ALLURE SECURITY

DATA LOSS DETECTION & RESPONSE (DDR)

KNOW IN REAL TIME WHEN DATA IS ACCESSED OUTSIDE OF DEFINED PERIMETERS, MANAGE THIRD-PARTY RISK, IDENTIFY EXTERNAL AND INSIDER THREATS

Data protection is hard

Protecting data without impeding everyday business missions is an almost impossible task. Information Rights Management (IRM) solutions can protect files, but depend on end users properly classifying them and setting file permissions.

Data Loss Prevention (DLP) solutions are good at dealing with structured data, such as social security or credit card information, but poor with less structured information such as trade secrets, HR data, and financial or legal reports.

Organizations need to share documents to conduct daily business, and protection policies are not always followed. So, how do you know if documents are being accessed outside of defined perimeters? And how do you know who the perpetrators are once information has been breached?

Track data loss with Allure Security

Allure Beacons leverage patented geofencing and document telemetry technologies to alert users in real time when documents are accessed inappropriately or maliciously. This is a safeguard for when protection fails, particularly for documents that have been misclassified or trusted with a third party. Alerts include the necessary details to respond to breaches quickly and appropriately.

Allure Decoys are used to drastically reduce dwell time and identify hackers doing reconnaissance. Allure plants fake representations of real documents to track hackers. They will think they've stolen high-value documents, when instead they've accessed bogus information, and you are alerted to this activity.

Beacons and Decoys work independently or together to complement data protection initiatives, detect data loss and identify adversaries.

Know when and where documents are opened, and get detailed access information

Beacon alerts are customized based on an easily-managed perimeter.
All tracked activity is logged for historical reference.

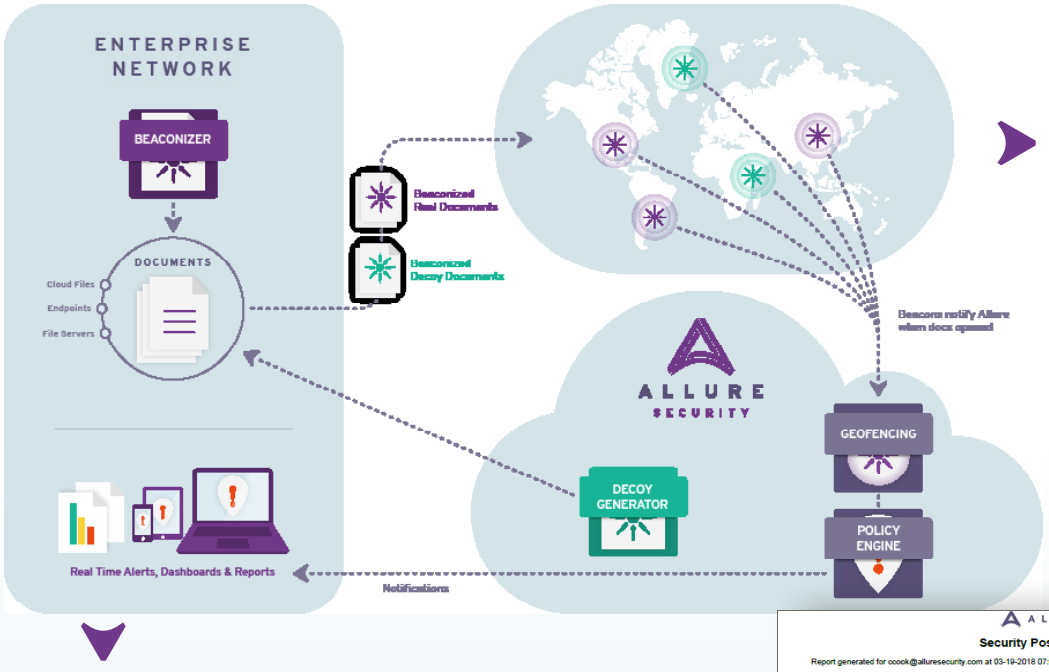
How customers use Allure Security:

1. **Third-party risk**: If a beaconized document leaves a third party, you'll receive an alert when that document is opened, initiating the appropriate response and limiting the financial and reputational damage to the company. This provides peace of mind as regulations like GDPR make organizations responsible for third-party breaches.

2. **Archived document monitoring**: For documents meant to always be at rest, beacons allow you to track opens as a way to monitor for suspicious and malicious activity, whether archived internally or at a third-party hosting site.

3. **Decoys for deception**: Allure Decoys allow you to create and plant fake documents to track an adversary with fake data, and detect attempts at compromising the real data. Dwell time is significantly reduced, and quick actions can be taken to identify the perpetrator and better protect the targeted information.

4. **IRM and DLP support**: Allure's technology is frequently included in IRM and DLP strategies. Beacons detect when documents escape protection measures, track high-value documents while protection initiatives are in progress and assist with document classification efforts.

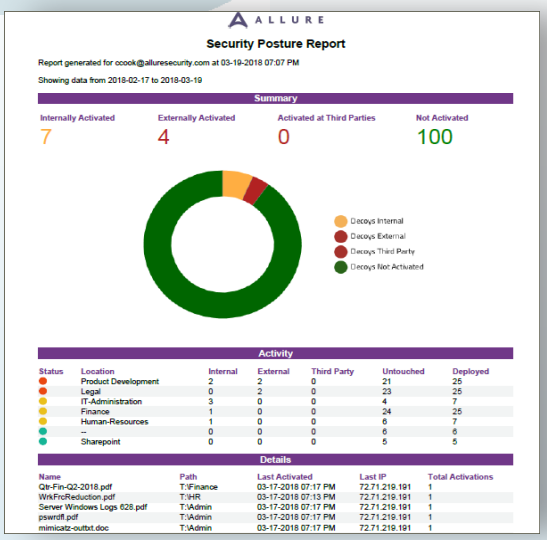


Undetectable by users

Users see no change to the document and there is no interuption in experience.

Deploy in minutes

Deployed as-a-service, customers can drag and drop files to be beaconized via Allure's web-based portal, or download and use Allure's desktop app (Mac or Windows) to beaconize individual documents, entire folders or directories, on-demand.


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
pswrdlt.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.