



A deep dive into the Microsoft 365 Audit Trail

A Gravity Union Webinar

www.gravityunion.com

Housekeeping

1. Use the Q/A panel to ask questions or share comments
2. The recording will be posted on our YouTube channel:
(Gravity Union – YouTube)

What we'll cover today

- ✓ A brief history of auditing in SharePoint (and the broader ecosystem)
- ✓ What M365 offers in terms of audit trails
- ✓ What kind of information can we get from the audit trail?
- ✓ How do we get it?
- ✓ Why is it important?
- ✓ Gaps and issues
- ✓ Compliance considerations
- ✓ Overview of Gravity MOAT
- ✓ Questions

Introductions



Jas Shukla

Director of Business Development

- ✓ 15 years experience in enterprise technology consulting
- ✓ Previously with Microsoft on the SharePoint product team
- ✓ UX designer in a previous life



Michael Schweitzer

President and CEO

- ✓ 20 years of enterprise technology experience
- ✓ Microsoft and Collabware certified
- ✓ Collabware MVP recipient
- ✓ Vancouver Office 365 user group board member
- ✓ ARMA Canada guest speaker
- ✓ Collabware User Group Board Member
- ✓ SharePoint Saturdays guest speaker
- ✓ Over 100 SharePoint ECM projects completed

Who we are

A boutique compliance-inspired services firm helping organization in their digital transformation journey

Gold
Microsoft Partner



Gold Certified
Collabware Partner



Content Services Microsoft Partner

- Recognized by Microsoft for the success we deliver to customers with Microsoft Content Services technology
- Partner with Microsoft, providing feedback on the product functionality and roadmap
- Special support from Microsoft for our project work



Content Services
Partner Program
Charter Member

Experience Overview

50+

Years of combined
Collabware
experience

10,000+

Users using our
SharePoint and
M365 solutions

40+

Microsoft
certifications

25+

Collabware and
Collabspace projects

250+

Years of SharePoint
experience across
our team

18

Collabware certified
consultants

50+

Million documents
migrated and
managed in our
solutions

100%

Project success rate

What is an audit trail?

Let's level set!

What is an audit trail?

- ✓ A log of events in an application, examples:
 - Logging in
 - Viewing a file
 - Deleting a file
- ✓ Metadata (descriptions) about the event
 - Who, what, where, when, how

```
1 {
2   "creationtime": "2020-12-01t01:18:27",
3   "id": "5bccfed8-827e-43ab-aec6-183d91362700",
4   "operation": "userloggedin",
5   "organizationid": "02c5ecf0-1cec-4a5b-8ded-cd12a3052900",
6   "recordtype": 15,
7   "resultstatus": "succeeded",
8   "userkey": "mshimada@gravityunion.com",
9   "usertype": 0,
10  "version": 1,
11  "workload": "azureactivedirectory",
12  "clientip": "64.52.27.140",
13  "objectid": "00000002-0000-0ff1-ce00-000000000000",
14  "userid": "mshimada@gravityunion.com",
15  "azureactivedirectoryeventtype": 1,
16  "extendedproperties": [
17    {
18      "name": "useragent",
19      "value": "microsoft office/16.0 (windows nt 10.0; microsoft outlook 16.0.12527; pro)"
20    },
21    {
22      "name": "userauthenticationmethod",
23      "value": "1"
24    },
25    {
26      "name": "requesttype",
27      "value": "oauth2:token"
28    },
29    {
30      "name": "resultstatusdetail",
31      "value": "success"
32    },
33    {
34      "name": "keepmesignedin",
35      "value": "false"
36    }
37  ],
```

Why are audit trails important?



Why we need to keep it

- ✓ Meet certain **regulatory compliance** standards
- ✓ Provide **evidence** in litigation or investigations
- ✓ Understand what happened with **comprised accounts**
- ✓ Provide insight into **adoption**
 - How heavily are our systems being used?
- ✓ Provide insight into **compliance**
 - How much of our content is being classified?



Information Systems Audit Trails in Legal Proceedings as Evidence

Caroline Allinson

*Information Security Section, Information Management Division, Queensland Police Service,
GPO Box 1440, BRISBANE Qld 4001, Australia.*

and

*Research Student, Information Security Research Centre (ISRC), Queensland University of Technology,
Brisbane, Queensland, Australia.*

Keywords: Law enforcement, audit trails, evidence, investigation, expert witness, information security, policy, court, survey, computer.

Abstract

Australian State and Commonwealth Governments are interested in the collection, storage and presentation of audit trail information, particularly within a legal framework. Law enforcement agencies have a legal obligation to keep audit records of all activity on information systems used within their operations. Little to no research has been identified in relation to the use of internal audit systems for evidentiary purpose.

A brief history of audit trails is given with requirements for such audit trails beyond the year 2000.

The Queensland Police Service (QPS), Australia, is used as a major case study. Information on principles, techniques and processes used, and the reason for the recording, storing and releasing of audit information for evidentiary purposes have been studied.

To assist in determining current practice in the Australian Commonwealth and State Governments the results of an Australia wide survey of all government departments are given and contrasted to the major study for QPS.

Reference is also made to the legal obligations for authorization of audit analysis, expert witnessing and legal precedence in relation to court acceptance or rejection of audit information used in evidence.

It is shown that most organizations studied generate and retain audit trails but the approach is not consistent nor is it comprehensive. It is suggested that these materials would not withstand a serious legal challenge.

1. Introduction

This paper examines the status of computer based information systems audit trails in relationship to their presentation in legal proceedings as evidence.

Over the past few decades audit has developed more than one meaning. Traditionally it was used in



MORE FROM FORBES

Feb 22, 2021, 08:37am EST

EU/UK Data Flows Can Continue – For Now

Feb 22, 2021, 06:00am EST

How China's Most Dangerous Cyber Threats Are 'Made In America'

Feb 21, 2021, 10:00am EST

Got A 'Day Of Hack' Email With Your Password? Here's 3 Things To Do Now

Feb 21, 2021, 05:14am EST

Apple Issues Bold Blow To Google With This Brilliant New Security Move

Feb 19, 2021, 10:41pm EST

Safety Certification Giant UL Has Been Hit By Ransomware

Feb 18, 2021, 12:46pm EST

Hackers Leak Gigabytes Of Data Stolen From International Law Firm Jones Day



ADVERTISEMENT

Cisco Umbrella Secure Access Service Edge (SASE) For Dummies

May 2, 2019, 08:43am EDT | 63,594 views

Microsoft Office 365 Accounts Under Attack -- What You Need To Know



Davey Winder Senior Contributor
Cybersecurity

I report and analyse breaking cybersecurity and privacy stories



I realized that I was just as qualified as any of these people.

ADVERTISEMENT

coastcapital.
SPONSOR CONTENT
Building a better RRSP
How do you build higher retirement savings?

gravityunion.com Overview Error Code: 6CH9-ZZDI4Q-KNJ0 - Message (HTML)

File Message Help Tell me what you want to do

Ignore Delete Archive Reply Reply All Forward Meeting IM More

Junk Delete Archive Reply Reply All Forward Meeting IM More

Move to: ? To Manager

Team Email Done

Reply & Delete Create New

Move OneNote

Assign Mark Categorize Follow

Policy Unread Tags Up

Translate Editing

Read Aloud Speech

Zoom Zoom

Report Message Protection

Dynamics 365 Insights Customer Manager

gravityunion.com Overview Error Code: 6CH9-ZZDI4Q-KNJ0



Delivery Status Notification (Delay) <info@digitalrenter.com>
To Michael Schweitzer

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Reply Reply All Forward

Tue 2021-02-23 10:28 AM



Hello mschweitzer@gravityunion.com.

This is an overview with the activity of your account for Tuesday, February 23, 2021

In this period 7 message(s) have been put to a stop to deliver inbox.

Error Code: 6CH9-ZZDI4Q-KNJ0

[View Message](#)

****This is an automated message please do not reply**.**

© 2020 gravityunion.com All rights reserved

CNBC GLOBAL CFO COUNCIL

1 in 5 corporations say China has stolen their IP within the last year: CNBC CFO survey

PUBLISHED FRI, MAR 1 2019 5:00 AM EST | UPDATED FRI, MAR 1 2019 10:21 AM EST



Eric Rosenbaum
@ERPROSE

SHARE [f](#) [t](#) [in](#) [✉](#)

KEY POINTS

- Theft of intellectual property by Chinese companies is a major point of contention between the Trump administration and Chinese government.
- Just under one-third of CFOs of North America-based companies on the CNBC Global CFO Council say Chinese firms have stolen from them at some point during the past decade.
- U.S. trade policy remains a negative for businesses around the world, but right now European CFOs are expressing the biggest concerns about trade policy as an external risk factor.

Introducing
CANARY HOUSE

The Next Phase
of Canary District

Condominiums
Coming 2021





Sections

Get one year for CA\$39

Sign in

(Michael Nagle/Bloomberg News)



By **Hayley Tsukayama**
Reporter

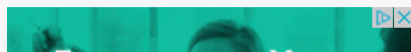
Dec. 19, 2016 at 8:03 a.m. PST

This post has been updated to reflect the date when Yahoo found out about the 2013 attack.

The scale of a second Yahoo breach disclosed on Wednesday was staggering, exposing information associated with a billion accounts. But, perhaps even more staggering was that the theft happened three years ago — and had not been reported until now. That probably left a lot of consumers wondering: Why does it take so long to find out that I've been hacked?

In Yahoo's case, the reason for the delay is a fairly simple one. The company didn't know about the breach for years after it happened. Yahoo has said that it first received the information that led it to finding out about the 2013 attack on November 7. Its security team was alerted by outside investigators rather than an internal team.

"[Law] enforcement provided us with data files that a third party claimed was Yahoo user data," wrote Yahoo's chief information security officer Bob Lord in a blog post. "We analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data."



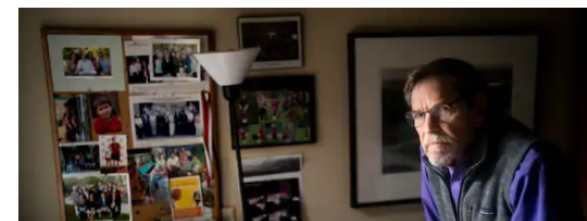
ASCENT
Real Estate Management Corporation

**Your Property. Our Passion.
The Best Partnership.**

Strata • Rental • Co-op
Property Management

LEARN MORE

Most Read Technology



Other real world examples

- ✓ Found **suspicious** deletions – user was deleting SharePoint synced folder on desktop
- ✓ Lead researcher quit a job – was able to determine which files they looked at and **downloaded** before leaving
- ✓ Where files are viewed – determine if files were being viewed **outside** of the **country** (nuclear non-proliferation act)
- ✓ Lawsuit evidence – prove if an employee had **read** the **overtime policy**
- ✓ Accidental death investigation – was the current **procedure** being followed?

A brief history of auditing in SharePoint (and ecosystem)

Back when I was a SharePoint Admin, we had to back up our content databases uphill, both ways.

Audit trails in SharePoint and on-premises ecosystem

- ✓ **Needed** to be turned on for a given Site Collection
- ✓ **Limited** (add, edit, delete, view)
- ✓ Turning on “View” could **slow** things down
- ✓ Other information was available in other various locations
 - Search – Central Admin
 - Authorization and Authentication – Windows, Exchange and IIS logs
 - Other events – cryptically buried in SharePoint log files
 - Third party applications for web analytics
 - Solutions like **Collabware** added a custom Audit Trail to compensate

Issues with on-premises

- ✓ **Hard** to **consolidate** across site collections, other sources
- ✓ Audit trails **disappeared** on content when moved (i.e. record centers)
- ✓ Could be turned on and off (lack of **integrity**)
- ✓ Needed several **add-ons** to complete the picture of the audit

How does M365 approach audit trails?

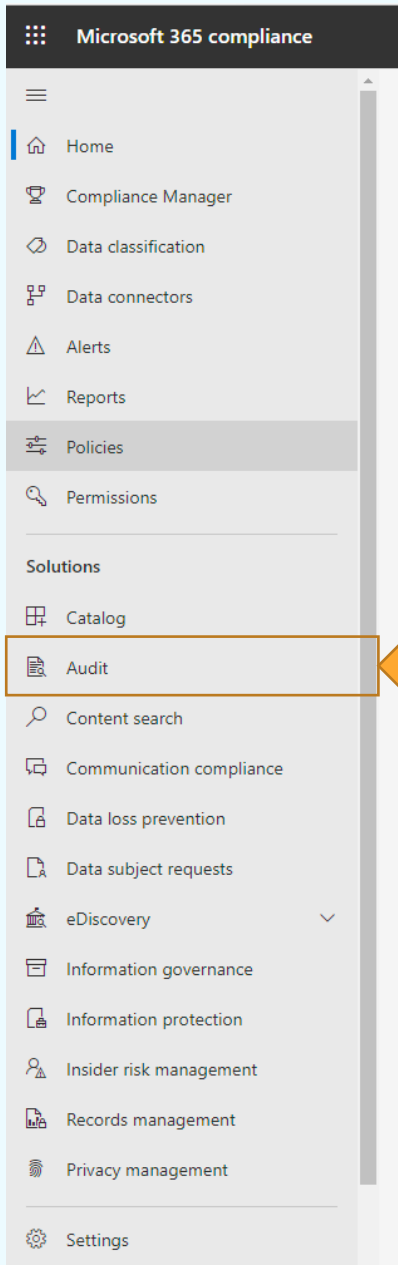
You get an audit, and you get an audit, and you get an audit...everyone gets an a-u-d-i-t!

Microsoft 365 audit trail

- ✓ Microsoft 365 offers a **centralized** location for
 - **all sources** (SharePoint, Teams, One Drive etc. Active Directory)
 - **all activities** (view, edit, download, create folder etc.)
- ✓ ~**1000** activity types
- ✓ **100s** of different types of metadata (user name, IP address, browse etc.)

Gaining Access

- ✓ With **enough** permissions:
 - <https://compliance.microsoft.com/>



Gaining Access

✓ With **enough** permissions:

- <https://compliance.microsoft.com/>

- Microsoft 365 compliance
- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention
 - Data subject requests
 - eDiscovery
 - Information governance
 - Information protection
 - Insider risk management
 - Records management
 - Settings
 - More resources
 - Customize navigation

Audit

[Learn about audit](#) [Show in](#)

Search Audit retention policies

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search

[View all activities](#)

Start date
Start time

End date
End time

Export 0 items

Applied filters:

Date	IP Address	User	Activity	Item	Detail
------	------------	------	----------	------	--------

No data available

What kind of information can we capture?

Give me all the datas

Everything

Source	Example Events
Azure Active Directory	Login, failed log in attempts.....
SharePoint	File Added, File Viewed, File Deleted...
One Drive	File Added, File Viewed, File Deleted...
Microsoft Teams	Meeting Started...
Exchange	Email sent, Email Received, Attachment Opened....
Power BI	Report viewed, data refreshed....
Power Automate	Workflow started....
And more.....

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Audit**
 - Content search
 - Communication compliance
 - Data loss prevention
 - Data subject requests
 - eDiscovery
 - Core
 - Advanced

Audit

Search Audit retention policies

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have done with groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Create audit retention policy

Search

Activities: Show results for all activities

Users: Search

File, folder, or site: Add all or part of a file name, folder name or URL

View all activities

Start date: Sat Jan 16 2021

Start time: 00:00

End date: Mon Jan 18 2021

End time: 00:00

Search Clear all

Export

Applied filters:

Date	IP Address	User	Activity	Item
------	------------	------	----------	------

No data available

Activities

Clear filters

- Accessed file
- Changed retention label for a file
- Deleted file marked as a record
- Checked in file
- Changed record status to locked
- Changed record status to unlocked
- Checked out file
- Copied file
- Discarded file checkout
- Deleted file
- Deleted file from recycle bin
- Deleted file from second-stage recycle bin
- Detected document sensitivity mismatch
- Detected malware in file
- Downloaded file
- Modified file
- Moved file
- Recycled all minor versions of file
- Recycled all versions of file
- Recycled version of file
- Renamed file
- Restored file
- Uploaded file
- Viewed page
- View signaled by client
- Performed search query

Apply Need help? Give feedback

Exports

- ✓ Max **50,000** events per download
- ✓ Excel with embedded **JSON** format

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
- Catalog
- Audit**
- Content search
- Communication compliance
- Data loss prevention
- Data subject requests
- eDiscovery
- Information governance
- Information protection
- Insider risk management
- Records management
- Settings
- More resources
- Customize navigation

Audit

[Learn about audit](#)

Search Audit retention policies

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search

Activities

[View all activities](#)

Users

MS Michael Schweitzer ×

File, folder, or site ⓘ

Start date

Start time

End date

End time

Search
Clear all

↓ Export ↓

Applied filters:

Date	IP Address	User	Activity	Item	Detail
Feb 24, 2021 5:45 AM	207.81.212.226	mschweitzer@gravityunion.com	Accessed file	docsethomepage.aspx	Accessed fro
Feb 22, 2021 11:01 AM	207.81.212.226	mschweitzer@gravityunion.com	Accessed file	docsethomepage.aspx	Accessed fro
Feb 17, 2021 7:53 AM	207.81.212.226	mschweitzer@gravityunion.com	Accessed file	docsethomepage.aspx	Accessed fro
Feb 21, 2021 8:44 AM	70.36.51.25	mschweitzer@gravityunion.com	Accessed file	docsethomepage.aspx	Accessed fro

File Home Insert Draw Page Layout Formulas Data Review View Help

Clipboard: Paste, Cut, Copy, Format Painter

Font: Calibri, 11, Bold, Italic, Underline, Text Color, Background Color

Alignment: Wrap Text, Merge & Center

Number: General, Currency, Percentage, Decimals

Styles: Normal, Bad, Good, Neutral, Calculation, Check Cell, Explanatory, Input, Linked Cell, Note

Cells: Insert, Delete, Format

Editing: AutoSum, Fill, Clear, Sort & Filter, Find & Select

Analysis: Analyze Data, Sensitivity

POSSIBLE DATA LOSS Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format. [Don't show again] [Save As...]

D2: {"CreationTime":"2021-02-24T13:45:28","Id":"7a943fe4-bd1f-4055-d597-08d8d8ca7286","Operation":"FileAccessed","OrganizationId":"02c5ecf0-1cec-4a5b-8ded-cd12a3052900","RecordType":6,"UserKey":"i:0h.f|membership|10037ffe95eccb6e@live.com","UserType":0,"Version":1,"Workload":"SharePoint","ClientIP":"207.81.212.226","ObjectId":"https://gravityunion.sharepoint.com/sites/Marketing2/Events/Forms/Marketing Event Document Set/docsethomepage.aspx","UserId":"mschweitzer@gravityunion.com","CorrelationId":"6667ae9f-50e3-b000-ea32-7da3e81b23c7","EventSource":"SharePoint","ItemType":"File","ListId":"e43be9df-a29e-487e-bbb5-7f0ab6e214b7","ListItemUniqueId":"41331955-66f8-4c34-ba26-34804b7659af","Site":"e244d17c-53ee-4a3d-9359-1a3626ac1604","UserAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 Edg/88.0.705.74","WebId":"aa077d5f-bfb1-4f54-"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	
1	Creation	UserIds	Operations	AuditData																											
2	2021-02-2	mschweit	FileAccessed	{"CreationTime":"2021-02-24T13:45:28","Id":"7a943fe4-bd1f-4055-d597-08d8d8ca7286","Operation":"FileAccessed","OrganizationId":"02c5ecf0-1cec-4a5b-8ded-cd12a3052900","RecordType":6,"UserKey":"i:0h.f membership 10037ffe95eccb6e@live.com","UserType":0,"Version":1,"Workload":"SharePoint","ClientIP":"207.81.212.226","ObjectId":"https://gravityunion.sharepoint.com/sites/Marketing2/Events/Forms/Marketing Event Document Set/docsethomepage.aspx","UserId":"mschweitzer@gravityunion.com","CorrelationId":"6667ae9f-50e3-b000-ea32-7da3e81b23c7","EventSource":"SharePoint","ItemType":"File","ListId":"e43be9df-a29e-487e-bbb5-7f0ab6e214b7","ListItemUniqueId":"41331955-66f8-4c34-ba26-34804b7659af","Site":"e244d17c-53ee-4a3d-9359-1a3626ac1604","UserAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 Edg/88.0.705.74","WebId":"aa077d5f-bfb1-4f54-"																											
3	2021-02-2	mschweit	FileAccessed																												
4	2021-02-1	mschweit	FileAccessed																												
5	2021-02-2	mschweit	FileAccessed																												
6																															
7																															
8																															
9																															
10																															
11																															
12																															
13																															
14																															
15																															
16																															
17																															
18																															
19																															
20																															
21																															
22																															
23																															
24																															
25																															
26																															
27																															
28																															
29																															
30																															
31																															
32																															
33																															
34																															
35																															
36																															
37																															

```
1
2 "creationtime": "2020-12-01t01:18:27",
3 "id": "5bccfed8-827e-43ab-aec6-183d91362700",
4 "operation": "userloggedin",
5 "organizationid": "02c5ecf0-1cec-4a5b-8ded-cd12a3052900",
6 "recordtype": 15,
7 "resultstatus": "succeeded",
8 "userkey": "mshimada@gravityunion.com",
9 "usertype": 0,
10 "version": 1,
11 "workload": "azureactivedirectory",
12 "clientip": "64.52.27.140",
13 "objectid": "00000002-0000-0fff1-ce00-000000000000",
14 "userid": "mshimada@gravityunion.com",
15 "azureactivedirectoryeventtype": 1,
16 "extendedproperties": [
17   {
18     "name": "useragent",
19     "value": "microsoft office/16.0 (windows nt 10.0; microsoft outlook 16.0.12527; pro)"
20   },
21   {
22     "name": "userauthenticationmethod",
23     "value": "1"
24   },
25   {
26     "name": "requesttype",
27     "value": "oauth2:token"
28   },
29   {
30     "name": "resultstatusdetail",
31     "value": "success"
32   },
33   {
34     "name": "keepmesignedin",
35     "value": "false"
36   }
37 ],
```

How else can we use it?

What is it good for?

Governance Examples

- ✓ Identify and manage the creation of sites, lists, libraries, folders not inline with standards, patterns and practices
- ✓ Identify unused or under-used applications\sites\libraries\groups\teams
- ✓ Identify where security protocols are not followed (external sharing, breaking inheritance)

siteurl	actioncount
https://gravityunion.sharepoint.com/sites/proposals/	4048
https://gravityunion.sharepoint.com/sites/#####-meradiscovery/	2479
https://gravityunion.sharepoint.com/sites/marketing2/	1935
https://gravityunion.sharepoint.com/sites/presentations/	1643
https://gravityunion.sharepoint.com/	1505
https://gravityunion.sharepoint.com/sites/recruiting/	1360
https://gravityunion.sharepoint.com/sites/#####-spoandcollabspaceroollout/	1341
https://gravityunion.sharepoint.com/sites/#####-collaborationsites/	1299
https://gravityunion.sharepoint.com/sites/delivery-therelaunch/	1220
https://gravityunion-my.sharepoint.com/	1028
https://gravityunion.sharepoint.com/sites/#####-collabspacimplementation/	852
https://gravityunion.sharepoint.com/sites/branding/	713
https://gravityunion.sharepoint.com/sites/skylab/	608
https://gravityunion.sharepoint.com/sites/#####documentmanagement/	569
https://gravityunion.sharepoint.com/sites/#####-spoandcollabspaceroollout/	473
https://gravityunion.sharepoint.com/sites/operations/	438
https://gravityunion.sharepoint.com/sites/receivables/	372
https://gravityunion.sharepoint.com/sites/draftcontracts/	355
https://gravityunion.sharepoint.com/sites/administration/	319
https://gravityunion.sharepoint.com/sites/#####harepointandcollabwarerollout-guprivatchannel/	313
https://gravityunion.sharepoint.com/sites/proposals	293
https://gravityunion.sharepoint.com/sites/proposals/b57f85ce-2feb-4f04-85b9-40eaec137d1	234
https://gravityunion.sharepoint.com/sites/-sp2019modernization/	231
https://gravityunion.sharepoint.com/sites/testingsandbox/	184
https://gravityunion.sharepoint.com/sites/recruiting	182
https://gravityunion.sharepoint.com/sites/townshipof#####/	178
https://gravityunion.sharepoint.com/sites/signedcontracts/	170
https://gravityunion.sharepoint.com/_layouts/15/officeextensionmanager.aspx	161
https://gravityunion.sharepoint.com/sites/projecthub/	160
https://gravityunion.sharepoint.com/sites/partners/	146
https://gravityunion.sharepoint.com/sites/skylab	141
https://gravityunion.sharepoint.com/sites/recruiting/143b99dc-b66b-4f64-8e9a-414e7bc2ee37	140
https://gravityunion.sharepoint.com/sites/moat/	127
https://gravityunion.sharepoint.com/sites/ocm/	103

Security Examples

- ✓ Identify external user activity
- ✓ Report on access to sensitive information
- ✓ See if people are accessing data outside of regional jurisdiction (data sovereignty)
- ✓ Help identify compromised accounts

userkey	failedlogincount
dspeers@gravityunion.com	28
mschweitzer@gravityunion.com	12
dchan@gravityunion.com	12
jchin@gravityunion.com	11
shoff@gravityunion.com	8
jbotelho@gravityunion.com	4
acrandall@gravityunion.com	3
dsaini@gravityunion.com	3
kcreswell@gravityunion.com	3
dhelmer@gravityunion.com	2
rgaron@gravityunion.com	2
rtishenko@gravityunion.com	1
mmarchetto@gravityunion.com	1
ske@gravityunion.com	1
jshukla@gravityunion.com	1

Compliance Examples

- ✓ Identify content that is not classified
- ✓ Identify content that should be declared as a record but is not
- ✓ Identify content that should have been disposed of but is not
- ✓ Identify content that was deleted, that should have been kept

Record States Over Time



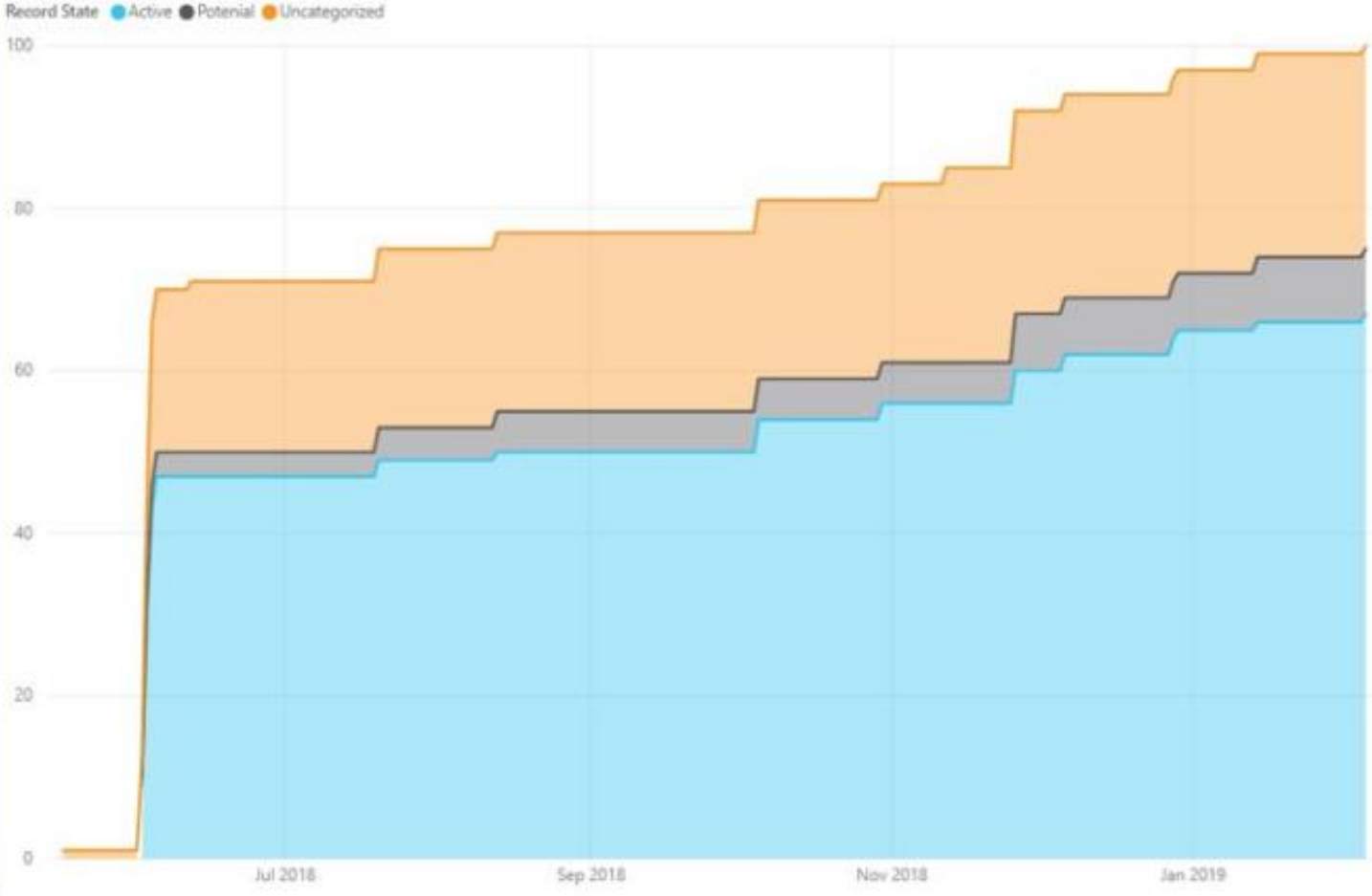
Date Range
Activity Date
Last 1 Years
21/03/2018 - 20/03/2019

Site Collections

- Select All
- administrator
- Content Type Hub
- Gravity Union Collaboration Portal
- Portal
- Records Center

Sites

- Select All
- Administration
- administrator
- BRR
- Content Type Hub
- HR
- IM
- Legal
- Portal
- Records Center



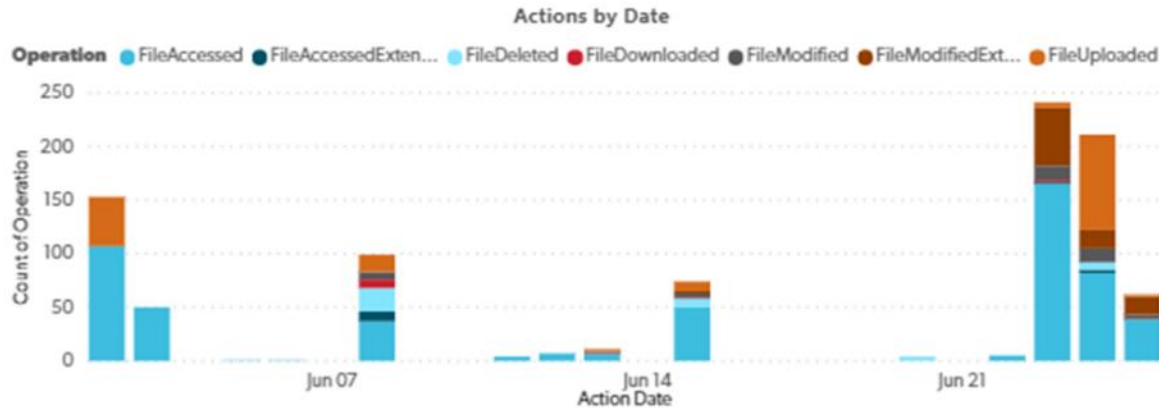
Have questions? We can help! Contact Gravity Union at contact@gravityunion.com



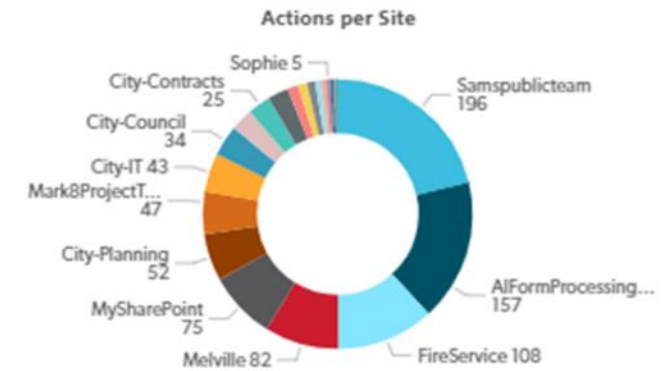
Adoption Examples

- ✓ Identify usage of applications, sites, lists, libraries
 - Is the new group leveraging the solution as expected?
- ✓ Observe if email traffic decreases down after a Teams or Yammer deployment
- ✓ See if people are sharing links instead of emailing documents

Audit Log - Actions By User



User	Site Name	Operation	Action Count
adminjeff@gravityuniondev.com	City-Clerk	FileAccessed	
		Total	
	City-Contracts	FileAccessed	
		Total	
	City-Finance	FileAccessed	
		Total	
	City-HR	FileAccessed	
		Total	
	City-IT	FileAccessed	
		Total	
	City-Planning	FileAccessed	
		Total	
	FireSafetyCommittee	FileAccessed	
		Total	
FireService	FileAccessed		
	Total		
Melville	FileAccessed		
	Total		



Have questions? We can help! Contact Gravity Union at contact@gravityunion.com



Compliance considerations?

Right! Time to get serious.

Archive audit trails for longer than what Microsoft offers

- ✓ Many compliance standards require that the audit trail is kept for the life of the document
- ✓ 90 days/1 year is likely not enough and there are limitations with audit retention policies
- ✓ Many companies will need to extract the audit trail entries and store them outside of M365

Place into a discoverable format

- ✓ Excel downloads are not easily consumable
- ✓ Need to pull into a database

Place audit trail entries on hold

- ✓ Protecting audit trails from disappearing while the content is involved in:
 - Litigation
 - FOI\FOIA (Freedom of Information)
 - ATIP (Access to Information and Privacy)
 - Investigations
 - Regulatory requirements (depending on the governing body)

Anonymize or destroy the audit trail

- ✓ You may want to keep the data for documents that have been deleted or disposed for analytics, be remove any personally identifiable information (PII)
 - i.e. remove usernames

Gaps and issues in the M365 Audit Trail

Now the bad news

Disappearing audit

- ✓ E3/E1 saves **3 months** of audit data (per user)
- ✓ E5 saves **1 year** of audit data (per user)
- ✓ Audit retention rules to store some audit data longer (requires E5 + additional license per user)

Retention policies

- ✓ You can have a maximum of **50** audit log retention policies in your organization
- ✓ To retain an audit log for longer than 90 days, the user who generated the audit log **must** be assigned an **E5** license or have an E5 Compliance or E5 eDiscovery and Audit add-on
- ✓ **Shortest rule wins** - if you create an audit log retention policy for Exchange mailbox activity that has a retention period that's shorter than one year, audit records for Exchange mailbox **activities will be retained for the shorter duration** specified by the custom policy
- ✓ Advanced Audit License is **required** (additional **cost** above E5?) \$ per user

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention
 - Data subject requests
 - eDiscovery
 - Core
 - Advanced

Audit

Search Audit retention policies

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Create audit retention policy

Search

Activities: Show results for all activities

Users: Search

File, folder, or site: Add all or part of a file name. fo

View all activities

Start date: Sat Jan 16 2021

Start time: 00:00

End date: Mon Jan 18 2021

End time: 00:00

Search Clear all

Export

Applied filters:

Date	IP Address	User	Activity
------	------------	------	----------

No data available

New audit retention policy

Create a policy to retain audit logs for up to one year based on the Microsoft 365 service where the activities occur, specific activities in the selected services, and the user who performs an activity. [Learn more](#)

Name *

Description

Please choose users or record types to apply this policy to.

Users

Record type

Duration *

- 90 Days
- 6 Months
- 9 Months
- 1 Year
- 10 Years

Priority *

Save

Cancel

Need help?

Give feedback



- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
 - Catalog
 - Audit
 - Content search
 - Communication compliance
 - Data loss prevention
 - Data subject requests
 - eDiscovery
 - Information governance
 - Information protection
 - Insider risk management
 - Records management
 - Privacy management
 - Settings
 - More resources

Audit

Search Audit retention policies

Create audit retention policy

Priority	Policy name	Record type	Activities	Users
No data available				

New audit retention policy

Create a policy to retain audit logs for up to one year based on the Microsoft 365 service where the activities occur, specific activities in the selected services, and the user who performs an activity. [Learn more](#)

Policy name *

Description

Please choose users or record types to apply this policy to.

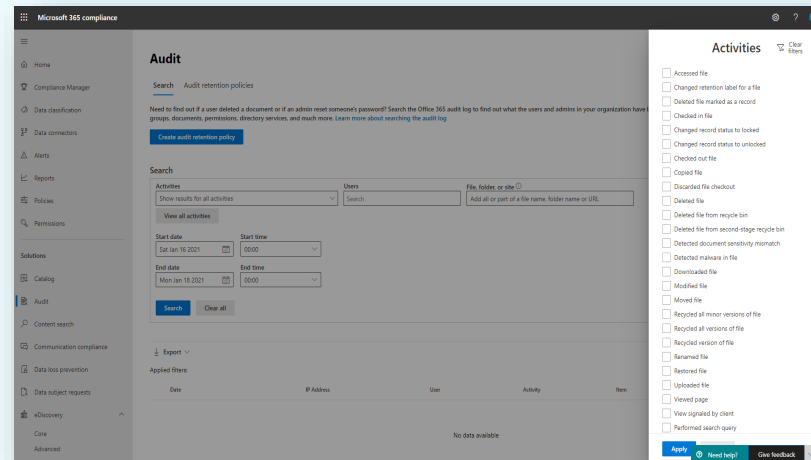
Users

Record type

- SharePointFieldOperation
- SharePointFileOperation
- SharePointListOperation
- SharePointSearch
- SharePointSharingOperation
- SkypeForBusinessCmdlets
- Sway

Download limit

- ✓ **50,000** audit entries per download
- ✓ Average user creates **300-400** events per day



Example

- ✓ Company with **1000** users will produce:
 - **400,000** daily audit events
 - Require **8** downloads
- ✓ It's not easy to slice and dice the audit in order to download (recall: 50k Limit)
 - How to **split up** effectively into 50k chunks?
(time is the easiest)

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Reports
- Policies
- Permissions
- Solutions
- Catalog
- Audit**
- Content search
- Communication compliance
- Data loss prevention
- Data subject requests
- eDiscovery
- Information governance
- Information protection
- Insider risk management
- Records management
- Settings
- More resources
- Customize navigation

Audit

[Learn about audit](#)

Search Audit retention policies

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search

Activities

[View all activities](#)

Users

MS Michael Schweitzer ✕

File, folder, or site ⓘ

Start date

End date

[Search](#) [Clear all](#)

↓ Export ↓

Applied filters:

Date	IP Address	User	Activity	Item	Detail
Feb 24, 2021 5:45 AM	207.81.212.226	mschweitzer@gravityunion.com	Accessed file	docsethomepage.aspx	Accessed fro
Feb 22, 2021 11:01 AM	207.81.212.226	mschweitzer@gravityunion.com	Accessed file	docsethomepage.aspx	Accessed fro
Feb 17, 2021 7:53 AM	207.81.212.226	mschweitzer@gravityunion.com	Accessed file	docsethomepage.aspx	Accessed fro
Feb 21, 2021 8:44 AM	70.36.51.25	mschweitzer@gravityunion.com	Accessed file	docsethomepage.aspx	Accessed fro

Inability to create custom reports

- ✓ Not in a format that supports creating custom reports for the organization

Not everyone has access

- ✓ Most end users do not have access to the compliance center and have to go through IT

Introducing Gravity MOAT

A compliance focussed audit trail management solution

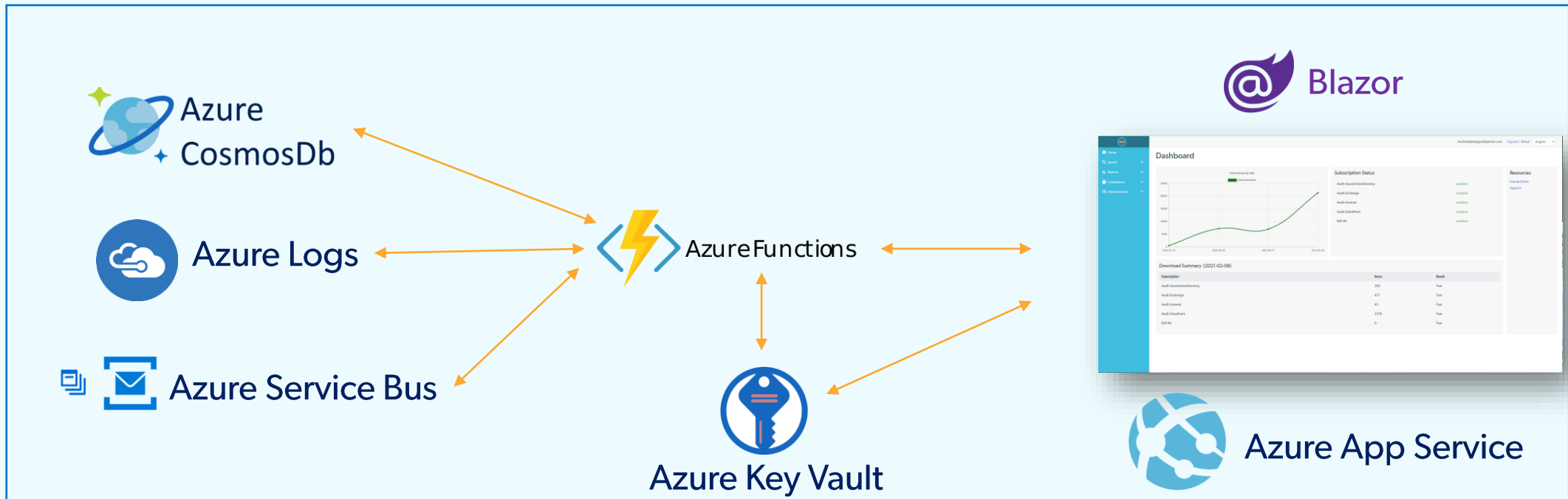


Gravity MOAT

- ✓ Compliance focussed **M**icrosoft **O**ffice 365 **A**udit **T**rail archiving
- ✓ Stored in **your** Azure environment (complete **ownership** of data)
- ✓ Allows custom **reports**
- ✓ Allows for complete **control** over the audit
- ✓ Multi lingual
- ✓ Allows **access** to the audit trail without needing access to the compliance center in *Microsoft 365*



Solution architecture



Search, reporting and export

- ✓ Quick searches (user, IP, document, list, site)
- ✓ Advanced search
- ✓ Reporting
 - 100's of prebuilt reports in application and Power BI
- ✓ Export results into JSON, XML or Excel



Compliance

- ✓ **Auto-delete** audit trail based on source application (workload)
- ✓ Delete or **anonymize** audit trail entries upon record disposition
- ✓ Place audit trail entries on **legal hold**




```
{
  "creationtime": "2020-12-01t00:52:03",
  "id": "aa0e659d-23df-4b52-809d-08d8959351b3",
  "operation": "fileaccessed ",
  "organizationid": "02c5ecf0-1cec-4a5b-8ded-cd12a3052900",
  "recordtype": 6,
  "userkey": "ANONOMYZED",
  "usertype": 0,
  "version": 1,
  "workload": "sharepoint",
  "clientip": "40.82.191.74",
  "objectid": "https://gravityunion.sharepoint.com/sites/.../siteassets/open notebook.onetoc2",
  "userid": " ANONOMYZED",
  "correlationid": "5cdf929f-60d7-b000-0986-b02c9839c382",
  "eventsources": "sharepoint",
  "itemtype": "file",
  "listid": "ade49883-0a0f-4fab-8f62-ba1749ee678d",
  "listitemuniqueid": "7cb1a5f7-9925-4388-ac11-5376e2052d40",
  "site": "820df841-5e3d-4d18-a63c-07716a787166",
  "useragent": "mswaconsync",
```



API

- ✓ Place audit trail entries on hold
- ✓ Delete or anonymize audit trail entries
- ✓ Custom sources



Surfacing in SharePoint

The screenshot displays a SharePoint interface for a library named 'Draft Contracts'. A 'MOAT View' overlay is open, showing a table of file operations. The table has four columns: Time, Operation, User, and Name. The 'Name' column contains a large block of redacted text. The background shows a list of files in the 'Draft Contracts' library, with a 'Name' column also containing redacted text.

Time	Operation	User	Name
2021-02-02t18:41:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:40:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:39:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:38:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:38:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:37:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:40:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:37:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:36:...	fileaccesssed	app@sharepoint	[Redacted]
2021-02-02t18:36:...	filemodified	ccote@gravityun...	[Redacted]
2021-02-02t18:36:...	fileaccesssed	ccote@gravityun...	[Redacted]
2021-02-02t18:36:...	fileaccesssedexte...	app@sharepoint	[Redacted]
2021-02-02t18:36:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:36:...	fileaccesssedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:35:...	fileaccesssedexte...	app@sharepoint	[Redacted]
2021-02-02t18:35:...	filemodifiedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:35:...	fileaccesssedexte...	ccote@gravityun...	[Redacted]
2021-02-02t18:35:...	fileaccesssedexte...	app@sharepoint	[Redacted]



Surfacing in SharePoint

- ✓ Document Activity
- ✓ List Activity
- ✓ Site Activity
- ✓ Deleted Items List
- ✓ Deleted Items Library



Extensible

- ✓ Custom reports
- ✓ Adding additional data sources
- ✓ Custom SharePoint integration (think automated governance)



DEMO

A quick tour of Gravity MOAT



- Home
- Search
- Document
- User Activity
- Site Activity
- Library Activity
- IP Address Activity
- Advanced Search
- Reports
- SharePoint
- Teams
- OneDrive
- Exchange
- User
- System
- Active Directory
- Compliance
- Audit Management
- Workload Management
- Legal Holds

Active Directory Reports

Failed User Logins

Pick Date Range:

2021-01-01 - 2021-01-22

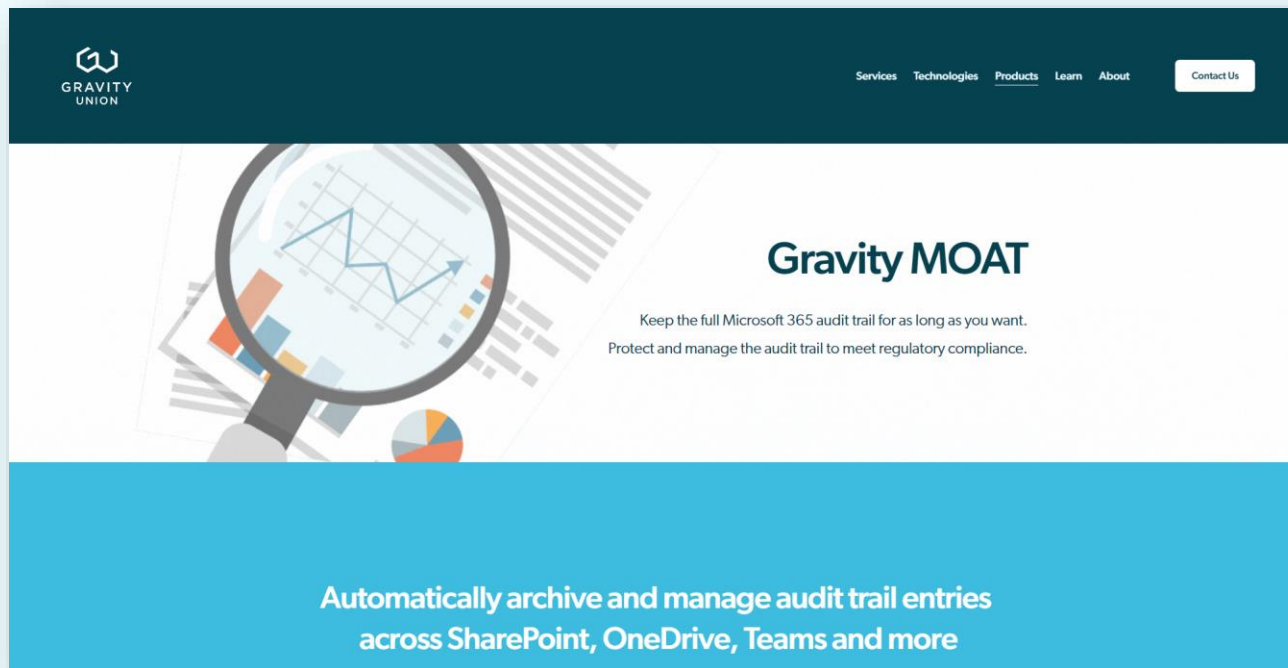
Run Report

Failed User Logins

userkey	failedlogincount
dspeers@gravityunion.com	28
mschweitzer@gravityunion.com	12
dchan@gravityunion.com	12
jchin@gravityunion.com	11
shoff@gravityunion.com	8
775ed966-d11a-453b-913c-64606538c27f	5
jbotelho@gravityunion.com	4
acrandall@gravityunion.com	3
dsaini@gravityunion.com	3
kreswell@gravityunion.com	3
dhelmer@gravityunion.com	2
rgaron@gravityunion.com	2
c4f11901-980a-4c10-a3a4-76ee02909640	2
rtishenko@gravityunion.com	1
mmarchetto@gravityunion.com	1

Learn more

<https://www.gravityunion.com/moat>



The screenshot shows the Gravity MOAT website landing page. At the top left is the Gravity Union logo, and at the top right is a navigation menu with links for Services, Technologies, Products, Learn, and About, along with a Contact Us button. The main content area features a magnifying glass over a line graph and a pie chart. The heading "Gravity MOAT" is prominently displayed, followed by the text: "Keep the full Microsoft 365 audit trail for as long as you want. Protect and manage the audit trail to meet regulatory compliance." A blue banner at the bottom of the page contains the text: "Automatically archive and manage audit trail entries across SharePoint, OneDrive, Teams and more".



Q&A

Next webinar

- ✓ Problems with adoption?
- ✓ People hate SharePoint or Teams?
- ✓ Messy SharePoint solution requiring too much maintenance?
- ✓ Spending too much time fixing things instead of adding value to your implementation?

Next webinar



 GRAVITY UNION

Craft a great UX with Teams and SharePoint

Webinar on March 25, 2021

<https://go.gravityunion.com/ux-webinar>



**Thank you for
joining!**

mschweitzer@gravityunion.com

www.gravityunion.com



GRAVITY
UNION

Compliance Inspired Digital Transformation

SharePoint | Office 365 | Collabware | Collabspace

www.gravityunion.com

www.gravityunion.com