

Box Security Events

Uncover threats to your Box data

Challenge

Many security teams lack the ability to distinguish between normal and risky user activity in Box. Creating a shared link to a file may not be concerning on its own, but a watch list user sharing public Box links from a new geolocation after accessing sensitive on-premises data for the first time is. Analysts spend far too much time stitching together disparate logs to answer the question “Is my data safe?”

Solution

Varonis gives you the ability to quickly correlate alerts in your cloud and on-prem environments to user behavior in Box. Search a complete forensics audit trail of Box activity to quickly see the who, what, when, where details.

Save threat hunting queries that correlate risky Box activity with other Varonis data streams to surface potential attacks such as:

- Shared links created by disabled or stale AD users
- Permission changes on highly sensitive folders
- Box file downloads by users who triggered brute-force or geohopping alerts

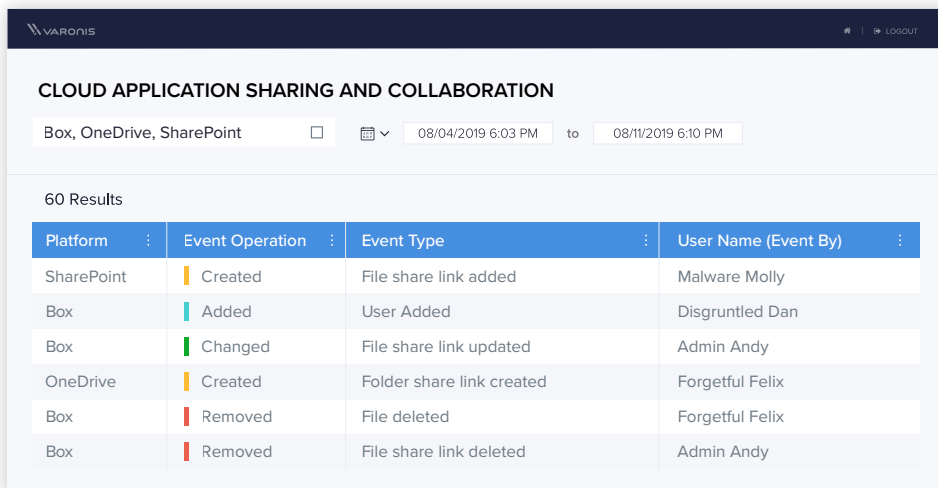
Customer Success

“Varonis has given us the ability to respond faster.

It used to take us 25 minutes and three teams to hunt down and fix a problem. Now one user can solve the same problem within five minutes.”

Chief Security Officer
U.S. County

[READ THE CASE STUDY >](#)



The screenshot shows the Varonis interface for "CLOUD APPLICATION SHARING AND COLLABORATION". It displays a search for "Box, OneDrive, SharePoint" with a date range from "08/04/2019 6:03 PM" to "08/11/2019 6:10 PM". The results show 60 items. The table below lists the first six results.

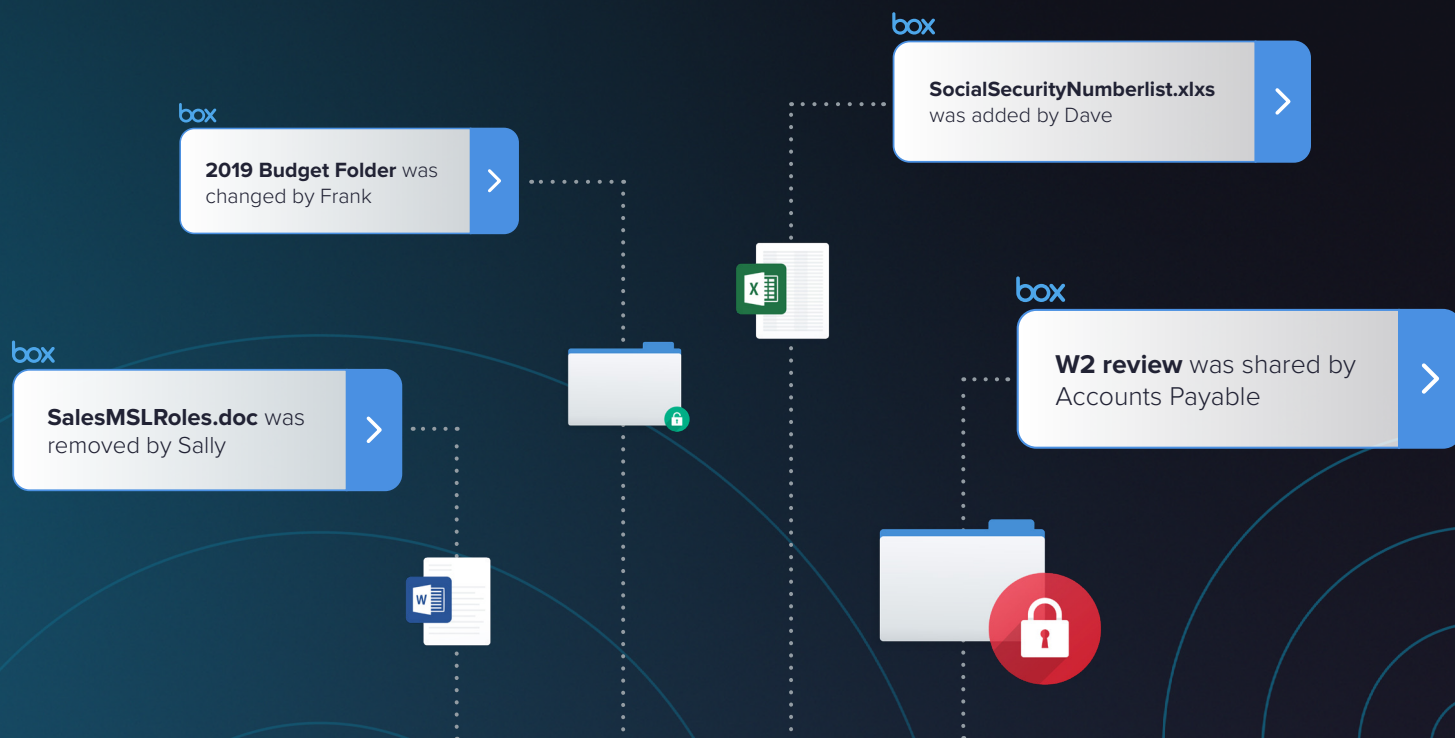
Platform	Event Operation	Event Type	User Name (Event By)
SharePoint	Created	File share link added	Malware Molly
Box	Added	User Added	Disgruntled Dan
Box	Changed	File share link updated	Admin Andy
OneDrive	Created	Folder share link created	Forgetful Felix
Box	Removed	File deleted	Forgetful Felix
Box	Removed	File share link deleted	Admin Andy

- ◀ Search a complete forensics audit trail of Box activity to quickly see the who, what, when, where details.

Level-up your **Box** security event auditing

Our partnership with Box provides unlimited API calls for the Varonis application and won't impact your quotas.

- Sharing link activity
- User admin role changes
- User impersonations
- User login activity
- User changes
- Security group changes
- Object renames
- Device associations
- File & folder creates
- File & folder deletes/restores
- File & folder moves/copies
- File & folder uploads/downloads
- File & folder permission changes
- File locked/unlocked
- Organization invitations
- File & folder invitations



Complimentary Incident Response Service

If you're under attack, or just looking for some help to understand what you're seeing, call on the expertise of our Incident Response team. They'll help you investigate and resolve any incident, whether you're a Varonis customer or trial user.



MATT RADOLEC

Security Architecture
& Incident Response

Try Varonis for Box Free

All Varonis products are free to try and come with an engineer-led risk assessment. The easiest way to get started is with a short 1:1 demo and discovery conversation.

[CONTACT US](#)