Data Sheet

mimecast

Compliance Monitoring

Gain control, modernize supervision workflows, and minimize risk with Mimecast's Supervision solution

Today's financial services firms face regulatory requirements set by FINRA, the SEC, IIROC and FCA to establish supervisory policies, implement safeguards to protect client record privacy, monitor accuracy of disclosures, and authorize any alterations.

These firms face regulatory audits to prove that they have supervised their key personnel. All types of communication need to be captured and reviewed, including email, public social media, enterprise collaboration, and instant messages.

Supervision review personnel must sort through large volumes of data sets to find any evidence of malfeasance in a timely manner. When identifying potentially risk-laden content, they must flag it for further review and route relevant data via workflow. Managers must be able to monitor and report on reviewer productivity to understand where bottlenecks occur in the review process.

To demonstrate compliance, integration with an enterprise archive is a key requirement for compliance supervision to preserve relevant content and provide chain of custody and detailed audit and access controls.

The volume of digital content in today's organizations is overwhelming. There is no feasible way for reviewers to view all communications content without the right digital assistance and productivity tools.

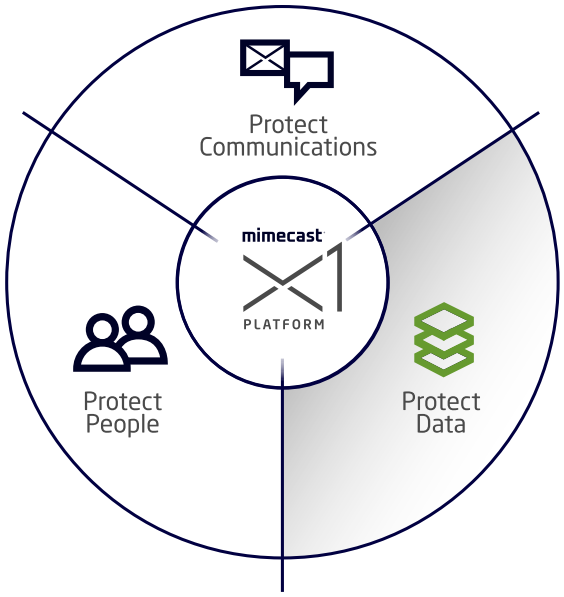
Key Benefits
Data Supervision

- Reduces false-positives with accurate, targeted data selection
- Increases productivity and review efficiency
- Customizes flexibly to meet your organizational needs
- Provides key insights and analytics reporting to identify and address workflow bottlenecks

Confidently meet regulatory requirements

Mimecast's Supervision solution enables compliance personnel to systematically review and discover targeted data among the volume of communications organizations face today. Integrated with the industry leading Mimecast Cloud Archive, users can facilitate an auditable, managed supervision review process, flexible to meet the needs of the business while utilizing a scalable, immutable SEC 17A4 validated and tamper-proof archive.

To reduce the number of false positives in sampling data, targeted detection rules can focus on specific senders/recipients and to accelerate the process. In addition, queues can be configured with an upper limit upon which to be populated with email. This helps limit the amount of email a reviewer must go through while still identifying risk. Today's supervision demands require reviewers to be highly productive.



Tools to simplify review

Supervision includes numerous capabilities to allow organizations to react, customize and modify supervision workflows as necessary in addition to being more productive including hit highlighting, keyboard shortcuts, custom labels, and advanced filtering. These help the reviewer easily navigate through their queues, refine the list of messages with flexible filters, quickly identify the offending content, and efficiently perform actions on emails.

Customized workflow

Messages can be moved from one queue to one or multiple escalation queues depending on the desired outcome. Also, messages from multiple review queues can be escalated to a single escalation queue for simpler final review.

Multi-tier escalation

Different review teams can be associated with each group of monitored employees and each type of violation. Separate escalation teams can also be assigned to further review and make final determinations on items identified as problematic by the initial review teams. Reviewers and Escalation Managers can leave comments on reviewed messages to provide context around their decision making.

Reviewer productivity reporting

Reports on the volume of items reviewed by each reviewer on each team over time allow supervision administrators to ensure that all reviewers are executing their assigned review work.

Configuration tracking and evidence of review reports

Finally, firms must be able to demonstrate compliance with regulations and illustrate the process and enforcement mechanisms that help them comply. To meet these needs, Supervision audits all changes to configuration so that you can demonstrate exactly how the system was configured at any point in time. This includes which rules were used to find violations, which lexicons applied to monitored employees and who was tasked with review of each group of messages. Additionally, Supervision reports at the policy and individual level provide evidence to regulators that you selected messages in accordance with your stated review policy and that these messages were ultimately reviewed.