Proofpoint Automate

Optimierter Prüfvorgang und Reduzierung der False Positives dank Machine Learning

Durch die bahnbrechenden Umwälzungen im Bereich der digitalen Kommunikation werden mehr Inhalte – und mehr Inhaltstypen – generiert als je zuvor. Diese „Informationslawine“ setzt ihrerseits weitere Umwälzungen in Gang. Künstliche Intelligenz (KI) und Machine Learning (ML) sollen die Überprüfung der Compliance und E-Discovery transformieren. Doch auch wenn sich die für Compliance, Überwachung und rechtliche Aspekte zuständigen Teams auf die Versprechen von KI freuen, haben sie mit der Realität zu kämpfen. Diese Technologien sind häufig ineffizient, teilweise einfach nicht effektiv – und die meisten lassen sich nicht skalieren.

Proofpoint Automate kann Ihnen helfen. Als Bestandteil der Proofpoint Digital Communications Governance-Produktfamilie ergänzt die Lösung die umfangreichen Erkennungs- und Analysefunktionen von Proofpoint Supervision, sodass Ihr Überprüfungsvorgang erheblich optimiert wird.

Die im Finanzdienstleistungsbereich und anderen regulierten Branchen geforderte Überwachung der Kommunikation ist seit jeher ein Balanceakt. Unternehmen müssen ein weites Netz auswerfen, um alle relevanten Compliance-Probleme zu finden. Werfen sie es jedoch zu weit aus, kommt es zu False Positives – und damit zu zusätzlicher Belastung für die zuständigen Teams.

Proofpoint Automate ist ein Add-on für Proofpoint Supervision, das die Belastung Ihrer Prüfer mithilfe von ML erheblich verringert. Sie können Proofpoint Automate-Modelle (also den Code, mit dem sämtliche Kommunikationsformen bewertet werden) problemlos bereitstellen, validieren und implementieren. Dadurch können Sie die Entscheidungsfindung im Hinblick auf die Überwachung verbessern und wesentliche Teile Ihres Workflows automatisieren.

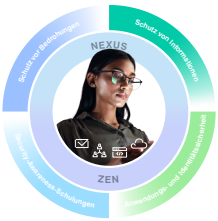
Anders als eigenständige ML-Tools baut Proofpoint Automate auf den schon sehr umfassenden Workflows und Berichten auf, die in Proofpoint Supervision verfügbar sind. Wenn Sie Proofpoint Automate hinzufügen, können Sie die Effizienz und Effektivität Ihrer Überwachungsmaßnahmen noch weiter steigern und gleichzeitig die Kosten weiter senken.

Reale Ergebnisse

Bei Tests konnte die Zahl der False Positives durch die Verwendung von Proofpoint Automate mit der Kennzeichnungsdeduplizierung-Funktion um bis zu 84 % reduziert werden. Natürlich werden die Ergebnisse für jeden Kunden unterschiedlich ausfallen, da die KI-Modelle, die Datensätze und das Training von Modellen je nach Unternehmen stark variieren können. Proofpoint Automate-Kunden berichten jedoch über folgende Verbesserungen:

- 25–50 % weniger False Positives
- ROI von durchgängig 125 % pro Jahr

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.



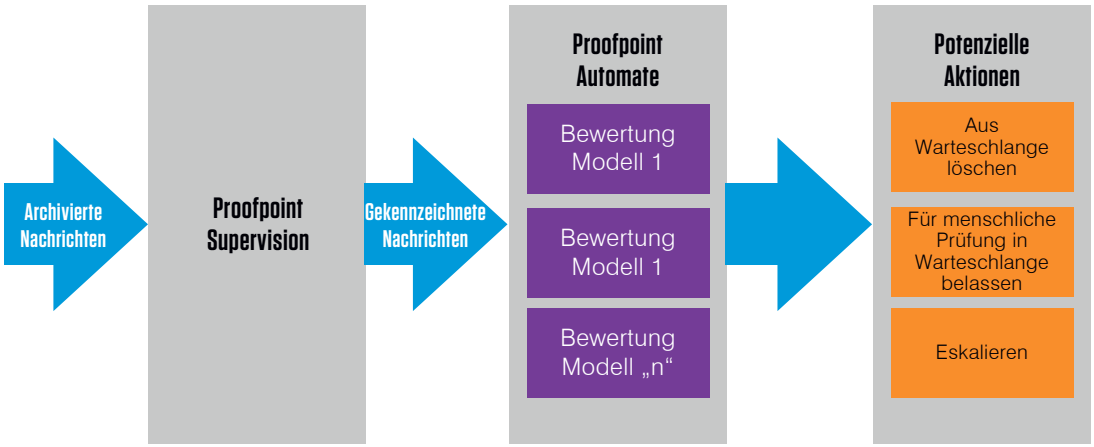


Abb. 1: Workflow von Proofpoint Supervision mit Proofpoint Automate.

Proofpoint Automate-Modelle haben für Kunden, die das Add-on schon länger einsetzen, bereits die folgenden Verbesserungen ermöglicht:

- **Erkennung von Haftungsausschlüssen:** Für vorab genehmigte Inhalte wird der Text für Haftungsausschlüsse vorgeschlagen, die der Konfiguration von Proofpoint Supervision hinzuzufügen sind.
- **Erkennung von Ausschlüssen:** Es werden Versender (z. B. von Newslettern) und Betreffzeilen vorgeschlagen, die der Konfiguration von Ausschlussregeln hinzuzufügen sind.
- **Automatische Prüfung:** Gekennzeichnete Nachrichten werden einer Zweitbewertung unterzogen. Dabei besteht die Möglichkeit, die Nachrichten nach Bedarf intelligent zu löschen oder zu eskalieren.

Diese Verbesserungen sind erst der Anfang. Das offene, skalierbare KI-Modul von Proofpoint Automate kann komplexere und vielfältigere Klassen von kommunikationsbezogenen Entscheidungen handhaben. Dazu zählt die Erkennung von betrügerischen, belästigenden, diskriminierenden und nötigenden Aktivitäten sowie weiteren Richtlinienverletzungen. Mit Proofpoint Automate kann Ihre Implementierung der Proofpoint Intelligent Compliance-Lösung einen noch größeren geschäftlichen Unterschied machen.

Modelle für die Automatisierung und Optimierung der Überprüfungsabläufe

Bei herkömmlichen Compliance-Tools und statischen Regeln können sich Prüfwarteschlangen für die Überwachung schnell mit Inhalten mit geringem Risiko füllen. Dies können Boilerplate-Texte, Standard-Haftungsausschlüsse und automatisierte Benachrichtigungen sein – um nur einige Beispiele zu nennen. Die Prüfung solcher Inhalte geht mit einem hohen Zeit- und Ressourcenaufwand einher.

Da die Compliance-Teams ohnehin schon überlastet sind, bedeutet dies höhere Kosten und eine sich länger hinziehende Wertschöpfung.

Proofpoint Automate optimiert Ihre Prüfwarteschlangen, sortiert Inhalte mit geringem Risiko intelligent aus und vermeidet so False Positives bei künftigen Prüfungen. Bei anderen Compliance-Prüftools kann es Wochen oder sogar Monate dauern, bis neue Haftungsausschlüsse und Versender von Newslettern identifiziert werden. Proofpoint Automate verkürzt diesen Zyklus durch ML-Modelle, die bei der Überprüfung eine wesentlich schnellere Entscheidungsfindung ermöglichen.

Mit Proofpoint Automate lässt sich die Ablehnung oder Eskalation von Inhaltszweitprüfungen komplett automatisieren. Die Prüfer können sich also auf die wirklich geschäftskritischen Inhalte konzentrieren, ohne befürchten zu müssen, dass ihnen in Anbetracht der gesamten Datenmenge Richtlinien-verletzungen entgehen.

Eine technische Betrachtung: Modelle und Automatisierung der Überprüfung

Proofpoint Automate bewertet mithilfe von ML-Modellen Nachrichten, die von Proofpoint Supervision zur Überprüfung gekennzeichnet wurden (siehe Abb. 1). Dies können Nachrichten jeden Typs sein, der von Proofpoint Archive unterstützt wird, zum Beispiel:

- E-Mails
- Social-Media-Beiträge (z. B. X oder LinkedIn)
- Collaboration-Plattformen (z. B. Slack oder Microsoft Teams)
- Mobile Daten (z. B. WhatsApp- oder Sprachnachrichten)

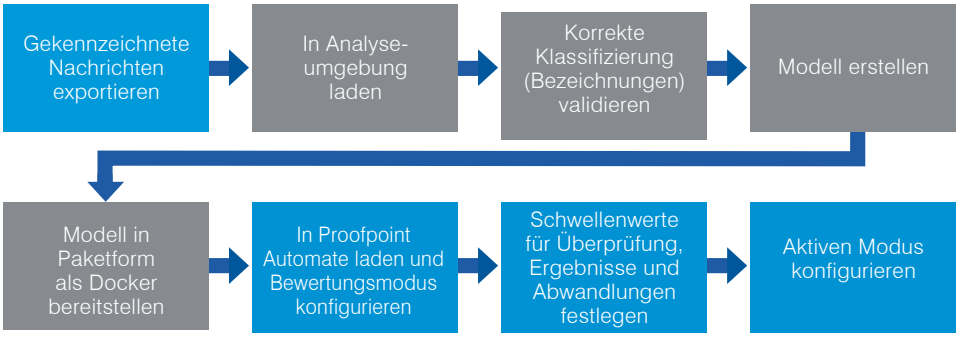


Abb. 2: Proofpoint Automate – Training und Bereitstellung von ML-Modellen.

Die Modelle werden für Elemente konfiguriert, die für eine oder mehrere Regeln gekennzeichnet wurden. Mit den einzelnen Modellen werden die relevanten Elemente bewertet. Anschließend wird ihnen ein spezifischer Wert, der Score, zugewiesen. Dieser Score wird dann in Proofpoint Supervision den Nachrichten hinzugefügt.

Im Bewertungsmodus können Prüfer die Nachrichten weiterhin überprüfen. Anhand der generierten Berichte lassen sich Vergleiche zwischen modellgestützten und menschlichen Prüfentscheidungen anstellen. Sobald Sie sich von der Zuverlässigkeit des Modells überzeugt haben, können Sie es aktivieren und damit dieselben Aktionen wie ein menschlicher Prüfer durchführen lassen. Auf diese Weise erhalten Sie eine automatisierte, autonome Überprüfung.

Für gekennzeichnete Nachrichten mit entsprechenden Proofpoint Automate-Modellen können in Proofpoint Supervision folgende Bereiche und Aktionen für Scores eingerichtet werden:

- **0,0 bis 0,15:** Hohe Zuverlässigkeit, dass das gekennzeichnete Element kein Problem darstellt. Proofpoint Automate löscht das Problem.
- **0,15 bis 0,8:** Niedrige Zuverlässigkeit bei der Nachrichten-bewertung. Proofpoint Automate belässt die Nachricht zur menschlichen Prüfung in der Warteschlange.
- **0,8 bis 1,0:** Hohe Zuverlässigkeit, dass das gekennzeichnete Element ein Problem darstellt. Proofpoint Automate eskaliert die Nachricht zur weiteren Untersuchung.

Wenn die Modelle aktiviert sind, werden sämtliche Bewertungen, Aktionen und zugehörigen Daten mit demselben Standard protokolliert, der zugrunde liegen würde, wenn ein menschlicher Prüfer die Entscheidung träfe.

Wichtige Attribute von Proofpoint Automate-Modellen

Wie die meisten ML-Modelle wurden auch die von Proofpoint Automate mithilfe von Daten entwickelt, mit denen ML-Algorithmen trainiert werden.[1] Bevor ein Modell erstellt wird, müssen zunächst die Daten vorbereitet werden. (Dieser Schritt wird manchmal auch als Daten-Wrangling oder Datenaufbereitung bezeichnet.) Die Daten werden erfasst, vorbereitet und in zwei Datensätze unterteilt: einen Trainingsdatensatz und einen Testdatensatz. In dieser Phase müssen die Daten klassifiziert und gekennzeichnet werden, damit sich die Bedeutung beschreiben lässt, die ein Mensch daraus ableiten würde.

Proofpoint Supervision stellt einen natürlichen Mechanismus zur Kennzeichnung von Daten bereit. Sie müssen also nur noch Ihre Mitarbeiter dazu schulen, wie sie Probleme bei der Prüfung korrekt kategorisieren. Die Nachrichtendaten (einschließlich Metadaten dazu, welche Kennzeichnungen übereinstimmten und warum) und Prüfentscheidungen lassen sich problemlos aus Proofpoint Supervision exportieren. (Das Format eignet sich gut zum Erstellen von Proofpoint Automate-Modellen.)

Wenn die Daten aufbereitet sind, haben Sie ein Basismodell. Sie können das Modell mit dem Testdatensatz testen, um seine Effektivität zu messen. Die Effektivität wird in der Regel anhand von zwei Werten gemessen: der Genauigkeit (Precision) und der Trefferquote (Recall).[2]

Einfach ausgedrückt, ist die Genauigkeit der Prozentsatz der Ergebnisse, die korrekt als relevant klassifiziert wurden. Bei der Trefferquote handelt es sich um die Anzahl der Nachrichten, die korrekt identifiziert (also nicht übersehen) wurden.

1 Javatpoint: „Machine learning life cycle“ (Lebenszyklus für Machine Learning), im Dezember 2024 abgerufen.
2 Wikipedia: „Precision and recall“ (Genauigkeit und Trefferquote), im Dezember 2024 aktualisiert.

Training und Bereitstellung von Modellen

Wenn das Basismodell fertiggestellt ist, können Sie neue Modelle trainieren und vergleichen, um festzustellen, welche Modelle bessere Werte für die Genauigkeit und die Trefferquote bieten. Manchmal stellen die beiden Werte möglicherweise einen Kompromiss dar. In einigen Situationen ist unter Umständen die Trefferquote wichtiger, in anderen die Genauigkeit.

Wenn ein Modell im Proofpoint Automate-Framework verwendet werden soll, wird es in Paketform als Webdienst zur Verfügung gestellt, der unsere REST-API-Spezifikation implementiert und in einem Docker-Container bereitgestellt wird.[3]

Das Modell kann dann eingerichtet und in der Produktionsumgebung in einem dieser Modi betrieben werden:

- **Bewertungsmodus:** In diesem Modus werden die einzelnen Nachrichten in einer bestimmten Klasse basierend auf dem Modell bewertet, aber keine Aktionen ausgeführt. Auf diese Weise wird das Modell in der Produktionsumgebung mit realen Daten getestet, ohne dass tatsächliche Prüfungen durchgeführt werden.
- **Aktivierter Modus:** In diesem Modus werden die Nachrichten in einer Klasse bewertet und entsprechend bearbeitet. Sie können auch eine Sampling-Rate angeben, um eine Auswahl von Nachrichten zu bewerten, aber keine Aktion für sie durchzuführen. Bei diesem Ansatz können Berichte zu Abweichungen erstellt werden, in denen die Leistung des Modells mit der Leistung menschlicher Prüfer verglichen wird.

Diese zwei Modi für neue und aktualisierte Modelle bieten zwei wesentliche Vorteile: Erstens können Sie sie effektiv bewerten. Zweitens erhalten Sie den Nachweis für erfolgreiche Tests, den Sie unter Umständen zur Erfüllung von Validierungsanforderungen benötigen. Sie können aktualisierte Modelle im Hinblick auf von menschlichen Prüfern und vom entsprechenden Modell getroffene Entscheidungen miteinander vergleichen.

Flexibles Ökosystem für die Modellausführung

Proofpoint Automate ist eine äußerst flexible Plattform. Sie ermöglicht die Ausführung von Modellen, die in einer beliebigen Sprache geschrieben wurden, und die Nutzung praktisch jedes Analyse-Frameworks, das zu Ihren Anforderungen passt.

Sie können die enthaltenen Standardmodelle direkt verwenden. Ihre Datenauswertungsteams können auch neue Modelle entwickeln, die innerhalb des Frameworks ausgeführt werden. Dank dieser Flexibilität können die Kenntnisse Ihres Teams über Ihr konkretes Unternehmen einfließen, ohne dass eine völlig neue skalierbare Plattform entwickelt und unterstützt werden muss. Falls Sie mehr Unterstützung benötigen, können Ihnen Proofpoint Professional Services auch bei der Erstellung benutzerdefinierter Proofpoint Automate-Modelle behilflich sein.

Fazit und nächste Schritte

Mit Proofpoint Automate wird das, was KI und ML versprechen, tatsächlich in großem Maßstab umgesetzt. Dank unseres einzigartigen Frameworks können Sie die Überwachung der digitalen Kommunikation so optimieren und verbessern, dass sie den behördlichen Bestimmungen und unternehmensspezifischen Anforderungen entspricht. Das Framework lässt sich schnell bereitstellen, vereinfacht das Training und Tests und bietet einen hervorragenden ROI. Mit Proofpoint Automate können Sie Ihre Überwachungsmethoden sicher modernisieren und so ein neues Maß von Effizienz und Effektivität erzielen.

3 Docker: „What is a Container?“ (Was ist ein Container?), im Dezember 2024 abgerufen.

Mehr unter Proofpoint.com/de