Security & Compliance

Protect and govern your data in OneDrive and SharePoint

Microsoft

Empower your organization with frictionless security

Security is essential to transforming the modern workplace. Change is accelerating, requiring employees to be able to work anytime, anywhere, and from any device. The complexity of modern workplaces is compounded by the expanding range of applications and services across the vendor landscape. Meanwhile, threats to your intellectual property are ever increasing, whether caused by malicious actors or simply human error.

One of the biggest challenges in digital transformation is ensuring security across an organization's entire digital landscape without reducing user productivity. Piecing together many individual solutions can result in a complex security posture that overburdens operations and encourages users to bypass security measures. In this new world where data and users roam free, protecting your information assets requires a new approach.

Microsoft 365 includes built-in security solutions that integrate easily and share insights from the trillions of security signals on the Intelligent Security Graph across the global Microsoft ecosystem. It allows you to reduce the number of security vendors that you manage by unifying security and productivity tools into a single suite that safeguards users, data, devices and applications. And centralizing your collaborative and mission critical content in SharePoint and OneDrive reduces the attack surface while simplifying modern user experiences across Microsoft Teams and the rest of the suite.

As valuable information flows in and out of your organization and threats become more sophisticated, the frictionless technologies native to Microsoft 365 target security risks without slowing down your business. **Act now to secure and control your data.**

Protect and govern your data

Sharing digital files has never been faster or easier. SharePoint and OneDrive are backed by Microsoft 365, protecting your valuable content without impeding end user productivity. Sensitivity labels classify and protect your business-critical data with encryption, content marking, and endpoint data loss protections addressing the critical need to ensure appropriate access to enterprise resources.

You can label SharePoint sites, Microsoft 365 groups, and teams to control device access policies, external sharing, and privacy levels. With autoclassification, you can scale document protection without requiring users to classify files. Microsoft 365 can identify sensitive content and auto-label it based on industry and regulation-specific templates or your custom business rules.

You can apply retention labels to regulated and critical content to prevent untimely deletion, mark content as a record, or trigger content disposal, so you keep what you need and reduce operational costs.

LEARN MORE:

aka.ms/DiscoverSensitivityLabels
aka.ms/DiscoverAutoclassification
aka.ms/DiscoverRetentionLabels

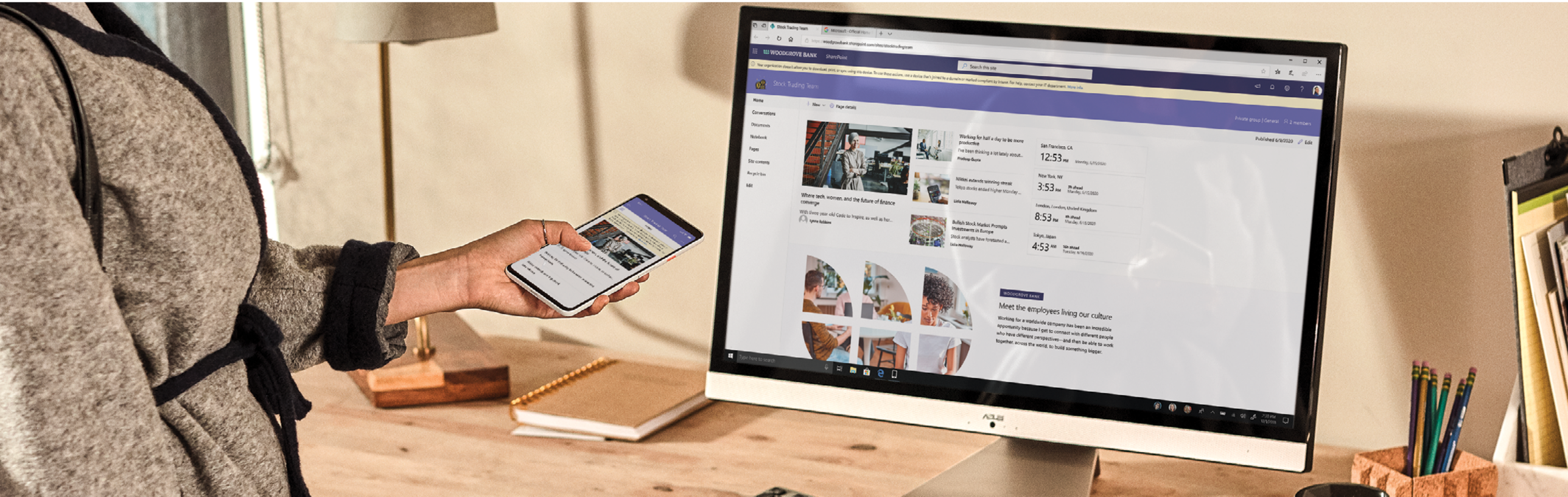
Enable your remote workforce

Today's organizations need a security model that more effectively embraces their mobile workforce and protects devices, apps, and data wherever they are located. You can support your employees and partners working remotely by providing more secure access to corporate resources through continuous assessment and device-based polices.

Microsoft 365 has best-in-class security with device management, allowing, limiting, and even restricting access to specified resources. You can limit access on unmanaged devices to browser-only access without the ability to print, download, or sync, allowing productivity while reducing the risk of accidental data loss. To reduce risk even further, you can block access from unmanaged devices entirely to prevent them from accessing specified resources.

LEARN MORE:

aka.ms/DiscoverDevicePolicy



Control data exposure

OneDrive and SharePoint empower a common sharing experience across your applications. You can decide how users share content and whether to add additional usage, time, or password restrictions. For people outside your organization, you can define what can be shared or prevent external sharing entirely. Sharing policies can be set for the whole organization or for individual sites. By choosing the options that meet your requirements, you can help ensure that collaboration inside and outside your organization can be delivered securely.

Beyond sharing, Microsoft 365 integrates additional frictionless controls – from multifactor authentication to watermarking, shared link expiration, and domain restrictions. You have the tools you need to centrally manage security and access across global teams, and the ability to customize protection policies to meet your unique security and compliance requirements.

LEARN MORE:

aka.ms/DiscoverSharing

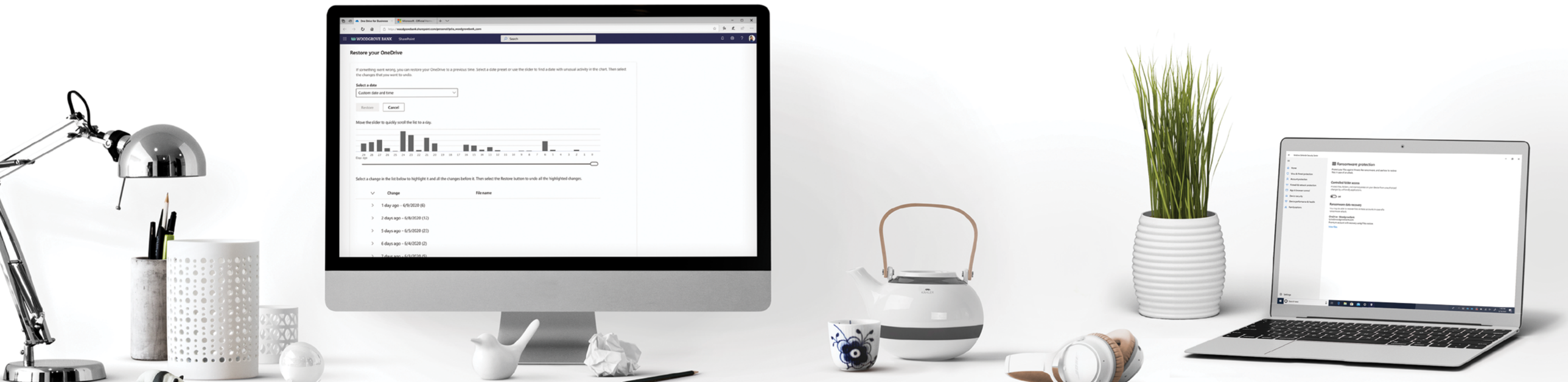
Safeguard against malicious content

Microsoft 365 helps protect your organization against sophisticated threats such as phishing and ransomware. Microsoft Defender Advanced Threat Protection (ATP) provides comprehensive protection by leveraging trillions of signals from the Microsoft Intelligent Security Graph and analyzing billions of emails daily. You can view trends in your sensitive data landscape, monitor policy violations and risky behavior, and fine-tune policies to balance security and end-user productivity.

OneDrive helps users focus on being more productive and helps you worry less about ransomware threats. Versioning helps to protect SharePoint and OneDrive files from ransomware attacks that corrupt data, while recycle bin retention allows administrators to recover files, folders, and list items that have been deleted. Individually, users can use point-in-time restore to rewind the state of their OneDrive to before a malicious attack occurred without requiring IT assistance.

LEARN MORE:

aka.ms/DiscoverRansomwareHandling



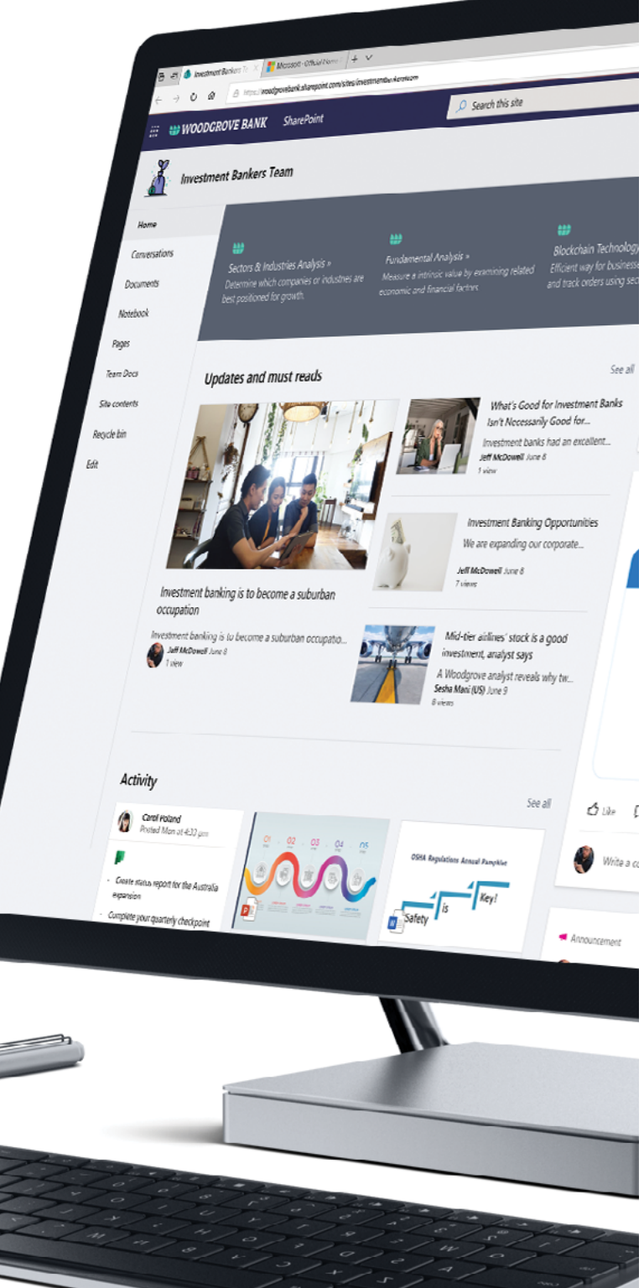
Your data, where you need it

With offices around the world, regulatory requirements and business obligations can lead to complex solutions to meet data residency needs. You can expand your digital footprint to multiple geographies and countries while operating as a single global enterprise with Microsoft 365 Multi-Geo. You can select geographies to store each user's OneDrive files, and where they can provision SharePoint and group-connected sites, all within a single Microsoft 365 tenant. It's easy to move a site from one region to another to meet changing data residency needs. With Microsoft 365 Multi-Geo, you can migrate to OneDrive and SharePoint to eliminate the high cost of hosting separate on-premises infrastructures across the globe.

Your users are now connected to the people and content that matter most, regardless of where they work. You can tailor sharing, security, and compliance policies separately for each region — all from a familiar admin experience.

LEARN MORE:

aka.ms/DiscoverMultiGeo



Information barriers and insider risk management

You can restrict communications among specific groups of users with help from Information Barriers in Microsoft 365. It allows you to segment your data and users to restrict unwanted communication and collaboration between groups and avoid conflicts of interest in your organization. In this way, you can avoid insider trading, comply with FINRA rules, and meet regulations in energy, healthcare, and other industries.

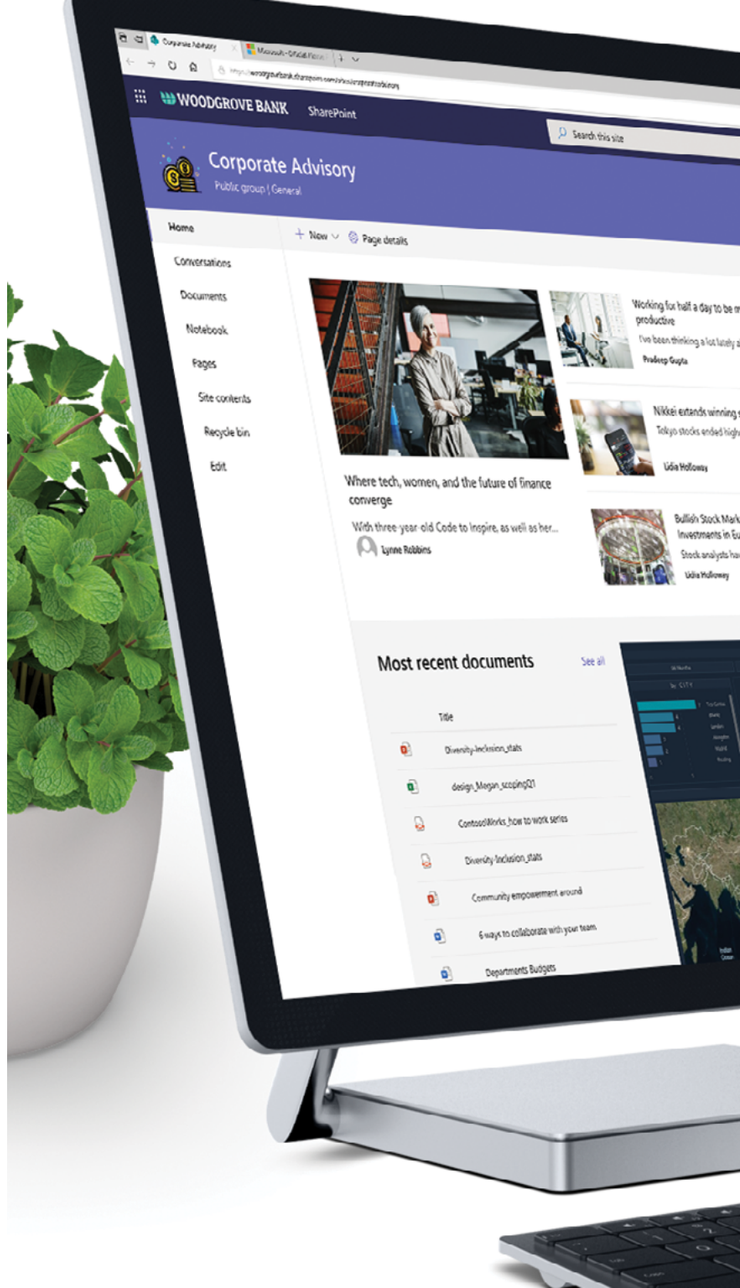
Information barriers lets you create policies to allow or prevent file collaboration, chatting, calling, or meeting invitations between groups of people in your organization. Checks are in place to prevent unauthorized communication.

Microsoft also supports insider risk management. You can minimize internal risks and detect, investigate, and act on unsanctioned activities with your SharePoint and OneDrive content, such as fraud, theft, or sensitive data leaks.

LEARN MORE:

aka.ms/DiscoverInfoBarriers

aka.ms/DiscoverInsiderRiskManagement



Microsoft compliance offerings

Microsoft offers a comprehensive set of compliance offerings to help your organization comply with national, regional, and industry-specific requirements governing the collection and use of data.

ISO International Organization for Standardization

CSA cloud security alliance®

ens Esquema Nacional de Seguridad

FDA U.S. FOOD & DRUG ADMINISTRATION

FedRAMP

DEPARTMENT OF EDUCATION · UNITED STATES OF AMERICA

FIPS 140-2 CRYPTOGRAPHY

DEPARTMENT OF DEFENSE · UNITED STATES OF AMERICA

enisa THE EU CYBERSECURITY AGENCY

AICPA SOC

SEE ALL CERTIFICATIONS:

aka.ms/DiscoverMSCompliance