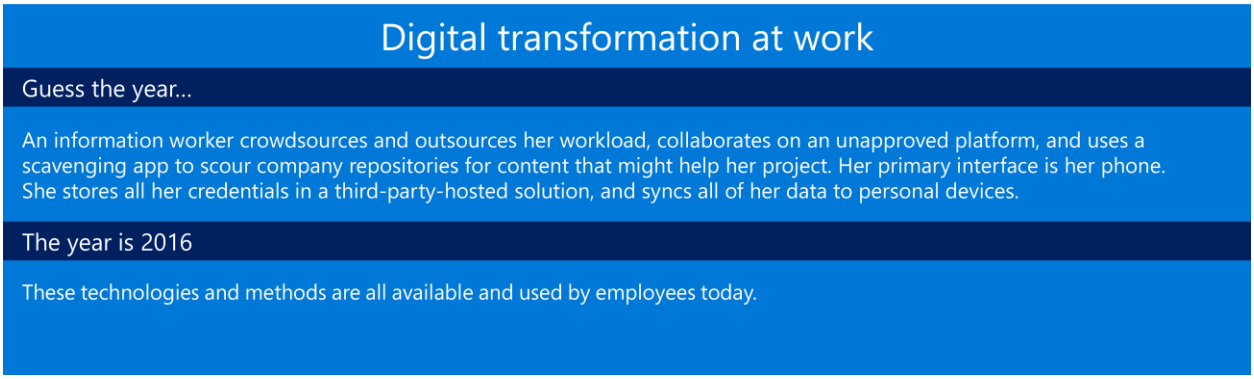
Changing our approach to information security at Microsoft

All businesses are becoming digital businesses, says Microsoft CEO Satya Nadella. To move forward, organizations of all sizes, in every industry, are pursuing transformation with digital technology. And as organizations embrace this digital transformation, their employees' ability to easily yet securely find and share content is crucial. Why? It's what empowers them to be innovative and creative at speed—two ingredients necessary for a successful transformation. However, these new demands create new risks. For this reason, organizations like Microsoft are changing their approach to information security, and fast.

As in other organizations, an increasing number of Microsoft employees are collaborating and managing content in the cloud, using their own mobile devices and connecting to third-party services using the Internet. They collaborate using platforms and services outside of the traditional corporate boundary of a firewall, extending into services that may or may not be centrally controlled by Microsoft IT. This collaboration trend affects every modern business and industry. In fact, analysts estimate that about 50 percent of the technologies adopted in a typical organization aren't selected by its IT organization. Rather, individual business units and workers make these decisions and may or may not engage IT in the process.

This digital transformation gives people the ability to easily collaborate—and to find and share content—and it enables new types of innovation and creativity. It also increases people's effectiveness and productivity at work. But along with its many positive effects, the digital transformation creates a security challenge. As soon as content leaves systems that are under an organization's control, it creates a potential security risk.

The traditional security approach—focused on securing internal systems where content is created, stored, and transported—is no longer sufficient. To transform successfully, we must think differently about information security and the methods we use. This is an urgent need. Because collaboration effectively changes where a business stores its content, it's imperative to use new ways to protect it regardless of where collaboration occurs. This means moving to a model that accounts for the flow of content, protecting content no matter where it exists, and signaling to the employee the security classification level of the content and its intended audience—both inside and outside the corporate firewall, on and off company-controlled systems.



Helping this effort, Microsoft Office includes new technologies that help discover and secure content. For example, among other capabilities, Microsoft Office Delve lets employees evaluate the security of their shared content, and minimize chances of sharing it inappropriately—commonly known as oversharing. Delve gives each employee a view of all of the content they have shared or have access to, and shows who else has access. If an employee discovers that they've overshared sensitive content, they put more access restrictions on it. Azure Information Protection—available for the Office client—lets employees classify their content, label it according to sensitivity, and apply encryption and usage rights as needed that persist even when the content leaves the organization boundary. Microsoft Teams, currently in preview, is a new chat-based workspace in Office 365. It brings together people, conversations, and

content—along with tools that teams need—so they can easily collaborate in a secure way. It includes data encryption, both at rest and in transit, and multi-factor authentication. New applications, services, utilities, and features like these are valuable additions to our security toolbox.

Improving collaboration and productivity

Digital transformation describes a major change in how organizations use information and technology, so that workers can be more productive and collaborative regardless of technical platform. This isn't an incremental update—it's a disruptive break in the way content is created and used.

Employees used to create content on intranet-only applications. Today, however, they often use a wide variety of consumer-oriented apps with varying levels of security for business purposes. The following trends and technologies are at the heart of this potentially risk-prone transformation:

- **Social workflow.** Crowdsourcing, mass collaboration, collaborative authoring tools, "no email" campaigns, external peer-to-peer communities, and unstructured processes are now mainstream.
- **Ubiquitous connectivity.** As we approach a device-agnostic, always-on state, conversations flow across multiple devices, and real-time interaction is the norm.
- **Exponential content growth that often transcends organizational boundaries.** Modern data analysis platforms can obfuscate origins and may collect content from internal and external sources to display a consolidated, informative view.
- **Abundant, loosely connected, and sometimes free technology.** Business units no longer exclusively source technology through IT, and they often use free third-party solutions outside the organization's control. Device use expands to include visualization platforms and wearables. Most are no longer controlled through domain-based architecture. An employee's identity is the new boundary.
- **New ways of collecting, processing, and storing data.** Artificial intelligence, machine learning, and bots are becoming mainstream. They give our employees an aggregated view of content. Natural language systems, smart advisors, digital dexterity, augmented reality, and human augmentation are on the horizon.

Digital transformation is beneficial in many ways. It helps engage customers, empower employees, optimize operations, and transform technical solutions. This is what makes it the focal point of Microsoft CEO Satya Nadella's core companywide initiatives. At Microsoft, business units and individuals are empowered to interact and collaborate with more content to make faster and better business decisions. Many other organizations are making the same change, and industry analysts expect digital transformation to continue growing rapidly.

Securing content, not just systems

Our goal in Microsoft IT is to enable our workforce be more agile and productive, as well as improve data quality for better business outcomes. Although digital transformation aligns with our goal, it means that our long-held approaches to security must be changed. To keep our company content secure, we must update and improve our IT risk and security strategy. And we must start doing it today.

Traditionally we've focused on configuring and hardening technology to prevent unauthorized access to content. This is analogous to putting money in a safe that you can open only with the right combination for the lock. Today, however, our employees collaborate and share content with others in many different ways, and digital assets are no longer confined to the corporate-owned network and systems. They can also reside on workers' personal devices and on public platforms. Without protection, valuable company and personal information may be compromised. So protection must travel with the content, and not drop off when it leaves a secured system. This may sound simple, but it represents a colossal shift in the way we must think about security at Microsoft and in IT in general.

We realize that we can no longer manage content exclusively using IT-controlled technology. We must also manage the content itself. At the same time, we want to give the right person access to the right content. In addition to hardening systems in the traditional manner, we need to use a combination of other methods to do this:

- **Labeling.** Employees label the content itself with watermarks, file headers, code headers, and other notices that indicate with whom it can be appropriately shared. Employees can also classify content according to its sensitivity, for example, *confidential* and *highly confidential*.
- **Signaling.** Signals help employees understand what content they're sharing and with whom they're sharing it. Signals consist of content labels that indicate the sensitivity of the content. Signals also indicate with whom the content will be shared.
- **Rights management.** Applying usage rights makes content available based both on its classification, or business impact, and the role of the person who's trying to gain access to it. The person must have rights to that particular classification of content. An employee classifies content, chooses the audience, and then assigns rights that give the audience access to the specific content. Rights management is effective as long as the system where the content is stored supports it.
- **Assigning roles.** Assigning roles to employees (such as by assigning them to a group) helps us manage the type of content that they can access.
- **Training.** Training is crucial. Employees need to understand signals, how to classify content, and why doing this is necessary. Understanding the reasons for not oversharing encourages employees to follow the procedures to handle their content appropriately.
- **Retention.** Retention policies control how long content is stored. Using them to store content for only as long as necessary—according to regulatory, legal, and company requirements—reduces the amount of content that can potentially be accessed and used inappropriately.
- **Encryption.** This is the most important control that doesn't depend on the underlying system. Encryption follows content wherever it goes. A person must have the encryption key in order to access the content. If an unauthorized person gains access to it, but doesn't have the key, they can't view or use the content. This is the most secure way to protect content that's moved outside of IT-controlled networks and systems.
- **Auditing and logging.** This lets you track where content is located and who has access to it.

Defining a four-way approach to security

In Microsoft IT, we've developed a new model for security that aligns with digital transformation. Even if we don't know what underlying technology was used to create or store the content, we still need to manage access to it. This helps prevent security breaches when employees share and collaborate. Therefore, our new model focuses on securing not just technology, but more importantly, the content itself.

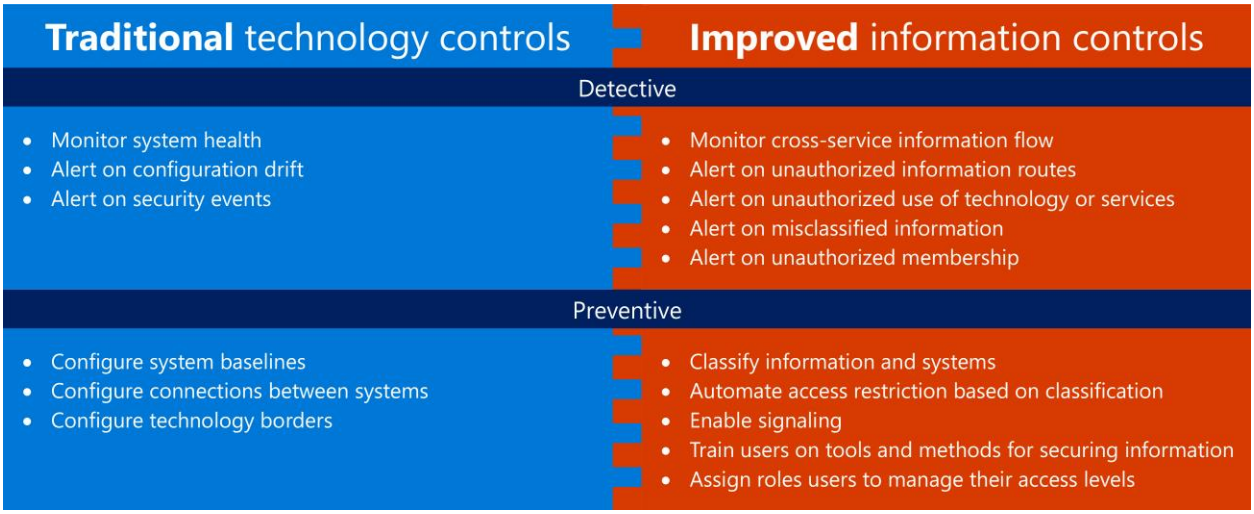


Figure 1. The four quadrants of an effective security strategy. Security experts suggest shifting your efforts into the right quadrant as much as possible, while not forgetting to cover the basics on the left side.

This model delineates a four-way approach to securing content, as shown in Figure 1. The left-side column represents our long-running, legacy approach to security using technology controls. The right-side column represents our new approach that follows content and secures the content itself. The bottom row concerns methods that prevent unauthorized people from gaining access to systems and content, and the top row concerns methods that detect activities.

Using this four-way security model gives us a good way to evaluate the level of information security at Microsoft. It helps us know where we need to improve our methods, and it informs our decisions about what technologies to adopt. It encourages us to move beyond solely relying on traditional approaches like controlling access to the applications that workers use, instead managing the content that workers create and share, regardless of its location.

To have good, robust controls to protect our content, we must use the methods listed in all four quadrants of the security model. This means that we must focus our efforts in the right-side column while continuing to cover the basics on the left. If we continue using the methods in the left-side column only, we'll be at the whim of whomever has control of the content.

The tasks in the right-side column that secure the content itself involve a new set of tasks for IT. These are done in two phases:

- **Preventive.** During this phase, we want to classify, store, and manage access to content. To be successful, we must expand our thinking beyond securing technology—hardening baseline configuration and monitoring technology events—and think about how content is actually created and managed in the organization—identifying instances of unapproved technology, improperly classified content, uncontrolled repositories, and overly broad access. Then we take steps to better secure the vulnerable and important content.
- **Detective.** During this phase, we try to learn what's being shared and what others can see from their perspective. This is the phase where find out where the organization is most vulnerable. Are the organization's secrets well-protected, or are they scattered across unprotected repositories that are available to everyone?

Using new technologies for securing content

In addition to using traditional tools for monitoring and alerting, to help with the tasks of detecting how content is being shared and helping to prevent oversharing, we use detective and preventative technologies available in Office 365:

- **Delve (detective).** Within their Delve sites, employees can view where their content is located in our company repositories and who has access to it. It doesn't matter what application was used to create the content or exactly where on the network it's stored. We encourage employees to regularly review their Delve site and secure any content that's overshared. Groups within the company can also assign someone to search using Delve and find out where the group's sensitive content is stored and who has access to it. If necessary, they can then improve repository security or change how sensitive content is classified to better protect it.
- **Azure Information Protection (preventive).** Azure Information Protection lets employees classify, label, and protect content. Our employees can classify their own content, or we can automate classification for content that has sensitive information—such as credit card and social security numbers—in it. We can specify encryption for sensitive content and define usage rights as needed. Classification labels and protection are persistent, regardless of where content is stored or who has access to it. Also, when Azure Information Protection has been applied, employees can see who has access to their content and where it's located. This is particularly useful when content leaves the organization boundary.
- **SharePoint, OneDrive for Business, and Exchange (preventive).** For business reasons, Microsoft employees often share content with others both inside and outside the company. Our sharing sites—SharePoint and OneDrive for Business—give signals to our employees that guide their sharing choices based on the sensitivity of the content stored on the site. Site owners determine which signals to display. These sites can be secured so that content is only accessible to specific individuals or groups. In addition, Exchange signals employees when they address a message to a person outside of Microsoft or there is sensitive data in the email.
- **Microsoft Teams (preventive).** It gives teams a place to collaborate that's secure and reduces the risk that they'll share content on non-secure platforms. It's a chat-based hub that gives teams access to everything they need to work together right in the app. Microsoft Teams includes Office 365 enterprise security and compliance features, broad compliance standards support, data encryption at all times, at-rest and in-transit, and multi-factor authentication for enhanced identity protection.

Partnering with our employees to secure content

As we work on the challenge of securing content, one of our most important goals is to create a partnership with our employees. We need them to accurately describe how they want to collaborate, and what will help them be effective and efficient in their work. In turn, we need to respond with elegant solutions that balance collaboration and security needs. Further, we must train employees how to keep their content secure—and help them understand and respect this balance, so that they won't try to bypass the security measures. When they do, we need to be aware of it, so we can encourage them to use more secure methods to protect content.

The following table summarizes our current information security goals and approaches as we partner with employees to address the new security challenges of the digital transformation.

Table 1. Goals and approaches to securing content

Improved security goal	Approach
We provide usable solutions that support all collaboration workflow within the organization. The solutions are simple, so that employees are less likely to circumvent them.	Work with employees to understand their collaboration needs and meet them. Set up SharePoint Online, OneDrive for Business, and Exchange Online with Groups and Rights Management. Encourage employees to set up Teams and Groups for collaborating on projects.
We use mechanisms to detect content flowing through unauthorized technologies.	Watch for known third-party service connections originating from the network boundary, and scan workstations for third-party clients facilitating unauthorized data transfer.
We know the value of each content item, where it's located, and who has access to it.	Establish standards across the organization for keywording, content classification (restricted/unrestricted), and people classification (group names and definitions). Establish what repository technology will be used and set up repository locations. Train our employees on these tools.
All employees classify their content using an established standard.	Train employees on Office Rights Management and Azure Information Protection. Encourage them to use these tools during the content creation process.
All collaboration workflow and associated technologies display the content's classification and list the people who have access to it. Employees can see both the classification and the audience to ensure they match to reduce oversharing.	Educate employees on the best methods for sharing, collaborating, and managing content in their communications and projects. Make sure that they know how to classify content and how to assign usage rights to it. Then check to make sure that they're are doing this according to the established standards.

Looking to the future

We expect digital transformation to continue growing within Microsoft and other organizations around the world. Empowering employees to use and share content in new ways gives them insights so they can achieve more in their work. According to Satya Nadella, organizations that succeed with digital transformation will be more engaged with their customers, optimize how they run their operations, and transform their products and services using digital content. Microsoft is actively working on technologies that support this, while helping organizations keep their content secure. Delve, Azure Information Protection, and Teams are some examples of these new Microsoft technologies.

For more information

Microsoft IT

microsoft.com/ITShowcase

Satya Nadella: Why businesses should embrace digital transformation, not only to survive – but also to thrive

Azure Information Protection

Data Classification Wizard

Enterprise Mobility + Security

Learn about Office 365 groups

Microsoft Office Delve

Microsoft Teams

Monitoring and protecting sensitive data in Office 365

Office 365 news in September at Ignite—intelligence, security and collaboration