

CLOUD DOCUMENT RISK INDICATOR GUIDE

The inevitable move by enterprises to cloud storage comes with a trade-off: reduced control and visibility in exchange for broader access, useability and productivity.

This guide will help you reduce cloud data loss using unique document activity indicators to detect common, persistent risks associated with the stealing or mishandling of sensitive and confidential files.

Data is being migrated to the cloud faster than it can be secured

Enterp	SG Tre	ends in Clou	d Secur	it	У									
	Very concerned Not very concerned	Somewhat concerned Not at all concerned	Malware		25%				59	%			13%	3%
		The sharing of sensitive da	ta with external parties		21%				62%				14%	3%
	The use of sha	dow IT cloud applications and services	that creates blind spots		21%				61%				15%	3%
	The sharing of sensitive d	ata with employees unauthorized to re-	eive and view the data		21%				57%				18%	<mark>3%</mark>
		Targe	ted penetration attacks		20%				58%				18%	4%
		The misuse of a privileged account	by an inside employee		19%				63%				15%	4%
	Exploits that take	advantage of known vulnerabilities in	unpatched applications		19%				63%				14%	5%
[Third-p	arties mishandling data		19%								16%	4%
			Ransomware		19%		22% <u>s</u> ı						16%	3%
[Employees not prope	rly applying access and permission con	trols when sharing data		19%		reside they h		ta, and	d 50%	know	-	18%	3%
Ex	ploits that take advantage of	known vulnerabilities in unpatched op	erating system versions		18%		they h	ave.					15%	4%
"Zero da	ay" exploits that take advant	age of new and previously unknown vu	nerabilities in software		18%		ESG Resea	arch 201	.8				17%	4%
		Misconfigured cloud service:	s or privileged accounts		18%				59%				19%	4%
	The creation	and sharing of shadow data in and via c	loud apps and services		17%				61%				19%	3%
		The misuse of any accour	nt via stolen credentials		15%				67%				15%	4%
				0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	3100%

Although cloud storage providers log voluminous amounts of user and file activities log analysis, file tracking and automated identification of misuse and malicious activity is limited or nonexistent. Additionally, the greatest risk associated with any confidential document is after it is downloaded, copied or shared with a third party, at which time the cloud storage provider loses visibility and is no longer able to log any of the document's activity. Cloud-share provided log viewers lack intuitive interfaces and geolocation insights, are not continuously analyzed for risk, and provide no visibility into activity after a document has left a cloud share.



+80%

of a company's sensitive data is contained in documents.





of spending within key enterprise IT markets will be cloud-based by 2022, up from 19% in 2018.

A New Approach

Allure Security helps organizations understand Office 365 use across organizations, and detect and respond to data loss resulting from stolen credentials, insider threats, malicious third parties, ransomware and human error. The Allure data loss detection and response platform taps into the information captured in cloud-share logs, and watches and analyzes comprehensive cloud document flows over time. Further, Allure's patented technology enriches logs with geolocation insights, and continues to monitor activity even after a document has left the control of the organization. These findings better inform and focus incident responses, detect activities that violate security policies and support training initiatives to significantly reduce data loss risks and consequences.

Allure Security's approach includes three main components: Watch, Extend & Detect





Watch Office 365 file activity closely: See who interacts with which files, when and from where. Security teams can know in real time if unusual or bulk downloads occur, if confidential or sensitive files are accessed anonymously, and if documents are opened in risky locations or via unauthorized domains.



Extend visibility beyond the cloud share: Agentlessly log activity even after documents are downloaded, copied or shared with third parties.



Detect leaks and breaches: Know if insiders, malicious third parties, bots or hackers are snooping around confidential and sensitive files, and whether any data is lost as a result. Also, security professionals can set up optional alerts to be informed when risky activity is in progress to inform response and limit data loss.

Users rely on Allure to provide critical visibility into cloud-share risk, take proactive measures to prevent data loss and gather data loss forensics. Allure's intuitive dashboard captures and visualizes risks so users can easily see notable events with granular details and geolocation information, identify key indicators used to calculate and prioritize risks, and monitor most active users, domains, locations and operations. Additionally, users can drill down into specific document and user activity to collect forensics during active investigations.

Indicator Guide



CRITICAL INDICATORS FOR CLOUD DATA LOSS RISK

The most critical step in addressing data loss risk is to detect the risk itself. Protection and prevention methods are effective, to a point. But data leaks, ransomware attacks and breaches still occur daily. Do you want to know if cloud files are at risk, how, where and by whom? Allure relies on its unique document indicators to provide organizations with this insight.

ALLURE	DETECTED	INFORMED
INDICATORS	RISKS	ACTIONS
Activity by risky geography Unusual user activities Activity by type (downloads, link sharing, anonymous access) Access via anonymous VPN Unusual device types Downloading of bulk files Threatening uploads (e.gexe) File extension changes Access failures Decoy file activities	Threat actor with stolen credentials Insider malfeasance 3rd party negligence Shared link mistakes Attempted intrusions Permission setting mistakes Unauthorized access Compliance failures	Targeted investigations Incident response Account suspension User training Permission updates Revoking shared links Periodic assessment reports Employee accountability





Stolen Credentials & Brute-Force Logins

RISK FACTORS

Credentials can be stolen or guessed via the consequence of spear phishing from relentless attackers, mistaken sharing of credentials by legitimate users, or poorly chosen passwords. Remote attackers typically perform information gathering actions when they first penetrate defenses.

DETECTION INDICATORS

Users exhibit patterns that are learnable: unusual access, abnormal user events, downloading documents to atypical or impermissible geolocations, changes in device types, renaming of files, or unusual quantities and time of day activities are good indicators. Legitimate users whose credentials have been stolen by masqueraders may also upload executable files. Such uploads are also very good indicators of credential theft and are clearly risky events. Decoy file actions are particularly useful indicators that should be of immediate concern.

RESPONSE

Investigate the user directly to learn if they indeed performed the notable events, and suspend user accounts until the issue is resolved. If indexed by Google or other crawlers, ask to delete the index and any cached copies. Users who have not legitimately uploaded executable files are certainly likely to have lost their credentials. The user accounts must be suspended and new credentials issued. Any uploads by that user account should be quarantined for investigation. Any downloads by those user account are likely examples of specific data loss. Gather all of the information, including download locations, to investigate the extent of the loss.

Insider Threat

RISK FACTORS

Insiders with authorized access may act against the security policies of the organization, willfully for personal gain or retribution, or accidentally by misconfiguring access or inadvertently sharing links to sensitive documents.

Insiders may take measures to hide their access via VPN or anonymous links, or changing of file type extensions to hide the true content of the files in question. Bulk exfiltration is easily accomplished by zipping a number of files together and downloading, especially to forbidden geolocations or via VPN access.

Uploads of active content, executable files, for example, is a high risk. Masqueraders who have gained legitimate credentials may upload executables to gain a foothold into the organization bypassing internal controls, such as firewalls, email and proxy-based content analyses.

Former employees who left the company recently may still have active user accounts and hence access to company storage. This special case of "insider" is not uncommon.

DETECTION INDICATORS

Sensitive beaconized documents that are accessed anonymously, or that are downloaded and opened at a competitor's location, or any other unauthorized location is a good indicator. VPN access creates increased suspicion and risk. File operations that change the file extension are particularly good indicators of malfeasance.

Zipped file downloads are also a particularly good risk indicator that needs attention. A bulk exfiltration may have occurred. Uploads of any executable content is of immediate concern and very high risk. And of course, any decoy file actions are high value indicators of malfeasance.

Any file download at a geolocation owned by a competitor is of immediate concern. Inspect the history of the file to determine those users who have accessed the file, and if any are determined to be no longer employees, immediately check whether the account is still active.

RESPONSE

Immediately suspend the user's account and thoroughly investigate by contacting the user to understand what documents were accessed and for what purposes. If VPN access was noted, identify the reasons if VPN accesses are not authorized. Any uploaded executable should be quarantined immediately and investigated.

			NOTABL	LE EVENT			
File:	https:/acme.sharepoint.com/sites/Finance/Shared Documents/FY2018/FY2018.04.FINAL_1.xlsx						
Time (EST):	02/15/2019 3:38 AM	User:	anonymous				
File System:	Acme-0365	IP Address:	76.119.111.60				
Beacon Type:	Watched	Operation:	Download				
Tags:	Finance,Sensitive	Risk Score:	100				
Version:							
Map Sat	ellite Abington Hanover 3			1.0			
3	Brockton	Marshfield					
5 P	20 (7) Pembroke		Provincetown				
Mansfield		Duxbury		orth Truro			
Mansheld	(79) Bridgewater						
1 m	Bildgewater	Kingston					
	Bridgewater	Nongal Cont					
Norton	Raynham	Plymouth	Cape Coa Bay				
boro			- Oay				
- Charles		South Pond					
	aunton Middleborough Car	ver 3 2					
(44)							
	Berkley Lakeville	Myles Standish Elisville		8			
	8 8	Myles Standish Ellisville State Forest		4			
		Myles Standish Ellisville State Forest		4			
	24 (B) (C) (C) (C) (C) (C) (C) (C) (C) (C) (C	State Forest		4			
Somen	eet Freetown Rochester	State Forest Wareham (1) Sandwic					
	ee	State Forest	Dennis	Brews +			
Somer Swansea	a to the second	State Eorest Wareham 55 C Sandwic Bourne	Dennis	124			
Swansea	2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	State Forest Wareham (1) Sandwic	CA Dennis	-			
Somer Swansea Th GoogleFall River (M	29 (20) ref Freetown Rochester Acoustnet 0 M	State Eorest Wareham 55 C Sandwic Bourne	CA Dennis	-			
Somer Swanses	Piymouth, MA US	State Eorest Wareham 55 C Sandwic Bourne	CA Dennis	-			
Somer Swansea To GoogleFall River Ca Location: Lat/Long:	29 (20) ref Freetown Rochester Acoustnet 0 M	State Eorest Wareham 55 C Sandwic Bourne	CA Dennis	-			
Google Fall River Coogle Fall River Location: Lat/Long: Accuracy Radius:	Plymouth MA US 61-906, -70662	State Eorest Wareham 55 C Sandwic Bourne	CA Dennis	-			
Svanes Svanes GoogleFall River GoogleFall River Location: Lat/Long: Accuracy Radius: Domain:	Plymouth, MA US 61.1916, -70.662 10 km	State Eorest Wareham 55 C Sandwic Bourne	CA Dennis	-			
Somer Swansea To GoogleFall River Ca Location: Lat/Long:	Freedom Redenerer Josephile Comparison Comparison Phymouth, MAUS 41,9106, -70.66/2 10 km comcast.net	State Forest Waterham (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	CA Dennis	-			
Some Series Coole Fall River Location: Lat/Long: Accuracy Radius: Domain: Organization:	Preton Preton Acaptore 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	State Forest Waterham (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	CA Dennis	-			
Some Some Coccile Lat/Long: Accuracy Radius: Domain: Organization: Reverse DNS:	Freeton Auguster Auguster Market Mark	State Forest Waterham (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	CA Dennis	-			
Somer Somer Coogle Fall River Coogle Fall River Accuragina Organizations: Reverse DNS: Other Info:	Freedom Contention of the Academic of Acad	Stare Forent Western D T sandare Borrn Borrn	CA Dennis	Report a map of			
Coogle all River Google all River Coogle	Freedom Contention of the Academic of Acad	Stare Forent Western D T sandare Borrn Borrn	Benntable Benntable Mag des 2009 George Term of Los	(124 Report a map of			
Coogle all River Google all River Coogle	Freedom Pyrmouth, MA US 413 104, - 706 Add 10 km comcast: Gala comcast: Gala comcast: Gala comcast: Gala comcast: Gala comcast: Gala Macalla SG (Windows NT 100, Wir Macalla SG (Windows NT 100, Wir	Stare Forent Western D T sandare Borrn Borrn	Benntable Benntable Mag des 2009 George Term of Los	Report a map of			
Coope all fiver Coope all fiver Laction: Lat/Log: Accuracy Radius: Domain: Organization: Reverse DNS: Other Info: Scope: User Agent: Listene: Forwarded:	Freedom Acquiter Acqu	Stare Forest Western Dorne Borne SERRE SERRE	Benntable Benntable Mag des 2009 George Term of Los	Report a map of			
Coope Fall River Coope Coope Fall Coope Fall River Coope Coope Fall Coope Fall River Coope	Freeton Anstheti Anst	Stare Forer United and the second secon	Benntable Benntable Mag des 2009 George Term of Los	Report a map of			
Coope all fiver Coope all fiver Laction: Lat/Log: Accuracy Radius: Domain: Organization: Reverse DNS: Other Info: Scope: User Agent: Listene: Forwarded:	Frenow Anather	Stare Forent Venetarian Director Instance st.met n64, z66). AppleWeb8/67/537,36 (8H	Benntable Benntable Mag des 2009 George Term of Los	Report a map of			
Coope all fiver Coope all fiver Laction: Lat/Log: Accuracy Radius: Domain: Organization: Reverse DNS: Other Info: Scope: User Agent: Listene: Forwarded:	Freeton Anstheti Anst	State Forer T Handheit Wenter Bozne Bozne statet Bozne Bozne st.net Mick Job AppleWeb6/6/5/37.36 (KH whit >10 Bozne Bozne Bit >20 Bit >20 Bit >20	Benntable Benntable Mag des 2009 George Term of Los	Report a map of			

Most Active Users		Most Active User Domains						
User	Events	High Risk	Medium Risk	User Domain	Events	High Risk	Medium F	
brussell@acme.com	120	0	0	acme.com	8610	21	12	
jdavis@acme.com	107	0	0	beanrogers.com	812			
lreed@acme.com	105	0	0	auditlp.com	297	0	0	
agarcia@acme.com	99			Comcast Business	101			
jmorgan@acme.com	99			Comcast Cable	41			
bart@acme.com	96	5	10	Seech-Infocom Ltd.	38		30	
dcook@acme.com	82		0	comcast.net	32			
cbennett@beanrogers.com	68	0	0	comcastbusiness.net	22		3	
kmyers@beanrogers.com	66			Earth Network Technology (HongKong) Co., Limited	17			
					13			
Most Active Locations	Events	High Risk	Medium Risk	Most Active Operations	Events	High Risk	Medium F	
US, MA	8358	13	10	Access	1771	12	7	
United Kingdom	826	0	0	Preview	1170	9	12	
US, FL	329			Download	915	10	22	
US, NC	297	0	0	Modify	785			
US, CT	95			Upload	650			
Ukraine	59	17	36	Сору	644		0	
Hong Kong	19			Delete	635			
Indonesia								
	15		10	AnonymousLinkCreated	469		0 0	
Czech Republic	15 8	5 7	10 1	AnonymousLinkCreated Move	469 452	0		



Third-party Breach

RISK FACTORS

Third-party breaches result from sloppy security procedures by the third party, willful disregard for the organization's security policies or malicious intent by someone who has legitimate access to confidential materials. Even with periodic vetting and contractual agreements in place, data loss risks persist without visibility into what happens to specific documents once they are in the control of the thirdparty.

DETECTION INDICATORS

Any beacon openings beyond the third party network is a clear indicator that the organization's documents leaked from the third party. Anonymous access to beacons and remote openings beyond the third party network is a clear indicator of a likely data loss.

RESPONSE

Restrict third party access to any sources in cloud shares, modify Allure's rule sets to alert whenever a third party access occurs to monitor what documents may be subject to loss.

61%

of surveyed respondents in a 2018 Ponemon Institute study confirmed that their organizations had experienced a data breach caused by a third party, which is up 5% from last year and 12% from 2016.



Link Sharing

RISK FACTORS

It is very convenient for a user to right click and copy a link they email or text to an external party, whether for convenience or laziness. This grants access to a remote party directly to the cloud storage where access may occur anonymously. Any anonymous access is suspicious. Link sharing may be determined by inspecting the history of the file that was accessed to see who last touched the document.

DETECTION INDICATORS

Anonymous accesses are highly indicative of a violation of policy, and the history of file touches may reveal who created and provided a link to the file. Bot accesses are also an indicator that a link was shared and indexing has been initiated by an automated crawler.

RESPONSE

Identify the user who last touched the file in question and investigate whether that person created and shared a link, how it was shared and who it washed with. If the file in question is tagged as sensitive, the user's account may be suspended until the investigation determines the severity of the possible security violation. If the crawler is identified, and the file in question is sensitive, contact the operator of the crawler and ask for all indexes and cached copies of the file be deleted.



-				
Ris		CO	rir	יסי
113	n -			15.

Unknown location (Scope = Unknown): +10 Sensitive files (Tags = Sensitive): +20 File download (Operation = Download): +20 Anonymous user (User = anonymous): +50

DETAILS	NOTABLE EVENTS RELATED EV	IENTS	
	First Tracked: 04/01/2019 11:36 AM EDT	By User: Jonathan	IP Address:
File Name	2:	FY2018 budget.xlsx	
File Syste	m:	AcmeOneDrive	
File Path:		https://acme.sharepoint.com/sites/Finar	nce/Shared Documents/FY2018
File Type:		xlsx	
Beacon Ty	/pe:	Watched	
Descriptio	on:	Add Description	
Last Event		04/01/2019 04:15 PM EDT	
Forbidden	Scope Events:	0	
	Scope Events:	3	
	cope Events:	25	
	on Recipients:		
		Email/SMS	
Tags:		Confidential <u>×</u> Finance <u>×</u> Add a ta	g
			DELETE SAVE



Permission Setting Mistake

RISK FACTORS

Permission setting mistakes are almost always a result of human error. Users don't often check their settings unless something goes wrong or someone from IT alerts them. The sharing of document links without the proper permissions applied allows unauthorized views and may be visible to automated crawlers that can result in search engine indexing by the bot.

DETECTION INDICATORS

Downloading documents not tagged as sensitive and that are remotely opened at unknown or bad geolocations may indicate a mislabeled document. Also, an unusual number of users accessing a documents tagged as "sensitive" or "confidential" may indicate permission settings are too broadly set.

RESPONSE

Public documents are hard to distinguish from mislabeled sensitive documents without investigation. Check the history of the file accesses to determine who may own the document and contact the user to establish the facts.

						filter	items		
Timestamp (EDT)	• Version	User	IP Address	Operation	Scope	Location	Risk Score		
04/01/2019 04:15 PM		kedwards@acme.com	74.94.137.241	Сору	Trusted	Natick, MA US	20	DETAIL	
04/01/2019 08:19 AM		Ireed@lacme.com	74.94.137.241	Access	Trusted	Natick, MA US	20	DETAIL	
04/01/2019 0B:14 AM		rtumer@acme.com	74.94.137.241	Access	Trusted	Natick, MA US	20	DETAIL	
04/01/2019 07:01 AM		hwatson@auditlp.com	204.235.114.167	Access	Unknown	Denver, NC US	30	DETAIL	
03/29/2019 01:54 PM		jackiephillips@acme.com	74.94.137.241	Modify	Trusted	Natick, MA US	20	DETAIL	
03/29/2019 11:31 AM		jenthompson@acme.com	74.94.137.241	Download	Trusted	Natick, MA US	40	DETAIL	
03/29/2019 10:23 AM		mjones@acme.com	74.94.137.241	Access	Trusted	Natick, MA US	20	DETAIL	
03/29/2019 06:07 AM		tgonzalez@acme.com	74.94.137.241	AnonymousLinkCreated	Trusted	Natick, MA US	20	DETAIL	
03/28/2019 12:41 PM		jmorgan@acme.com	74.94.137.241	Access	Trusted	Natick, MA US	20	DETAIL	
03/28/2019 07:41 AM		Ireed@acme.com	74.94.137.241	Сору	Trusted	Natick, MA US	20	DETAIL	





877.669.8883



Request a free risk assessment https://www.alluresecurity.com/free-trial



Allure Security is on a mission to stop data loss that results from theft or mishandling of files. Allure's technology continuously scores risk by analyzing document access and sharing activities inside and outside of an organization's control. Our SaaS application watches log activity in the cloud, enriches logs with geolocation insights, extends visibility beyond the cloud share, and detects leaks and breaches. Allure's actionable insights strengthen data security, detect breaches and leaks early, and inform data loss responses with unique file and user activity-based indicators.



"We rely on Allure Security as a force multiplier for our security team. It is amazing how Allure is able to collect and analyze cloud log data and present it in such an insightful and digestible manner to flag risks, inform our responses and help us enforce policies. Allure is able to give us visibility into our global file and user activity and effectively complements Microsoft's Security Center." --- Antonio Garcia, CISO at GRA