Box Account Takeover Protection

Analyze human behavior to keep Box closed to attackers.

File-sharing platforms are a top concern for CISOs

In a recent survey, when asked which platforms security leaders were most concerned would become targets in a breach attempt, file-sharing and storage apps like Box topped the list.

Unlimited storage means unlimited sensitive targets

The Box platform provides unlimited storage to the enterprise. With various departments in a Box customer's organization using the platform for storage, there is a significant amount of sensitive material to protect.

Box provides strong security, but it is one layer

Security teams need greater visibility into Box access. While Box Shield can detect compromised users, it is a singular solution that is not taking cross-platform activity into consideration to enhance detection.

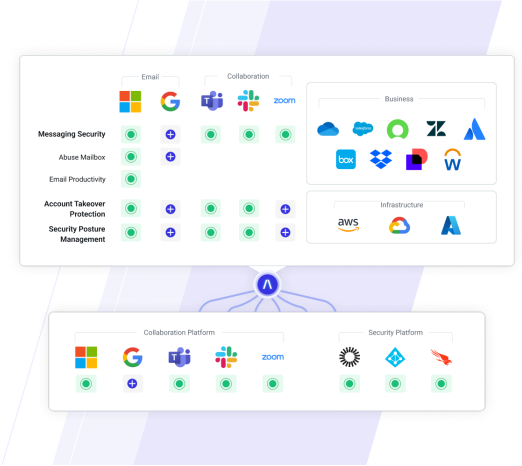
Extend Abnormal Protection Across All Platforms

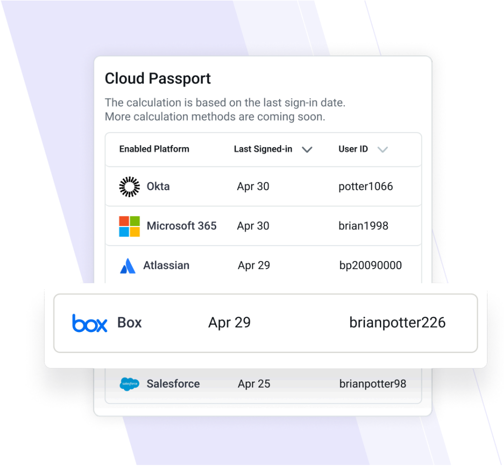
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are a primary concern for Security teams. When considering a breach, what target is more attractive than an organization's primary file storage platform? Box is secure, but considering CISO's concerns around storage app security, Box requires additional protections. To stop attackers from tearing open Box, security teams need an extensible platform that provides consistent visibility and security automation across not only Box but all cloud apps and services for holistic, higher fidelity detection. Abnormal provides that platform.

How Abnormal Secures Box

Simple API Integration

Connect directly to Box with Abnormal's cloud-native API architecture—automatically ingesting and normalizing sign-in signals related to every human in your organization that accesses the Box platform.





Cloud Passport

The calculation is based on the last sign-in date.
More calculation methods are coming soon.

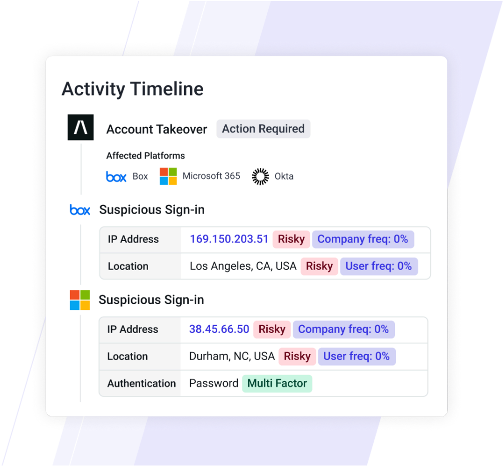
Enabled Platform	Last Signed-in	User ID
Okta	Apr 30	potter1066
Microsoft 365	Apr 30	brian1998
Atlassian	Apr 29	bp20090000
Box	Apr 29	brianpotter226
Salesforce	Apr 25	brianpotter98

Continuous Monitoring of Human Behavior in Box

Build dynamic behavioral profiles for every human in your organization that uses Box, develop a behavioral baseline and automatically detect and analyze anomalous activities that deviate from that baseline.

AI Account Takeover and Response

When suspicious activity occurs, Abnormal Human Behavior AI automatically triggers the creation of a contextual Case populated with Box activity. Each Case is scored based on detection confidence and continually enriched with new activity across all platforms integrated with Abnormal.



Activity Timeline

Account Takeover Action Required

Affected Platforms
Box Microsoft 365 Okta

Suspicious Sign-in

IP Address	169.150.203.51 Risky Company freq: 0%
Location	Los Angeles, CA, USA Risky User freq: 0%

Suspicious Sign-in

IP Address	38.45.66.50 Risky Company freq: 0%
Location	Durham, NC, USA Risky User freq: 0%
Authentication	Password Multi Factor

Try Abnormal Today

See how Abnormal can keep attacks out of your cloud email and connected platforms. Integrate in minutes via API.

abnormalsecurity.com/risk →

Abnormal