

Enabling a Safe Data Experience

Safely share information using Microsoft 365 or Google Workspace

Sharing data using cloud services like Microsoft 365 and Google Workspace has become the norm. Such collaboration happens between employees, guests, and 3rd-party contractors - regardless of the user's location and device.

As such data is a lot more accessible in the cloud. Data security technologies, many from the cloud providers themselves, are critical when it comes to controlling this data. These technologies are supposed to assist in avoiding internal data loss, external data breaches, and even ransomware attacks.

However, these data security technologies have become overwhelmingly complicated to manage and to use. To be used correctly and effectively, these technologies require many complex stages; from defining policies, classifying data, determining data locations, and enforcing policies per user groups, to finally reporting and analyzing the immense number of logs generated.

Moreover, on the users' side, the situation isn't simpler. Data protection has turned into a great nuisance, requiring agents to be installed correctly per each endpoint device and for users to explicitly set correct classifications per document and email generated. This overall level of complexity has meant that commonly available data security technologies are practically unusable.

Benefits

• Enable data sharing

Facilitate teamwork with the safe sharing of data across users, devices, and locations. All of this happens transparently, and without the need for the deployment of dedicated agents for each device.






• Faster and easier data security administration

Implement data security without the tremendous effort of setting policies and classifications.

• Protect files from external and internal threats

Proactively protect your most sensitive data from external threats, rogue employees, and unintentional misuse.

Core supporting features

-  Continuous discovery of data usage patterns
-  Software Mines™: decoys deployed in the data-sharing Safe Zones to monitor and control usage of data within these zones
-  Integrated data security training campaigns: increase awareness of data security within the data-security Safe Zones
-  File-GPS™: virtual data tagging and tracking of data's location leaving the Safe Zone
-  File Time Bomb: time-configured voiding of data shared beyond the Safe Zone

ITsMine provides safety and protection to your shared and distributed work environment, along with regulatory compliance. ITsMine's technology overcomes the major challenges and complexities of current data security solutions by automatically constructing "data security Safe Zones" for sharing and collaborating.

Beyond these Safe Zones, data is tracked and controlled to prevent intentional and unintentional misuse of your sensitive data.

With the right approach to protect data within the Microsoft 365 and Google Workspace cloud environments, your employees can easily and safely share information while you prevent data loss and data breaches, and meet regulatory requirements.

The ITsMine Magic

ITsMine's powerful offering includes a 3-layered solution:

- 01 Mapping**
Automatic discovery of clusters where users are sharing information (internally and externally)
- 02 Building and maintaining data-sharing Safe Zones**
Convert your data clusters into Safe Zones for sharing. Ensure that these zones are unbreachable from the outside, and not abused (intentionally and unintentionally) from the inside
- 03 Controlling and tracking files leaving the Safe Zones**
Track and protect access to files that are shared beyond the Safe Zone

