

ALLURE SECURITY FOR THIRD-PARTY RISK

REDUCE RISK USING DATA LOSS SENSORS FOR CONTINUOUS ASSESSMENT, IDENTIFY SNOOPERS & BAD ACTORS IN REAL TIME

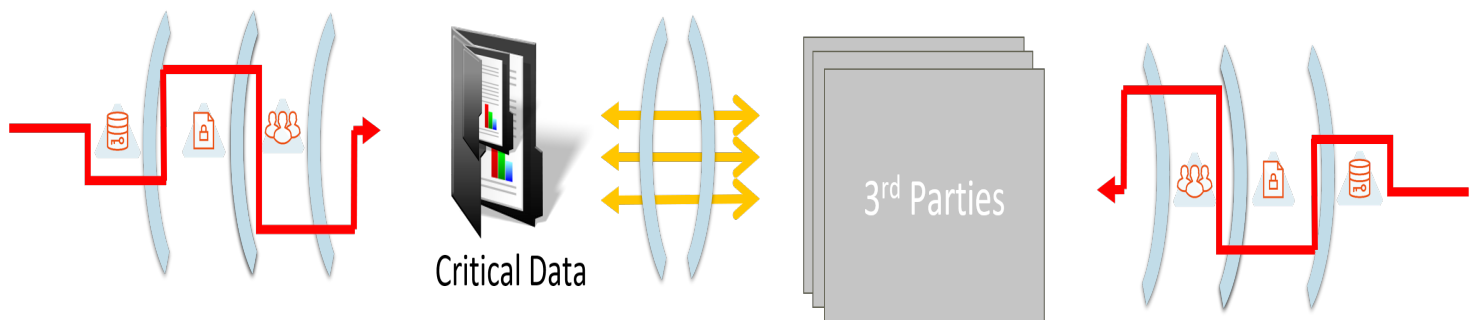
Third-party data breaches are increasing

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.

Sense breach activity 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 placing Data Loss Sensors in a combination of real and fake documents, depending on your third-party sharing practices. Sensors within fake documents identify data loss at the reconnaissance phase. Sensors in real documents track access and document flows associated with everyday business activities, and alert you in real time if this data flows outside of a third party and makes a second hop. Security teams can then take immediate action to prevent the data loss and identify the would-be leaker or adversary. Allure's approach helps you both prevent and reduce data loss, and gives you a hard metric against which to measure your third parties.

Data Loss Sensors 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 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 practical approach: visibility without impeding productivity. Not only does this provide more insight to 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



Undetectable by users

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

Deploy in minutes

No agents are required. Deployed as-a-service, Allure's desktop app (Mac or Windows) beaconizes individual documents, entire folders or directories, on-demand.

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

