Ankita Kirti Microsoft

06-10-2020 1(

Top 4 tips to protect your remote workforce with data compliance in OneDrive

Data loss is non-negotiable for your business. Not only can it cost your company huge amounts of time and money—not to mention the impact on your competitive edge if certain IP is compromised—exposure of sensitive information and assets can have enormous legal and compliance implications, too. These worries are heightened by the current business climate, which is seeing more and more people work outside the protective confines of their company's network.

Microsoft is committed to helping protect your company's most critical data as the business world changes before our eyes. For content stored in the Microsoft Cloud, that commitment starts with OneDrive.

Last month we shed light on the Top 5 reasons organizations use OneDrive for data security while working remotely emphasizing on how OneDrive helps with safe sharing and user productivity whilst empowering admins with tools to manage and monitor content wherever its used.

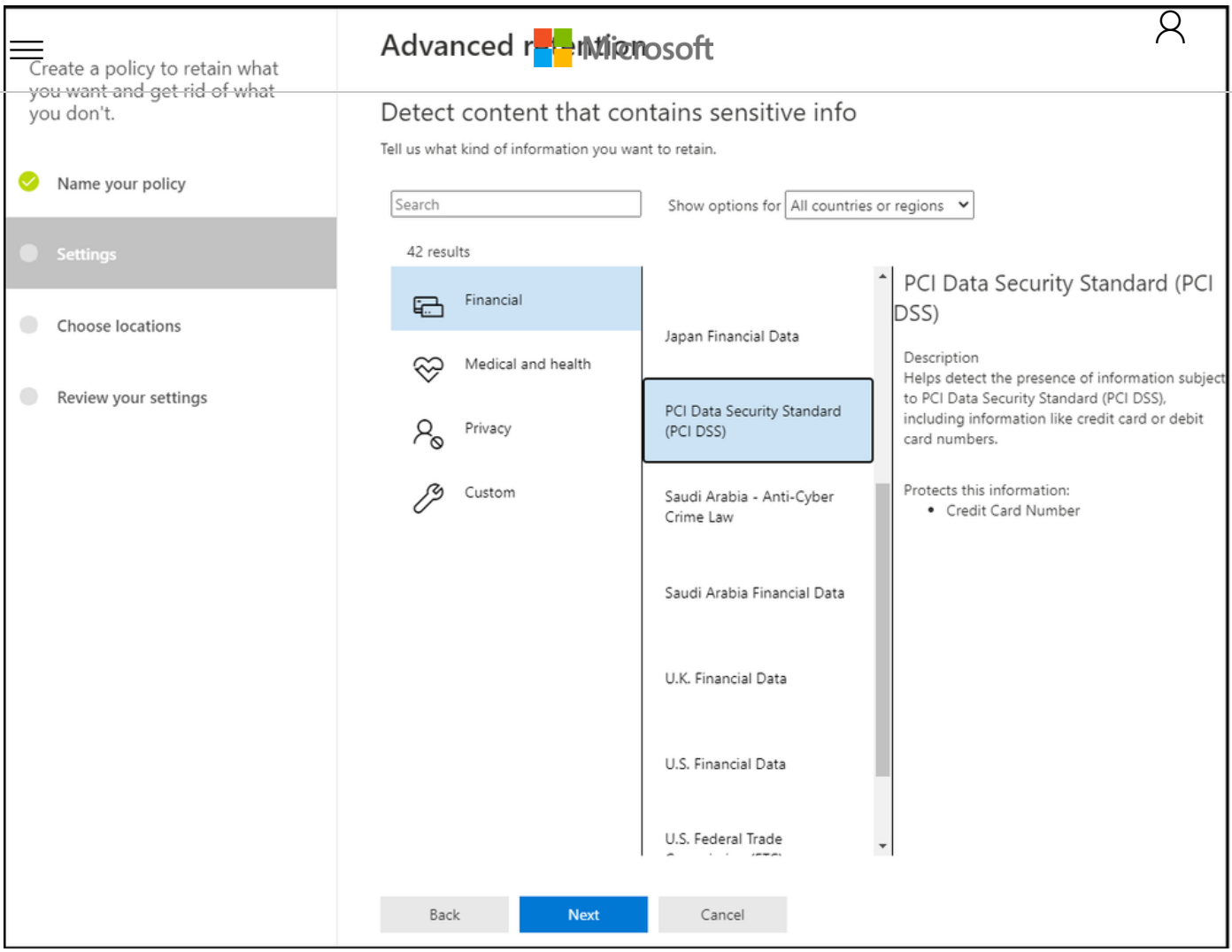
Read on to learn how Microsoft 365 and OneDrive helps keep your data secure and private at the same time reducing the stress on IT during compliance or litigation issues.

Govern Intellectual Property

As your digital data estate increases so does its vulnerability to attacks and leakage. It's an unavoidable fact of today's ever-evolving technology. But with the right governance and Microsoft, you can better protect your information against malware and data leaks. Microsoft 365 and OneDrive together give admins a robust toolset for combating ransomware, retaining critical data, and meeting litigation requirements—all extremely important in today's business environment.

Data retention

Due to compliance and/or legal requirements, your organization might be obligated to keep content for a certain period of time. Data retention in OneDrive is an effective tool for managing and governing the lifecycle of your data. Admins can set global retention policies on all organizational data as well as granular policies on critical users or content, like tax forms, press materials, competitive research, or work visas. They can also implement retention labels for crucial content to impose rules based on set classifications. Admins can automatically apply retention labels to specific types of information or empower their users to manually do the same.



Retain content with sensitive info

Data retention can also reduce risks associated with litigation and security breaches. If a user leaves your organization, files that are subject to a retention policy will be preserved for the duration of that policy with their respective sharing permissions intact. Similarly, admins can set policies that permanently delete old content when it's obsolete or redundant to further minimize the chance of malware.

Lastly, data retention policies and labels support record management for managing regulatory, legal, and business-critical records across your corporate data.

eDiscovery

Built-in eDiscovery in Microsoft 365 helps you identify, preserve, and review data in OneDrive that can be used as evidence during litigation. Admins can search for content related to a case using specific

entire OneDrive accounts being investigated. Analyzing search results using Advanced eDiscovery, which integrates machine learning, predictive coding, and test analytics, admins can further reduce the costs and challenges associated with sorting through large quantities of unstructured data.

As the business world transitions into a new world of work, protecting company data stored in the cloud becomes more important than ever. With malware protections and data retention in OneDrive, admins can help ensure the safety of critical information—even when users are working outside the office. The same is true for legal compliance: as an admin working remotely, you can still find and preserve cloud-based data to save yourself more time and your company more money.

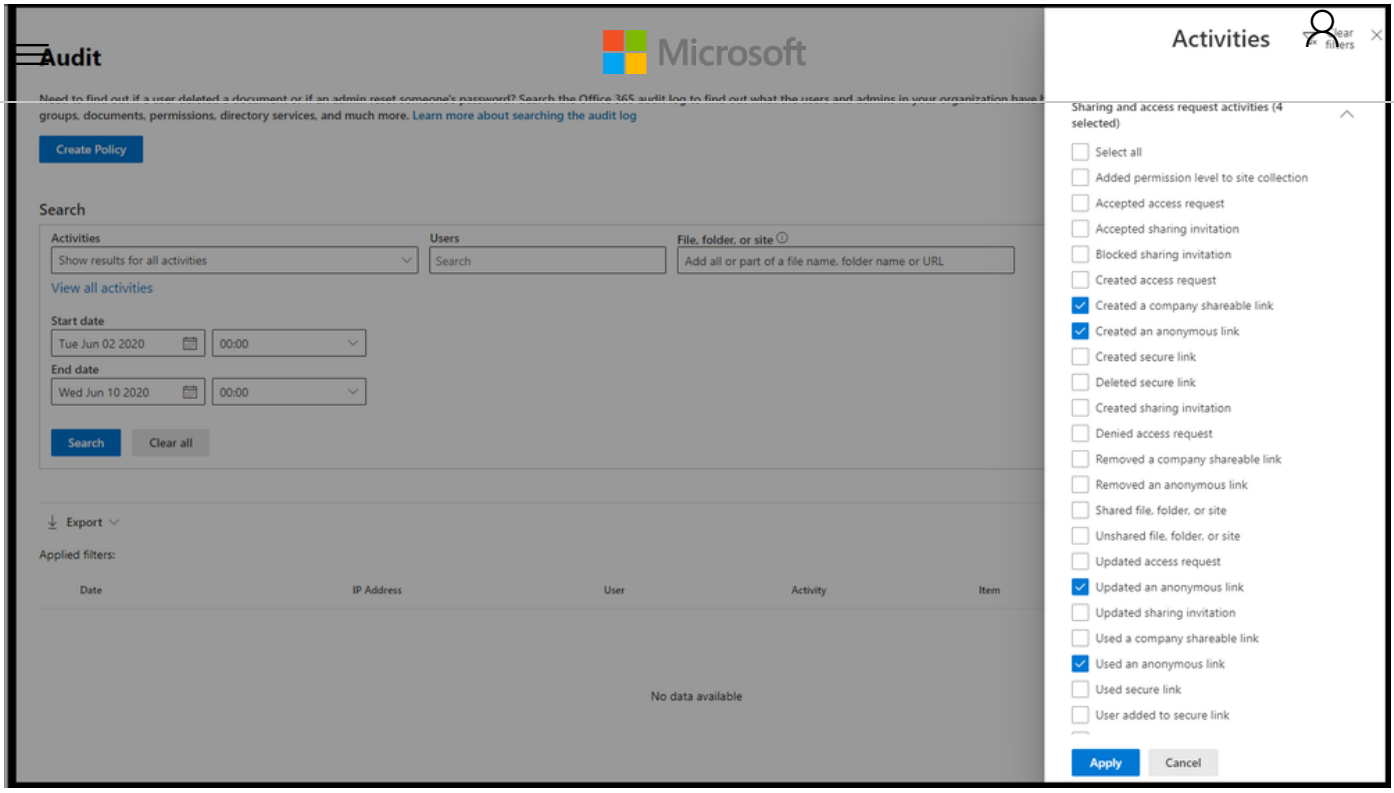
Ransomware

Ransomware attacks have increased dramatically in recent years, causing significant economic damage in their wake. And there's no sign that trend is slowing: by one estimate, ransomware will cost the global economy $20 billion in 2021. Microsoft 365 and OneDrive are designed to help protect your data from such attacks. If your company is infected by ransomware, Windows Defender on Windows 10 and OneDrive will detect and notify you of the attack; provide steps for cleaning your device; and, help you recover lost data with Files Restore**.** Files Restore reinstates your entire OneDrive to a previous time within the last 30 days. This feature can also be used if OneDrive files and folders get deleted, overwritten, or corrupted.

Drive Awareness and Insights

Having the right tools is a good first step toward protecting your company's confidential content. But knowing how users and other admins interact with that content adds an extra layer of security and control. Microsoft 365 offers detailed audit logs and reports that let you trace OneDrive activity at the folder, file, and user levels. That kind of transparency helps protect data while giving your admin team valuable user insights that could influence future IT decisions.

Audit logs and reports in Microsoft 365 Security and Compliance Center surface unprecedented levels of visibility into user and admin activities within OneDrive. Every user action, including changes and modifications made to files and folders, is recorded for a full audit trail. Admins can even audit the users themselves who made those changes, helping them understand how people share, request access, and sync content in OneDrive. Audit logs help uncover admin activities in OneDrive as well, such as changing a network or device access policies. Advanced auditing capabilities add to these auditing efforts with log retention policies and the ability to retain all records for a year to enable forensic and compliance investigations.



Audit log search

Deploying alert policies is another crucial step for monitoring activities performed by OneDrive users. These alerts notify admins when users share a file externally, assign access permissions, or create an anonymous link. Admins can define the alert conditions and policies that will best help them investigate, contain, and respond to any risks of data leakage.

In addition to custom settings, Microsoft 365 Security and Compliance Center also provides default alert policies for OneDrive, such as:

- an abnormal volume of files deleted from a user's OneDrive in a short duration of time
- a high volume of malware detected in files located in OneDrive accounts
- a large number of files shared externally
- unusual amount of activity (e.g., accessing, downloading and deleting files) performed on the externally shared files by users outside of your organization

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.