Reduce False Positives with Language-Powered, Advanced DLP

SUMMARY
Detect accidental or malicious loss of sensitive PII and PCI over email

Reduce false positive rates seen with legacy DLP solutions with language-based models that identify sensitive data within email context

Configure remediation actions in compliance mode (monitor and detect) or block mode (delete or block)

COMPATIBILITY
Office 365
Google Workspace
Microsoft Exchange

DEPLOYMENT
SaaS solution connected over API

CONTACT US
+1 (650) 260-5352
info@armorblox.com
www.armorblox.com

One of the biggest issues facing cybersecurity is around how businesses can better detect and prevent the loss of sensitive and confidential data. According to the IBM Cost of a Data Breach Report 2021, business email compromise is the number one initial attack vector resulting in the highest average total cost at $5.01 million. This is closely followed by phishing at $4.65 million, while attack vector by malicious insider(s) comes in at $4.61 million.1

Security teams want accurate detections, decreased false positives, and reduced manual incident investigation. This is a place where legacy DLP solutions fall short. Most legacy solutions that rely on conventional rules create unnecessary overhead for security teams with countless alerts. The high rate of false positives can result in security teams being pulled away from higher value activities or ignoring alerts altogether, due to limited bandwidth. This results in true data leaks not being investigated or prevented.

Problem
With the rapid growth of cloud-based communications, legacy DLP solutions have proven tedious, ineffective, and difficult for security teams. Downsides that security teams may have overlooked previously: false positive rates or tedious policy writing, are now reasons to look for alternative solutions. The problem with legacy, rule-based policy setup is that effectiveness is based on the ability to accurately predict situations. Unfortunately, this is near impossible when dealing with human behavior, resulting in limited instances where DLP detections are accurate. Organizations are looking for a new approach to DLP technology. Such as, implementing context identification to expand protection to all data types and applying natural language understanding (NLU) and deep learning to reduce false positives. In order to combat the restraints of antiquated legacy DLP technology, organizations look for solutions that bring language-powered capabilities to data loss.

Armorblox Advanced Data Loss Prevention
Armorblox Advanced Data Loss Prevention uses NLU and deep learning to bring intelligence to DLP. Understanding the content and context of email communications, Armorblox protects organizations from data loss while reducing false positives attributed to legacy DLP solutions. Armorblox ML models analyze and track user behavior and communication patterns to quickly identify anomalies that can lead to the exposure of sensitive PII (SSN, passport numbers), PCI (bank account numbers, credit card numbers), or encrypted account passwords contained within email or attachments to unauthorized recipients. Compared to rule-based policy setup, Armorblox protects all data types proprietary to organizations through custom policies and identifiers. Based on severity and occurrence preferences, remediation actions are automatically applied in the instance that sensitive data is detected within email communications, decreasing the need for manual intervention of upkeep.
Reduce false positives by applying NLU to improve efficiency of security operations

Benefit
Inclusion of NLU adds an intelligent layer to DLP, ensuring increased accuracy when protecting organizations from data leaks. Unlike legacy DLP solutions, Armorblox NLU-powered DLP improves detection and protection of sensitive data while reducing false positives in DLP alerts by 10x. 

DLP remediation actions can be configured in compliance mode (monitoring and detection) or block mode (applying enforcement actions such as delete or block delivery) if emails contain the wrong recipient or attachment. Visibility into incidents, trends, and auto-remediation actions provide a single-pane-of-glass view to monitor organization compliance health. Employee risk assessments provide insight and actions (revoke, block) necessary to maintain compliance.

Prevent accidental or malicious exposure of sensitive data by combining user-behavior analytics, content analysis, and insights from business workflows conducted over email

Benefit
Armorblox machine learning models analyze and track user behavior and communication patterns to quickly identify anomalies that can lead to the accidental or malicious exposure of sensitive PII, PCI, or passwords over email communications. Classification of sensitive data is unique to each organization (merchant codes, medical or patient records, routing numbers). Armorblox identifies and protects all data types to prevent data loss across business workflows.

Armorblox understands user behavior individually and across the organization, such as how and who the user communicates with, and frequency of interactions. Anomalies across communications paired with analysis of email attachments in outbound emails allow for quick and accurate detections to prevent data loss.

Save time and automate security response with custom policies versus static rule-based policy setup

Benefit
Armorblox understands data types that are critical for organizations in order to meet PII and PCI compliance requirements, with customizable auto-remediation actions applied across policies. Unlike static rule-based policy setup, Armorblox provides the opportunity to create custom policies that detect the presence of any data proprietary to the business or organizational workflow. Custom policies can include medical record numbers, identification numbers for vendors or customers, codenames for internal products, and specific acronyms or keywords considered IP. Custom policies are coupled with AI and ML-based detections that adapt and learn over time. This provides increased protection of sensitive data and automates security response for organizations.

Armorblox Advanced Data Loss Prevention brings intelligence to DLP to protect organizations from accidental or malicious exposure of sensitive data. Language-powered DLP reduces false positives and improves accuracy, while custom policies automate security response.