Dropbox

Read Me First: Partner Demand Gen Kit—Advanced team and Content Controls

Dropbox has launched The Advanced Team & Content Controls add-on. AT&CC brings enhanced security and administrative capabilities to Dropbox Business customers.

We've designed a new toolkit to help you offer AT&CC add on for your customers. It includes:

- How to have a conversation with your customers—talking points and questions included
- Emails to send to your customers
- Resources to use with your customers

If you need additional information or support, please reach out to your Channel Account Manager or **partners@dropbox.com**.

Thanks,
The Dropbox Partner Team

November 2020

How to have a conversation with your customer?

What is it?

The Advanced Team & Content Controls add-on brings enhanced security and administrative capabilities to Dropbox Business customers, including:

- Data Protection & Automation
- Visibility & Auditability
- User Lifecycle Management

The add-on's capabilities are powered by BetterCloud.

Benefits?

IT is juggling how to deploy and manage best-of-breed tools like Dropbox to teams, all while protecting data, having the right visibility and remediation paths, and ensuring compliance. In managing their Dropbox deployment, we find 3 main pain areas for our customers:

1. Data Protection
2. Visibility & audit-ability
3. User lifecycle management

Securely deploy, manage, and govern your Dropbox Business deployment with the Advanced Team & Content Controls Add-On.

Feature highlights

- Set up alerts and policies to scan for sensitive data and avoid data vulnerabilities
- Enforce granular policies that align with your organization's approach to security
- Take swift action by immediately transferring document ownership, making files view only, and removing all collaborators on a file
- Search across all Dropbox files and their permissions from a centralized dashboard
- Enable admins to make one-off and bulk actions on files and folders across their team
- Create least privilege roles for Team Admins
- Easily export reports to prepare for audits and gain peace of mind
- Ensure that new captured Dropbox users are added to the right team, with the right level of access

  NOTE: The above feature is our main push for user lifecycle management, as an extension of our Account Capture functionality.
- Save time and ensure compliance with custom automation workflows
- Automate on-boarding and off-boarding user accounts

Target Audience

Dropbox Business ITDMs (Enterprise & Advanced SKUs)

- Minimum 50 users & 1 year term
- Must match Dropbox user counts

Job Titles

- Network Admin
- IT Analyst
- IT Security Manager
- Information Security Manager
- IT Project Manager
- IT Procurement Manager
- IT Manager/Director
- CISO/CIO/CTO

Customer Profile

- IT and information security professionals looking to reduce the overhead of managing Dropbox, a tool they need
- SaaS forward or friendly
- Company size: between 250-1,000 employees

Discovery Qs

	Data protection	Visibility & auditability	User lifecycle management
1 Ask these first	How are you currently managing your Dropbox deployment to ensure sensitive documents aren't getting into the wrong hands? • Is that current process sufficient for your organization?	Would deeper visibility into your Dropbox environment be helpful for you? • Why, and to what end?	How do you currently manage onboarding and offboarding onto Dropbox? What about granting admin rights? [Especially for larger deployments] How does account capture fit into your service request process for Dropbox?

2 What to ask next

What specific compliance policies are you subject to or do you enforce?

- How do you enforce these policies today?
- What happens when you're not able to enforce these policies? How does that impact your organization?

How do you scan content to ensure compliance?

- Is it a manual process, and if so, how much time does it take?
- If you could automate the process, would you? Why?

How are you controlling access to sensitive information, such as PII, PHI?

- What happens if someone gains unauthorized access to this information?
- If you could tighten access controls, would you?

What tools are you currently using to monitor Dropbox activity (CASB/DLP)?

- How satisfied are you with these tools?
- If you could make monitoring Dropbox activity even more seamless, would you? Why?

What does the remediation process look like if a file is shared with someone inappropriately and/or puts company data at risk?

- What might happen if that remediation process gets delayed?
- What would an ideal process look like?

Once you identify a potential threat, how quickly can you respond to it?

- How might a delay in response impact your organization?
- If you could speed up the threat identification and remediation process, would you? Why?

What visibility do you need into your Dropbox tenant?

- Why, and what would that solve for?
- How would not solving that potentially affect your organization? What about for you personally?
- If you could ensure this visibility, would you? Why?

What specific reporting or auditing requirements do you have for Dropbox?

- How do you currently prepare for these reporting needs and audits?

How do you currently review access or sharing controls?

- If you could have greater visibility, would you want that? Why?

What happens if an employee that left the company downloads files from your account?

- Can you track activity like this?
- How would not being able to so affect your company? You personally?

How are you alerted when files are shared externally?

- Why are these alerts important for your organization? What happens next?
- What other alerts might be helpful?

How are you currently managing your Dropbox users, admins and groups?

- If you could centralize that process, would you? Why?

How do you currently control admin access to Dropbox?

- How might having a systematic way of doing so help you?

Are admins able to make one-off or bulk actions to files and folders?

- How might that ability help your users? Admins? You personally?

When employees or contractors join the organization, how do you ensure they have access to Dropbox on day 1?

- If you could expedite this process even further, would you?

How are you currently provisioning/de-provisioning Dropbox licenses when new employees join or leave your organization?

- How much time does the current process take?
- If you could shorten or automate that process, would you? Why?

How are you currently managing Dropbox access when employees move teams or need additional levels of access?

- How satisfied are you with the current process? If you could improve it, would you? Why?

When someone changes roles or leaves the company, how are you removing or adjusting their access to tools and sensitive data?

- How might automating that process be helpful for you?

What is your central user/team directory? Active Directory, Okta, Google, etc?

- How do you currently use your directory in the provisioning process?

How much time do you spend onboarding and off-boarding users?

- If you could reduce the amount of time spent on this, would you? Why?

3 What to listen for

- File scanning to discover: PII, CC numbers, SS numbers, Passport numbers, passwords, AWS encryption keys
- Inspection and detection of content going to Dropbox (DLP or CASB solutions)
- Any data that has specific security requirements, such as PII or PHI that needs special attention
- Visibility of file contents, activities, and events in an admin console
- Reporting on files, activities, and users
- Compliance
- Admin roles
- Custom security policies
- Bulk actions
- Account Capture
- Provisioning licenses
- Team directories
- Onboarding
- Off-boarding

Email Advanced Team and Content Controls Toolkit

Email 1

Subject Line: Data Loss Protection with Dropbox Advanced Team & Content Controls

Hi *(first name)*,

I hope you're well. The reason I'm reaching out today is to share some updates with you.

With our most recent product offering, Advanced Team & Content Controls, we are able to automate user onboarding/offboarding and extend policy based security throughout your organization.

[INSERT CUSTOMIZED CTA]

Thanks,

(partner rep name).

Email 2

Subject Line: Added Security for Dropbox

Hi *(first name)*,

I'd love to set up time for us to discuss how our new Advanced Team and Content Controls can impact your current Dropbox security with these offerings:

- **Safeguard Data:** Scan content, set granular content policy enforcement, and customize alerts with automated remediation workflows.
- **Gain Visibility and Auditability:** Create a single, searchable view of all Dropbox users, groups, file activities, and content settings.
- **Automate Routine Processes: Build custom workflows to streamline manual processes, such as onboarding and off-boarding.**

[INSERT CUSTOMIZED CTA]

Best,

(partner rep name).

Call to Action Guidance

Dropbox

An effective way to qualify leads is to provide a clear Call to Action (CTA) in your email closing. Each email should end with the same CTA that allows leads to indicate if they want to more information. Potential options include:

1. Drive traffic to your company website by adding a hyperlink to your Dropbox Business landing page

2. Create your own Google Request form so leads can indicate they want a call back

3. Create your own Calendly link that integrates with your calendar, allowing leads to schedule a call directly

4. Provide your contact information so a lead can contact you directly