ALLURE SECURITY

ALLURE SECURITY FOR THIRD-PARTY RISK

REDUCE RISK USING ALLURE DECOY DOCUMENTS FOR CONTINUOUS MONITORING AND ASSESSMENT

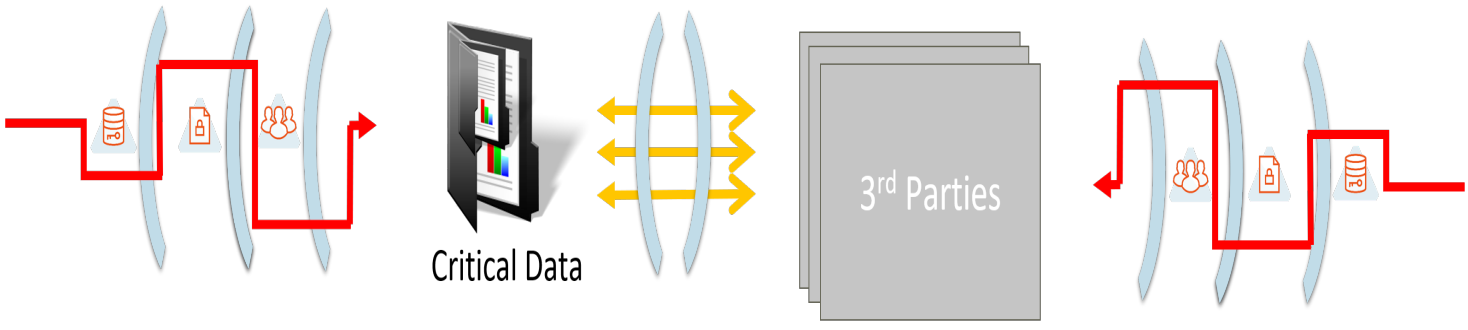
Third-party data breaches are increasing

According to a Ponemon Institute study, 56% of organizations have experienced a data breach due to a vendor, and the average number of third parties with access to sensitive information per organization has increased from 378 to 471. Additionally, only 18% of companies said they know if third-party vendors are sharing this information with others. Organizations also struggle to detect if an attacker gains access to a third party's credentials and attempts to gain access to internal data. To customers, it doesn't matter who's responsible for the breach. It's your business that suffers the reputational and financial cost. This risk is only compounded by new privacy regulations that make organizations liable for third-party breaches. To date, solutions have been scarce. Companies often rely on annual assessments that are limited in scope and/or access controls that are easily compromised. Both approaches have glaring gaps.

Active breach defense to stop data loss

Once a third party is breached, attackers have two paths to your data: access to the shared data itself or access to the internal network to snoop for the crown jewels. Allure tackles both challenges. We track and report on the integrity and security of third-party shares, and internal folders or directories that store your most valuable data. We do this by strategically placing Allure Decoy Documents, deceptive documents with beacons, in third-party folders and file shares. The documents have alluring names that are enticing to would-be leakers and hackers. If opened, inside or outside of the origionating folder or file share, real-time alerts are generated that provide proprietary geofence and telemetry insights. Security teams can then take immediate action to prevent the data loss and identify who is responsible for the breach. Allure's approach helps you both prevent and reduce data loss, and gives you a hard metric against which to measure the integrity of your third parties.

Allure Decoy Documents detect snooping inside the network and third-party shares, and alert if documents go outside the control of a third-party



All tracked activity is logged for historical reference, and detailed geolocation and telemetry data help identify leakers and adversaries

Benefits of real-time data loss detection:

There is a certain level of third-party risk that organizations have come to accept over the years, and it has created two extreme approaches. Some companies prioritize productivity and experience a loss of control once data has been accessed by a third party. Others severely limit access, and accept the loss of productivity and vulnerabilities associated with users not adhering to access policies. Allure provides a realistic approach: visibility without impeding productivity. Not only does this provide more insight into your organization, but third parties tend to be more careful when they know they are being watched and graded.

Manage risk

1. Deploy continuous risk assessment
2. Inform contract structuring and review
3. Achieve ongoing oversight
4. Focus assessment efforts on highest-risk partners
5. Update policies based on data loss findings
6. Document evidence to use in court
7. Provide risk reports to the C-suite
8. Detect if lost documents are posted on public websites

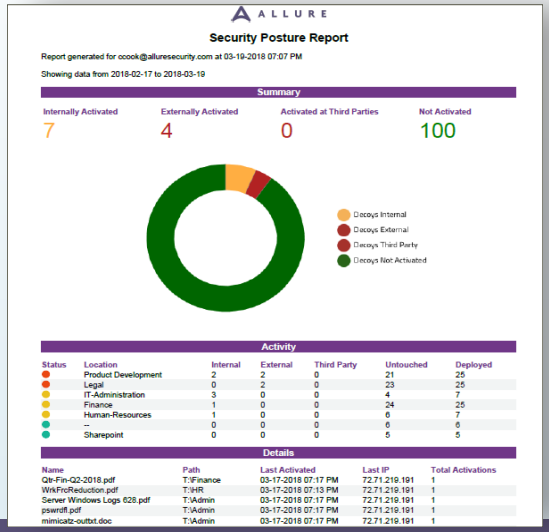
Stop and limit data loss

1. Revoke access to a third party once suspicious activity is detected
2. Take corrective action to prevent future activity
3. Invoke internal endpoint controls to isolate the data loss source
4. Move critical files that are at risk of being stolen
5. Address endpoint vulnerabilities that contributed to the breach
6. Narrow down suspects, and identify leakers and attackers
7. invoke penalty clauses accordingly
8. Gather forensics to determine the extent of a threat

Beacons are undetectable by users

Deploy in minutes

Allure is deployed as-a-service, and requires no software to download, no agents to install and no hardware to configure. Mean time to value is measured in minutes, with virtually no daily overhead from a personnel resource constraint. Allure is the only company to hold patents for decoy documents with beacons, making it making it completely unique in the market. See all patents here: http://www.alluresecurity.com/patents.


ALLURE

Security Posture Report

Report generated for ccook@alluresecurity.com at 03-19-2018 07:07 PM

Showing data from 2018-02-17 to 2018-03-19

Summary

Internally Activated	Externally Activated	Activated at Third Parties	Not Activated
7	4	0	100

Decoys Internal
Decoys External
Decoys Third Party
Decoys Not Activated

Activity

Status	Location	Internal	External	Third Party	Untouched	Deployed
	Product Development	2	2	0	21	25
	Legal	0	2	0	23	25
	IT-Administration	3	0	0	4	7
	Finance	1	0	0	24	25
	Human-Resources	1	0	0	6	7
	--	0	0	0	6	6
	Sharepoint	0	0	0	5	5

Details

Name	Path	Last Activated	Last IP	Total Activations
Qtr-Fin-Q2-2018.pdf	T:\Finance	03-17-2018 07:17 PM	72.71.219.191	1
WrkFrcReduction.pdf	T:\HR	03-17-2018 07:13 PM	72.71.219.191	1
Server Windows Logs 628.pdf	T:\Admin	03-17-2018 07:17 PM	72.71.219.191	1
pswrdfl.pdf	T:\Admin	03-17-2018 07:17 PM	72.71.219.191	1
mimicatz-outtxt.doc	T:\Admin	03-17-2018 07:17 PM	72.71.219.191	1

Want to learn more?
Contact info@alluresecurity.com today.