ALTITUDE NETWORKS

SOLUTION BRIEF

Microsoft 365 Integration

PROTECTING MICROSOFT 365 FILE-BASED COLLABORATION

Microsoft has evolved its productivity applications (i.e., MS Word, Excel, PowerPoint, OneNote, and Visio) and its collaboration platforms (e.g., SharePoint, OneDrive) into a single framework that many businesses and government organizations are using today. By providing collaboration platforms with its productivity applications, Microsoft has enabled productivity gains and expanded collaboration beyond just employees. Word, Excel, Visio and other files become readily shareable with external contractors and third-party vendors. Microsoft incorporated setup and file-sharing into its productivity tools which made It is fast and simple to share content and overall requires very little in the way of maintenance or management.

Productivity from Microsoft 365 via a multitude of internal and external groups working together does come with some risks. The simplicity of sharing a file with another employee or an external vendor makes it easy to share with the wrong persons or the wrong files. And once that link is shared it can be shared again and again. Additionally, the easy access is also tempting for those who could sell or use the information elsewhere. Also, it is easy to connect unknown third-party applications to file data to do a specific operation (e.g., convert to a PDF, change file formats, complete a process). Any of these third-party applications can copy, encrypt or delete your data automatically in an uncontrolled manner.

Placing heavy restrictions on Microsoft 365 users is simply out of the question given the organizations' commitment to productivity, operational speed and increased leveraging of contractors and third-party vendors. Given that IT Security groups must secure file-based collaboration but don't own the infrastructure using traditional security tools are going to be too cumbersome to adapt. IT Security must take cloud-native approach to a cloud-based challenge that leverages the latest technology to resolve a modern dilemma.

Cloud-focused detection and correction game plan for Microsoft 365

IT Security must embrace a solution that aligns with Microsoft 365 file collaboration's speed and flexibility but without compromising core security principles. Below is a basic set of requirements for protecting file-data collaboration without impacting it.

1 Auto classify files

The days of asking or expecting folks to label their data so that IT Security would then write policies to categorize and track data risks was a great concept that never happened. If it did, what was there was not consistent to be usable. Technology exists today that can scan logs, compile file metadata and cross correlate with core business phrases and terminology utilizing machine learning and data science to understand the data, its importance and value to the organization.

2 Know thy collaborators

Many organizations end up with a plethora of email addresses, domains, and applications connected to their infrastructure via sharing, copying, attrition (e.g., employees, contractors, vendors), and business transactions (e.g., acquisition or merger) that shouldn't have access to data. Security solutions must be able to correlate who should and who shouldn't have access to file data without manual input.

3 Find it fast

Any solution for file-data collaboration must continuously monitor, identify and surface file permissions quickly. Malicious insiders are operating at internet speed and so should your security of file-based data collaboration.

4 Ignore the noise

Security is overwhelmed as it is now with incoming alerts and trying to sort through tens or hundreds of alerts to figure out which ones to address and which ones to ignore is time consuming and energy-sapping. A solution must be able to differentiate between a marketing document which should be widely distributed and a strategy document that only a few should have access to.

5 Prioritize the problems

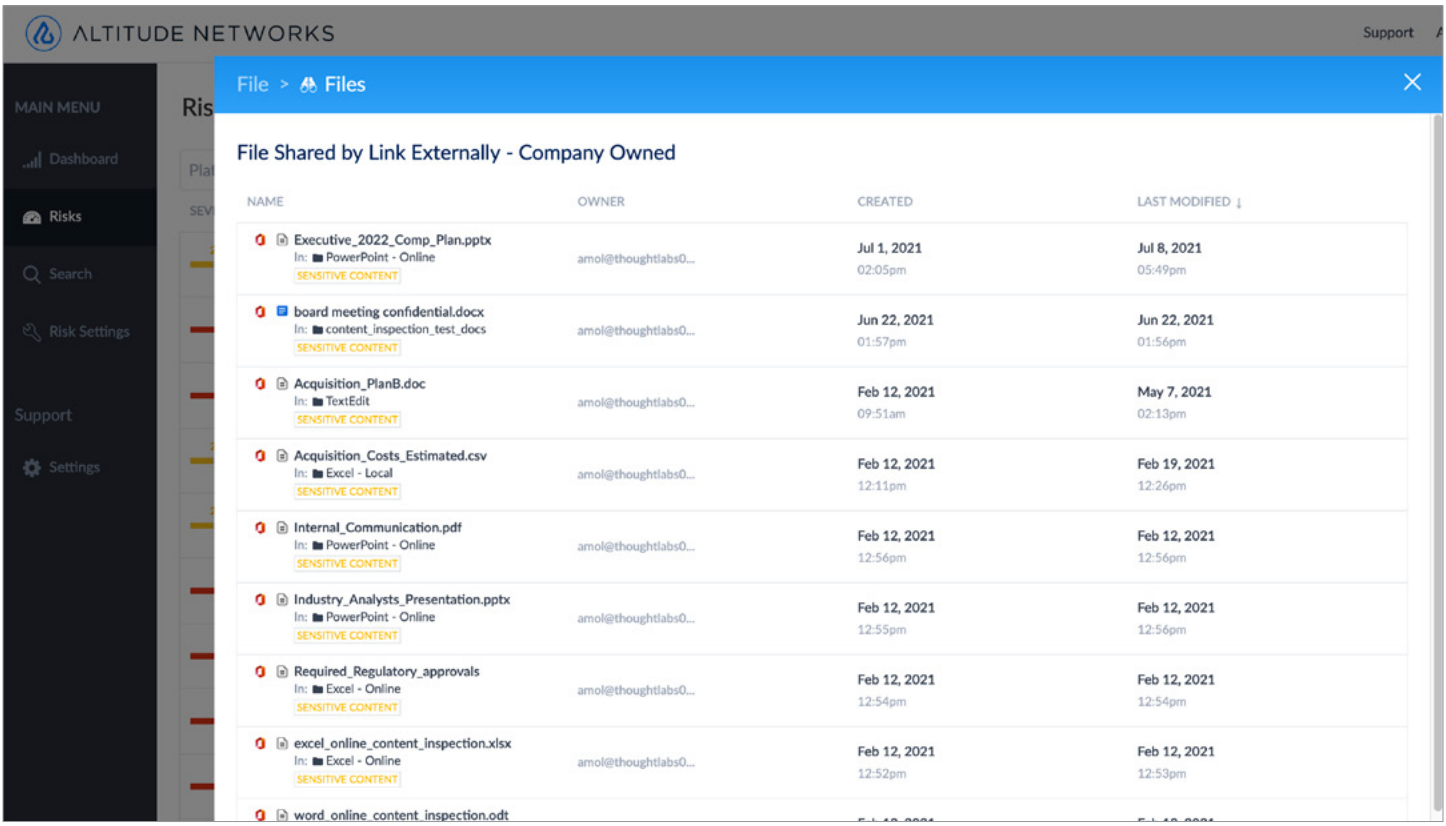
In large organizations with tens of thousands of files, even alerts on just tens of file access issues can overwhelm IT Security personnel who need to review each one. Prioritization of the risks is paramount as time is of the essence in resolving access. Wait too long to resolve the problem and you have a data breach.

6 Direct, simple remediation

Again, alerting IT Security that they have a problem with the idea that they will know how and where to go to fix it is antiquated. Presentation of file access risks along with a direct path to remediation must be delivered in a simple manner that enables IT Security to understand and quickly fix the problem.

Altitude Networks protects against malicious insiders

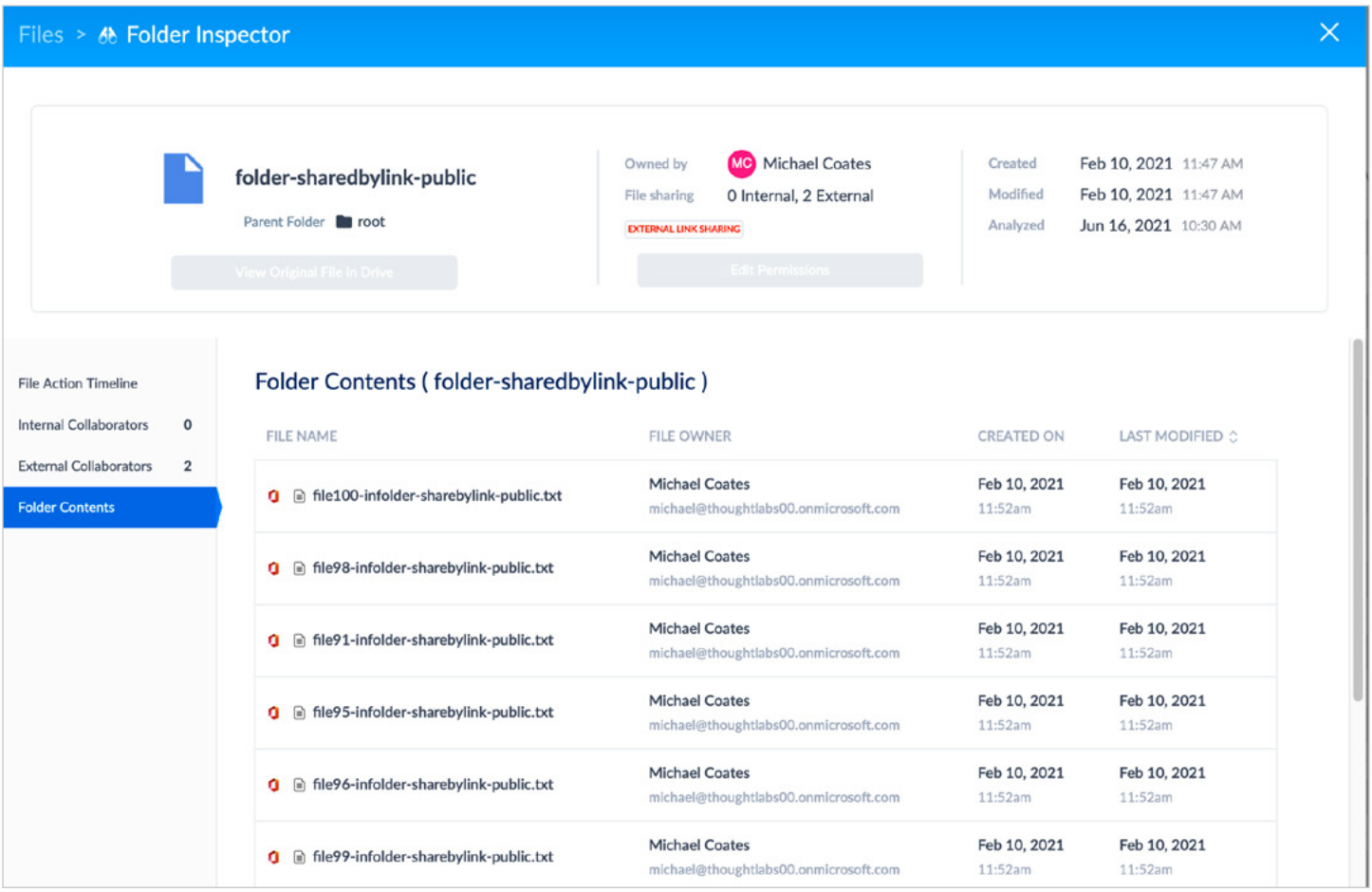
What makes Altitude Networks a unique SaaS DLP solution is its encompassing Risk Engine technology. The Altitude Networks Risk Engine is built upon machine learning and sophisticated data science. It automatically performs file sensitivity classification and identity mapping to build out a framework of sensitivities and access rights. It builds a knowledgebase of organization emails and applications versus external email, domains, and applications to identify risks. It surfaces sensitive files at risk based on sharing permissions, relationships, and behavior patterns and allows you to remediate them directly from its dashboard.



Altitude Networks Dashboard – Risks

The Altitude Networks Risk engine doesn't just categorize the risks, but it also shows you and your teams where to prioritize resolution efforts by analyzing the metadata of every file in your environment and the activity related to them from any user (employees or external accounts) any time. The Altitude Networks DLP Dashboard is designed to enable you and your teams to easily navigable to problem resolution as it presents risks insights by:

- Creator of most risks
- Files with most risks
- Owner of most at-risk files
- External account with most file access



Altitude Networks – Folder Inspector

Each category has risk scores (high to low) to help guide review and remediation. Simple remediation is presented alongside the risk for simple consideration and quick fix.

The solution is lightweight and built with ease of implementation and on-going administration in mind, so that organizations can realize risk mitigation on day one. It is set up to monitor and manage file collaboration permissions in 10 minutes via secure API connectivity to cloud environments.

To find out more about how Altitude Networks helps you and your team against ransomware visit www.altitudenetworks.com