ALLURE
SECURITY TECHNOLOGY

DATA LOSS DETECTION & RESPONSE (DDR)

EASILY DETECT INTRUSIONS WITH BEACONIZED DECOY DOCUMENTS

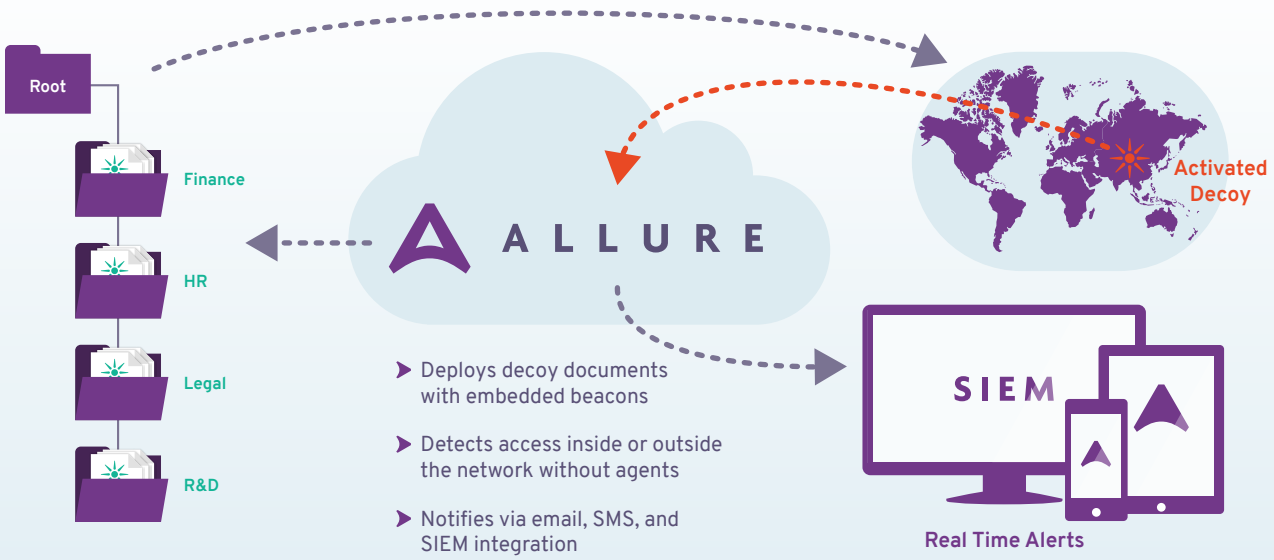
The Current Situation

Despite extensive deployments of numerous security technologies, breaches occur repeatedly—and go undetected for months. Organizations have focused on protecting their networks, applications, endpoints, and users, leaving their data to fend for itself. They typically have no idea when critical documents are accessed by malicious users, especially once those documents leave their network. This leaves them blind to internal breaches by insiders and Advanced Persistent Threats (APTs).

The Allure Solution

Allure DDR cuts through the white noise of endless security events and avoids the complexity and IT operational challenges of honeypots and honeynets. Instead, it protects the same critical assets that your adversaries are targeting by deploying "beaconized" decoy documents into your existing infrastructure. These decoys look and act like any other files, except that they are tracked wherever and whenever they're accessed—on PCs, mobile devices, or in the cloud. There are no agents to install, and Allure DDR alerts you as soon as the documents are accessed. Alerts can come from internal users overstepping their intended activities, or they can be a sign of an APT that's well underway.

Allure DDR cuts through the white noise of security events and alerts you to undetected insider threats and APT activity



Decoys That Work

The best place to detect activity related to your critical assets is by focusing right where the documents are located—in your file systems. Extensive research from Columbia University, funded by the U.S. federal government for nation-state security use, has identified several key aspects of a successful decoy-based intrusion detection system:

- **Believable** — The documents need to appear authentic.
- **Enticing** — They need to appear to contain information attractive to a threat actor.
- **Conspicuous** — They need to be deployed in a place where they're likely to be uncovered.

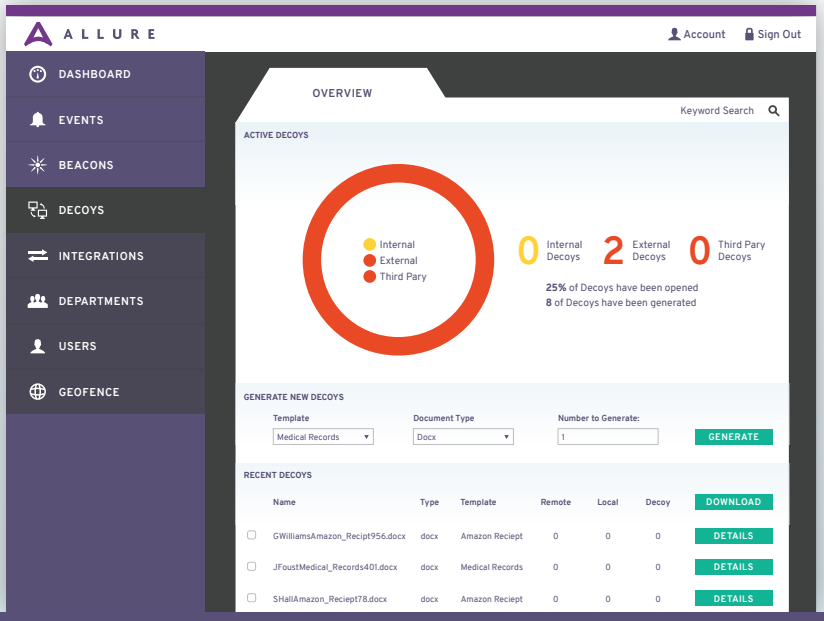
Done properly, this research concludes that a decoy-based system can detect over 99.9% of intrusion attempts with as few as 20 decoy files in five locations.

The Allure Approach

The Allure solution is based on "beaconized" decoys that are easily deployed in conspicuous locations.

- **Enticing documents** – Allure automatically generates and distributes fake PDF and Microsoft Office documents that contain enticing, believable decoy information, such as financial records, personally identifiable information (PII), and other commercially sensitive data.
- **Beaconized** – Allure applies proprietary beacon technology to each document, so that every access is tracked, without the need for agents, whether inside or outside the corporate network.
- **High efficacy alerts and reports** – When a decoy document is accessed, it's a highly reliable indicator of threat activity. Allure alerts you via SMS, email, or events sent directly to your SIEM. A secure Web portal shows the status of your decoy documents. You can drill down into details regarding who accessed each decoy, when, and where. Periodic reporting keeps you up to date with the state of your deployment.

Deploy decoy documents in minutes and monitor their status



Deploys in Minutes

Allure DDR is a SaaS application, so there's no hardware or software to set up, manage, or maintain. Once your account is created, you can begin deploying decoys and monitoring their status in minutes. Simply generate a set of fake yet believable decoy documents based upon our built-in templates, download them to your environment, and execute the included deployment application.

Dependable Alerting and Tracking

Once deployed, Allure helps provide continuous protection against both insider threats and APT—because it doesn't rely upon any of the other security controls in your environment. Allure *tracks the data itself*, providing a uniquely reliable solution with an extremely low rate of false positives. Wherever the data goes, inside or outside of your network, Allure knows—and you know, too.

Be alerted to accesses, both inside and outside the corporate network

Want to create and deploy decoy documents in minutes and detect insider threats and APTs lurking in your organization? Contact info@alluresecurity.com to get started today.