



How is your enterprise using AI Agents? Help us benchmark security and take the survey before November 30 →

# Dealing with Dropbox: Unmasking Hackers with User Behavior Analytics

Published 09/07/2016

Home > Industry Insights > Dealing with Dropbox: Unmasking Hackers with User Behavior Analytics

By Ganesh Kirti, Founder and CTO, Palerra

DropboxBlogDropbox was in the news a few months ago due to false reports of a data breach. Unfortunately, they've made headlines again. Vice reported that hackers stole over 60 million account details for the cloud storage service. This time, the breach is real, and a senior Dropbox employee confirmed the legitimacy of a sub-set of stolen passwords.

Many people keep sensitive documents in cloud storage services like Dropbox, Box, GoogleDrive, and OneDrive, and the latest breach shows that hackers are focusing on online storage cloud services more frequently. This opens the door to huge vulnerabilities if employees are storing sensitive enterprise information in the cloud. From a preventative perspective, security personnel should review their security measures for the following:

1. Require multi-factor authentication to access the application
2. Enforce password strength and complexity requirements
3. Require and enforce frequent password resets for employees

But manual processes and policies are not enough. At minimum, enterprises should look at automating the enforcement of these policies. For example, you may require multi-factor authentication, but how do you ensure that it's required at all times? A cloud access security broker (CASB) continuously monitors configurations to alert security personnel when changes are made, and automatically creates incident tickets to revert security configurations back to the default setting.

How can enterprises prevent further damage if their employees' credentials were compromised in this hack? We recommend utilizing user behavior analytics (UBA) to look for anomalous activity in an account. UBA uses advanced machine learning techniques to create a baseline for normal behavior for each user. If a hacker is accessing an employee's account using stolen credentials, UBA will flag a number of indicators that this access deviates from the normal behavior of a legitimate user.

Palerra LORIC is a cloud access security broker (CASB) that supports cloud storage services that are similar to Dropbox, including Box, GoogleDrive, and OneDrive. Here's a few indicators LORIC can use to unmask a potential hacker with stolen credentials in Box:

1. Flag a login from an unusual IP address or geographic location
2. Detect a spike in number of file downloads compared to normal user activity
3. Detect logins outside of normal access hours for the user
4. Detect anomalous file sharing or file previewing activities

The ability to gauge legitimate access and activities becomes even more important when you consider that many people use the same password for multiple applications. This is highly useful for the recent Dropbox breach. Instead of just protecting Dropbox, UBA helps the enterprise protect any cloud environment that could be accessed using the stolen Dropbox passwords.

If you're concerned that hackers may access your cloud storage environment using stolen employee credentials, you must take preventative and remedial action. Adding a cloud security automation tool prevents a breach by enforcing password best practices, and prevents additional damage after a breach by unmasking hackers posing as legitimate users by flagging anomalous activity.



Share this content on your favorite social network today!



## Latest from CSA



Cloud Threat Modeling 2025



Now Available: STAR for AI Level 2 and Valid-AI-ated for AI



Introductory Guidance to AICM

50% Off

CCSK + CCZT

Cloud Infrastructure Security Training

Cyber Monday 2025 | Learn More →

2026 CISO BUDGET REPORT:

Compare Your Security Spend with 300+ CISOs

Download now

WIZ

Control Framework & Mapping

AICM

Artificial Intelligence Controls Matrix

Now Available! Download Now →

Unlock Cloud Security Insights

Email Address

Sign up

Subscribe to our newsletter for the latest expert trends and updates

Enhance your cloud security skills with CSA's online training options. →



### Corporate Membership

Solution Providers  
Cloud Solution Providers  
Become a Member

### Join as an Individual

Chapters  
Working Groups

### Certificates

TAISE  
CCSK  
CCAK  
CCZT

### Events

Upcoming Events

### About CSA

Contact Us  
Press Releases  
Press Coverage  
Quality Policy

### Our Team

Board of Directors

MICROSOFT CORP.  
EXHIBIT 1054

#### Research

[Download Publications](#)  
[View Working Groups](#)  
[View All Topics](#)

#### Find a...

[Cloud Consultant](#)  
[Cloud Service Provider](#)  
[Trusted Cloud Provider](#)

[Webinars](#)  
[Past Events](#)

#### Education

[Blog](#)  
[Virtual Events & Webinars](#)  
[Training](#)  
[Cloud 101](#)

#### Popular Resources

[Security Guidance](#)  
[CCM](#)  
[CAIQ](#)  
[STAR](#)  
[GDPR](#)

[Management & Staff](#)  
[Careers](#)

#### Legal

[Privacy Notice](#)  
[Terms & Conditions](#)

[Cloud Security Glossary](#)



[Support](#)