Clean Up Data Spills with Cofense Vision

Automatically Hunt & Quarantine Across Entire Email Environments

Business Challenge

A data spillage is a security incident that occurs whenever sensitive or protected information is spilled onto a system, or to an individual or group of individuals, that is not authorized to process or handle such information. Examples include systems with a lower level of classification, unauthorized groups (e.g., NOFORN), or prohibited network enclaves. Data spills occur because it is so common and easy for employees to improperly handle large volumes of sensitive or classified data in a world of increased information sharing. And while enterprise-wide cyber security controls are essential to prevent spills from occurring in the first place, accidental email distribution of protected information is a typical fault that leads to a data spill. Making matters more difficult are the constant re-classification of information or improperly marked files or media. While most data spills are unintentional, it's usually because of poor user awareness or careless disregard for procedures. Whether these leaks are accidental or willful, it is essential for security teams to quickly scope, isolate, and contain the spill. Email presents a particularly difficult environment for security teams to scope and contain spills quickly. The challenges include poor native email search performance, reliance on email teams to assist, limited search scope, and unfulfilled compliance requirements.

Solution

Cofense Vision is a customer-hosted solution that stores and indexes copies of emails in a dedicated appliance. This enables fast threat hunting and quarantine across the entire email environment so security teams can quickly answer the questions "where has the information been sent?" and "who else received the information?" and then remove the information from all recipients' inboxes instantaneously. This removes reliance on email teams as searches in Cofense Vision occur against an offline copy of received emails allowing the security teams to contain data spills quickly without interacting with email teams. Searches can be conducted against a broad range of attributes such as sender, subject, attachment name/hash and mime type to fingerprint the leaked information and then quarantine the spilled data with a single click. Cofense Vision includes extensive auditing capabilities of search and quarantine actions to satisfy compliance obligations.

Challenges with current methods include:

Poor native search performance in Exchange and Office365. These environments are not optimized for fast threat hunting. Native searches, and searches by solutions that leverage native capabilities such as EWS are throttled to avoid impact on mail delivery performance. As a result, searches take an extended amount of time, increasing the time from data spill detection to containment.

Reliance on Email (messaging) Teams. Search and quarantine activities require elevated rights and privileged access is typically limited to email administrators. SOC teams often need to make a request or submit a ticket to mail teams to perform a search and initiate a quarantine, which can take hours or days. Additionally, email teams are focused on email delivery performance resulting in cross-team process delays that increase data spill exposure time.

Limited search scope. Native capabilities provide limited search criteria – e.g., sender and subject, making effective hunting difficult. Often, mail admins create scripts using PowerShell creating supportability issues. Some of native mechanisms have mailbox limits, requiring extensive work in large environments to ensure data spills are scoped and removed.

Unfulfilled compliance requirements. The Department of Defense and Intelligence Agencies require strict auditing to meet compliance obligations. Native search capabilities, and user-built scripts do not provide required levels of visibility and auditing to satisfy compliance needs.

> *Data spills occur because it is so common and easy for employees to improperly handle large volumes of sensitive or classified data in a world of increased information sharing. And while enterprise-wide cyber security controls are essential to prevent spills from occurring in the first place, accidental email distribution of protected information is a typical fault that leads to a data spill. Making matters more difficult are the constant re-classification of information or improperly marked files or media. While most data spills are unintentional, it's usually because of poor user awareness or careless disregard for procedures.*

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of close to 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn.

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175