

REDUCE DATA LOSS & HOLD ADVERSARIES ACCOUNTABLE

GET REAL-TIME ALERTS, RESPOND QUICKLY, IDENTIFY LEAKERS AND ADVERSARIES

Data Loss is Pervasive and Costly

Data loss has plagued organizations since the beginning of the computer age. As technologies for sharing and storing data evolve, the challenge of protecting that data becomes more difficult. Compounding the problem is the growing need for companies to share more data with growing numbers of third-party partners and outsourcers, and increasing privacy regulations restricting who can have access to certain data. Failure to protect data results in exorbitant costs. The Ponemon Institute's 2018 Cost of Data Breach Report sites the average cost of a breach is \$3.68 million, noting that the cost significantly increases depending on how many records are stolen: \$40 million for 1 million records lost; up to \$350 million for 50 million records lost.

Companies have tried to tackle this issue from many angles: DLP, encryption, network, endpoint and data access management, secure collaboration, etc. Yet, breaches keep occurring - 241 breaches were reported in the first half of 2018, according to the Privacy Rights Clearinghouse. This is because no matter what security tool is in place, people either find ways to get around them for convenience purposes or they accidentally open the door for an adversary to masquerade as a trusted employee or contractor and bypass the very systems designed to deny them access to confidential data.

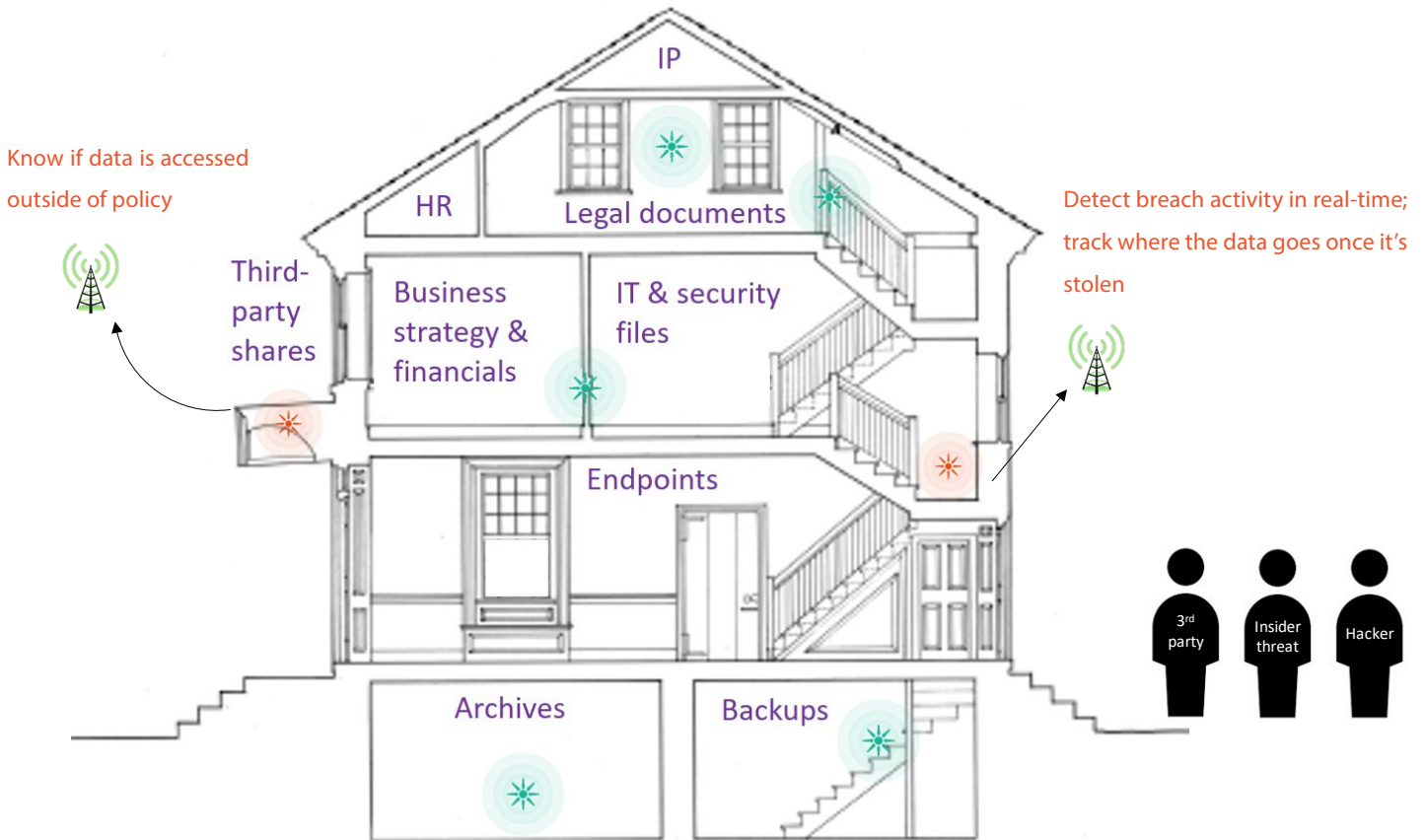
Even worse, more and more breaches are going undetected. The SANS 2018 Survey on Endpoint Protection and Response polled 277 IT professionals on endpoint security concerns and practices. The number of those who didn't know they had been breached jumped from 10% in 2017 to 20% in 2018.

Why detection?

All security tools designed to protect or prevent data loss rely heavily on trusting users to correctly classify documents, manage access controls and protect credentials. Hackers can take advantage of this by targeting employees and third parties to steal credentials, which gives them the access they need to perform their malicious intent. According to the 2017 Verizon Data Breach Investigations Report, 81% of breaches leverage stolen credentials.

Ask yourself:

1. How does encryption help if someone gains access to the keys or misuses authority?
2. What good are content collaboration security controls if credentials are stolen?
3. What happens to files once they are downloaded from a third-party share?
4. How can user behavior analytics monitor activity outside of the network?
5. What happens when DLP fails to block IP from leaving the network?



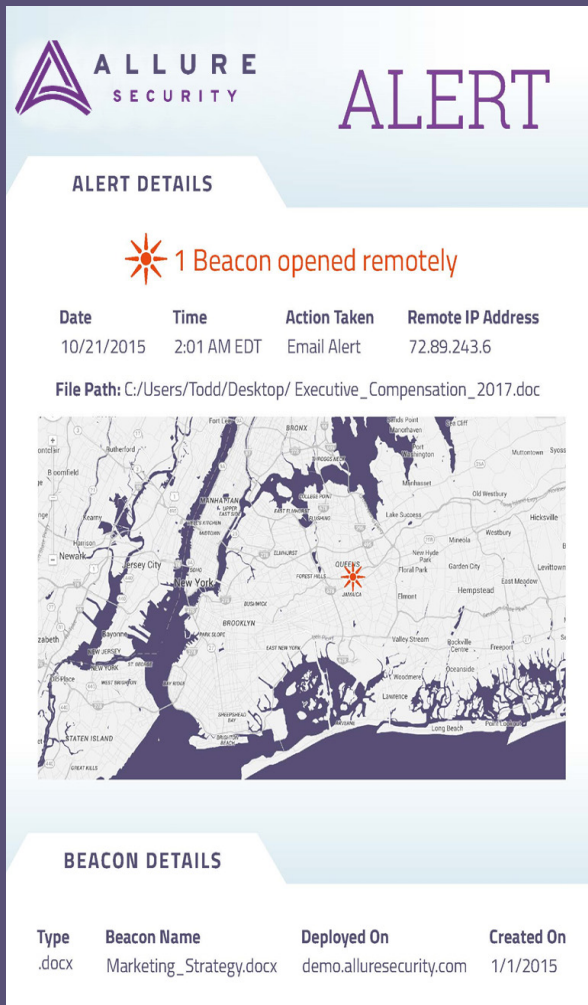
Install an alarm system with GPS for confidential data

Prevention alone won't stop data loss, just as installing locks on doors and windows won't keep determined burglars out of your home. And just like businesses, everyday needs require homeowners to give numerous people keys. Family and friends visit; neighbors bring in the mail, water plants or watch pets; and service workers like housekeepers, dog walkers and contractors come and go. Additionally, mistakes happen. The front door may be locked, but what if one of the kids left a window open?

Homeowners rely on alarm systems as a practical line of defense. If a thief gains access to a home, the alarm alerts the homeowner to call authorities. The alarm system also collects valuable information, like point of entry and video footage, to help authorities resolve the threat and catch the bad guy. With this insight, the homeowner can also address the vulnerability to prevent future theft.


Given the even greater complexity of our digital data, it seems only obvious that we should be putting alarms in these properties as well. Organizations must invest in technology solutions that go beyond prevention, and focus on detection and response. Data Loss Sensors, which act as an alarm system with GPS for confidential data, are deployed directly where the data is stored to give security teams the visibility they lack. Allure distributes beaconized documents that blend into companies' operational on-prem file systems and cloud file shares. Strategically placed with file names that are proven to be of interest to today's attackers, these Data Loss Sensors alarm when they are searched and opened. Data Loss Sensors act as silent tripwires when malicious insiders or adversaries attempt to gain access to confidential data, and report geofence and telemetry data in real-time.

A Data Loss Sensor is triggered. Now what?



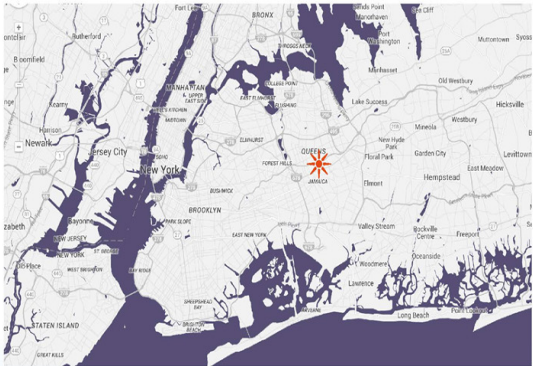
ALLURE SECURITY ALERT

ALERT DETAILS

 **1 Beacon opened remotely**

Date	Time	Action Taken	Remote IP Address
10/21/2015	2:01 AM EDT	Email Alert	72.89.243.6

File Path: C:/Users/Todd/Desktop/ Executive_Compensation_2017.doc



BEACON DETAILS

Type	Beacon Name	Deployed On	Created On
.docx	Marketing_Strategy.docx	demo.alluresecurity.com	1/1/2015

A detected breach informs security teams that a perpetrator is performing activities indicative of the early stages of an attack, and that an investigation needs to evaluate the activity, put countermeasures in place and identify the perpetrator. Just like the home security system example above, Allure alerts provide high value information to aid in operational and incident response as well as architecture review. Once a Data Loss Sensor is triggered, the following actions can be taken to prevent and limit data loss:

1. Revoke access using available permission controls
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 if the breach is caused by a third-party
8. Gather forensics to determine the extent of a threat by correlating with other threat intel
9. Detect if lost documents are posted on public websites
10. Update data security and compliance policies based on data loss findings

Who stole what data and where is it now?

When a breach takes place, the most pressing questions for the security team include:

1. What data was taken?
2. Where did it go?
3. Who did it?

Allure's alert information contains geolocation and telemetry details to help answer all three questions. Allure also works with customers to ensure the data is transferred to appropriate legal representatives, who maintain custody of the data for any subsequent legal proceedings.

Catch leakers and adversaries in the act

Attacker behavior generally follows several discernible phases. Network reconnaissance and scanning leads to initial compromise. Attackers typically acquire credentials within the victim's network by targeted phishing attacks. Attackers will then install malware, such as Remote Access Trojans, to maintain long-term persistence in the victim's network. While in the network, attackers will search and identify, acquire and bundle the data they ultimately exfiltrate. By the time the adversary reaches this phase, all existing security controls and prevention solutions have failed. However, when the attacker searches for valuable data to steal, Allure's Data Loss Sensors detect and inform security personnel of the attacker behavior.

Data Loss Sensors detect breach activity during the following stages of an attack:

1. Casing from the inside

Once inside the network, a data thief will first evaluate the access and files immediately available at the entry point. Next, the thief will try to upgrade credentials by searching for documents containing passwords, usernames, VPN instructions, email accounts, etc., located in IT and security repositories. Data Loss Sensors in these documents will send alerts when this type of suspicious activity is detected.

2. Searching for valuable property

Once the thief has full access, the next step is to riffle through the folders and directories most likely to contain high-value information, like archives, HR documents, executive and finance folders, and third-party shares. This can be done manually or via search algorithms, either of which uncover enticing files names. Data Loss Sensors in aptly named documents will trigger an alert when they are opened at this stage of an attack. It's like having alarms directly in the jewelry box and sock drawer.

3. Identifying and acquiring valuables

The thief will then narrow down targets and determine which documents potentially have the most value. The data will then be packaged into easy to export bundles, like zip files. It's common for files to be opened before exfiltration, similar to how a home thief might take a closer look at a valuable before putting it in a sack, which will trigger a Data Loss Sensor and send an alert. Data Loss Sensors also travel with the data after exfiltration and will alert when activated outside the network.

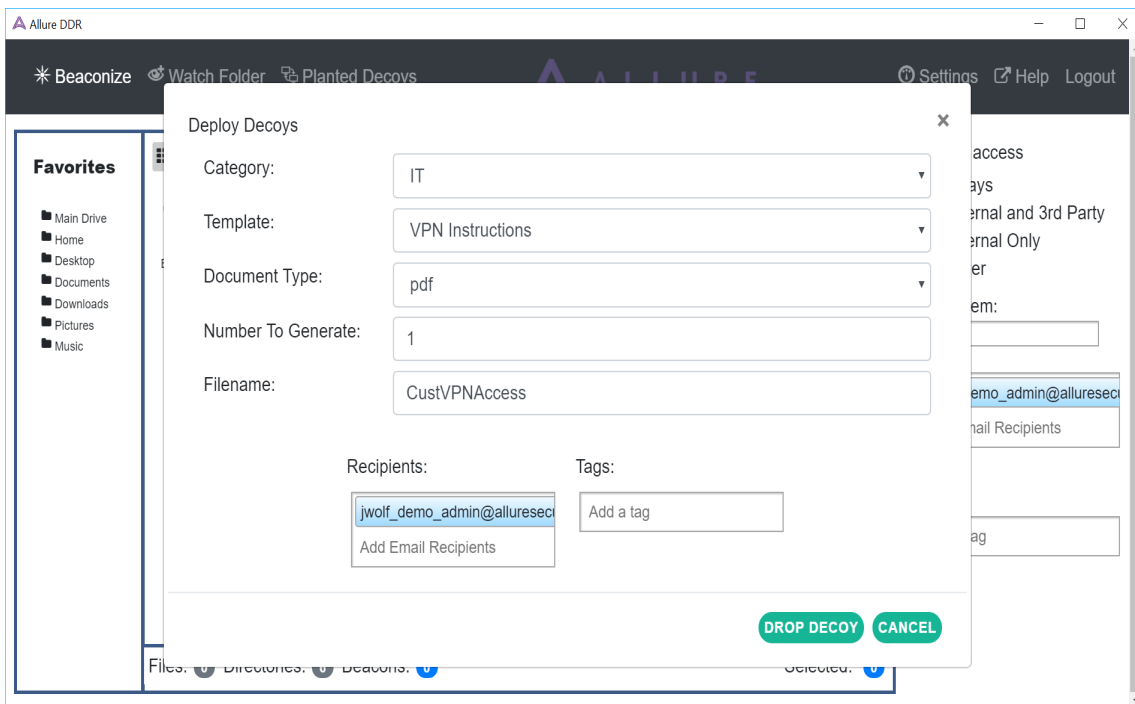
4. Fencing the goods

In order to sell valuable data to the highest bidder, the data thief must make it available for verification by the buyer. Data Loss Sensors help you know if confidential data is uploaded to public sites, and send alerts showing when, where and by whom files are opened once they leave a defined perimeter.

Deploy in minutes

Allure Security is deployed as-a-service, agentlessly. Data Loss Sensors track and report on the integrity and security of third-party shares and internal folders or directories that store your most valuable data.

Allure's desktop app (Mac or Windows) beaconizes individual documents, and entire folders or directories, on-demand. Users see no change to the documents and there is no interruption in user experience. Allure's user interface helps determine the names and placement of sensors based on file structures and extensive attacker behavior research. The Data Loss Sensors are designed to be enticing to attackers, quickly capturing their attention while they search for files to steal.



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

Citations:

[Ponemon Institute's 2018 Cost of Data Breach Report](#)

[Privacy Rights Clearinghouse](#)

[SANS 2018 Survey on Endpoint Protection and Response](#)

[2017 Verizon Data Breach Investigations Report](#)