Veritas Alta Surveillance

Überblick

Die Vielzahl der heutigen Regularien stellt Unternehmen aller Größen vor neue Herausforderungen. Die Kommunikation ist zunehmend fragmentiert, und es reicht nicht mehr aus, nur E-Mails zu überwachen. Auch andere Quellen wie Chats unterliegen unter Umständen der Überwachungspflicht, um Vorschriften einzuhalten. Mit dem zunehmenden Umfang der regulierten Kommunikation wächst auch die Herausforderung, die Compliance-Anforderungen zu erfüllen.

Compliance bei der Überwachung

Veritas Alta™ Surveillance (vormals Veritas Advanced Supervision) ist eine leistungsstarke Compliance-Lösung, mit der Unternehmen eine optimierte Überwachung der Kommunikation zur Einhaltung von Richtlinien durchführen können. Die Integration von Veritas Merge1 oder Veritas Alta™ Capture bildet das Framework für die Auswahl und Stichprobenbildung aus über 120 Inhaltsquellen. Somit können Sie die Überprüfungen entsprechend verwalten und den Prozess für Audit-Zwecke aufzeichnen (siehe Abbildung 1).

Veritas Alta Surveillance hilft, die Kosten und den Aufwand für die Überprüfung der Einhaltung der Vorschriften durch gezielte Stichproben und die optionale Hinzufügung einer Klassifizierung zu senken und gleichzeitig den Compliance-Nachweis zu erbringen.

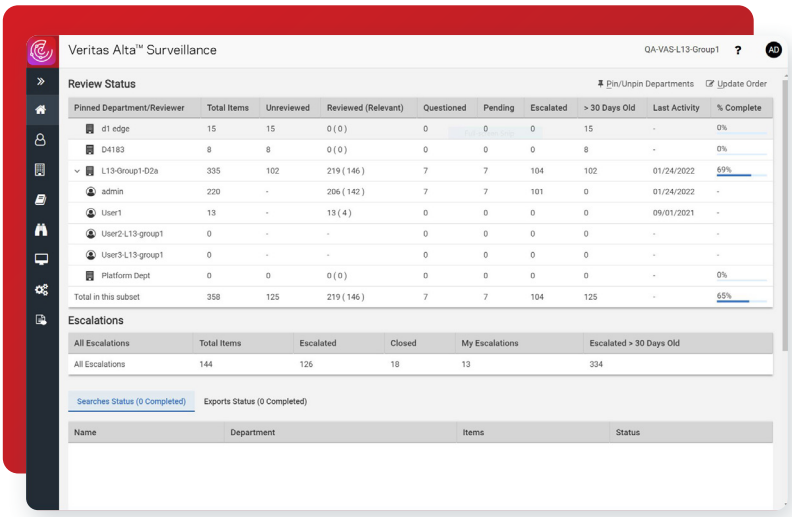

Abbildung 1. Dashboard von Veritas Alta Surveillance.

Vorteile

- Die neue intuitive Benutzeroberfläche bietet:
  - Workflow, der Überprüfer rasch zu den relevantesten Inhalten leitet
  - Details zum Prüfungsstatus
  - Feineinstellung von Überprüfungssätzen auf der Grundlage aller Metadaten, einschließlich Klassifizierungsrichtlinien, Hotwords und Hotword-Sätzen
- Ideal zur Anpassung an die zunehmenden Anforderungen für Langzeitspeicherung und Überwachung durch Vorschriften wie SEC, FINRA, MiFID II, Sarbanes- Oxley, IIROC, ESMA, ESA und SESC
- Optionale Verwendung von Veritas Alta™ Classification zum Herausfiltern von nicht zu prüfenden Nachrichten, sodass nur die relevantesten Inhalte in die Stichprobe aufgenommen werden
- Beaufsichtigung großer globaler Umgebungen und Überwachung ganzer Abteilungen und Unterabteilungen (siehe Abbildung 2)
- Möglichkeit der Zuweisung an Überprüfer-teams und deren Monitoring
- Überprüfung von Dateien und Tools für die Zusammenarbeit in einem facettenreichen, sortierbaren Dashboard
- Umfassende Klassifizierungsmöglichkeiten mit über 250 Richtlinien und mehr als 1.100 vordefinierten Mustern, die automatisch personenbezogene Daten, Gesundheitsdaten, Finanzdaten, Behördendaten und international regulierte Daten identifizieren (siehe Abbildung 3)
- Einsatz mehrerer Such- und Stichproben-mechanismen zur Inhaltserfassung anhand unterschiedlicher Variablen

Funktionsweise

Erstklassige Inhaltsarchivierung

Alle Inhalte werden indiziert und in einem unveränderbaren WORM-Speicher gespeichert, unabhängig davon, ob die Archivierung vor Ort oder in der Cloud erfolgt.

Bessere Überwachung, Stichprobennahme und Überprüfung

Mit Veritas Alta Surveillance können Sie strukturierte Überprüfungsprozesse einrichten, um alle relevanten Inhalte gemäß den Compliance-Richtlinien zu finden, zu prüfen und zu kontrollieren.

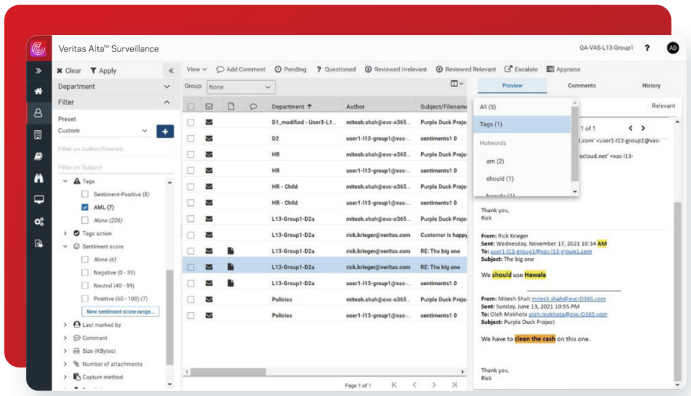

Abbildung 2. Hierarchische Darstellung der überwachten Abteilungen.

Schritt 1: Überprüfungsumfang festlegen

Definieren Sie in kurzer Zeit Ihre Kriterien:

- Wählen Sie die zu berücksichtigenden Inhaltsquellen
- Filtern Sie bereits überprüfte Elemente heraus (optional)
- Filtern Sie nach Datumsbereich und Zeit
- Legen Sie den Bereich der Absender/Empfänger fest
- Geben Sie bestimmte Textelemente an (Wörter oder Ausdrücke)
- Fügen Sie Hotwords/Hotword-Sätze hinzu
- Priorisieren Sie ein- oder auszuschließende Inhalte, die automatisch von Veritas klassifiziert wurden
- Schließen Sie bestimmte Textelemente (z. B. E-Mail-Haftungsausschlüsse) aus der Suche aus

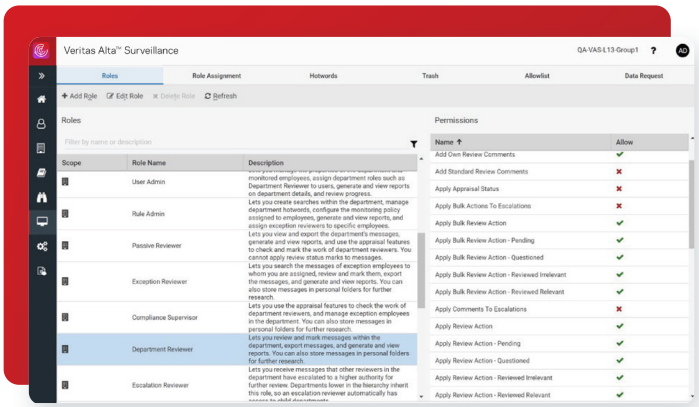

Abbildung 3. Überprüfungsfenster mit Highlight-Navigation durch Hotword- und Klassifizierungstreffer.

Schritt 2: Regeln für Stichproben und Suchen anwenden

Passen Sie die Regeln entsprechend der Anforderungen Ihrer Abteilung an:

- Nehmen Sie Stichproben für alle Inhalte oder pro Kanal für eine ganze Abteilung oder eine bestimmte Person
- Nehmen Sie Stichproben eines bestimmten Prozentsatzes
- Nutzen Sie garantierte oder statistische Stichproben

Schritt 3: Suchergebnisse überprüfen

Der zu überprüfende Inhalt wird auf einer benutzerfreundlichen Oberfläche dargestellt. Der Status jedes Elements wird festgehalten, und wenn weitere Maßnahmen erforderlich sind, wird dies in der ursprünglichen E-Mail markiert.

Folgende Überprüfungsfunktionen stehen zur Verfügung:

- Verwendung von Facetten zum Filtern der zu prüfenden Inhalte auf der Grundlage von Metadatenwerten
- Filterung nach gefundenen Hotwords und Hotword-Sätzen
- Filterung nach Inhaltsquelle und Klassifizierungstags
- Auswahl des Status „Ausstehend“ für zu überprüfende Elemente
- Anmerkungsfunktion für überprüfte Nachrichten
- Eskalierung von Nachrichten bei Bedarf an den vorgesetzten Compliance-Supervisor
- Schließung einer Stichprobe, wenn alle Überprüfungen und die nötigen Aufzeichnungen und Meldungen abgeschlossen sind

Schritt 4: Protokollieren

Führen Sie einen Audit-Pfad für den gesamten Prozess (siehe Abbildung 4). Sollte es zu Konfliktfällen kommen, lässt sich einfach untersuchen, was passiert ist, wenn der Administrator nachweisen kann, dass die Prüfung stattgefunden hat anhand:

- Systemkonfiguration
- Systembenutzer
- Gruppenkonfiguration
- Benutzeraktivität (Suchen, Prüfen)
- Audit-Pfad der Nachrichten im Überprüfungsprozess

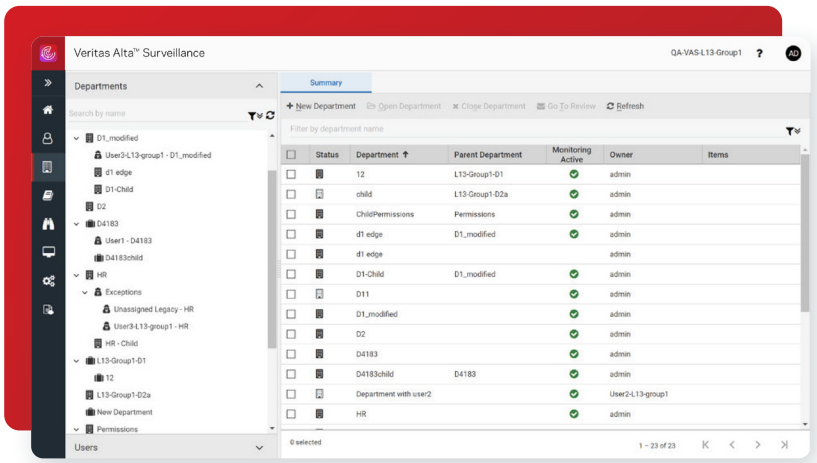

Abbildung 4. Verbesserte Suche nach Audit-Ereignissen

Produktfunktionen von Veritas Alta Surveillance

- **Vollständiges Management und Auditing**: Compliance-Überwachung und -Überprüfungsprozess
- **Mehrere Filteroptionen**: Stichprobenfilterung anhand von Klassifizierung, um irrelevante Inhalte zu blockieren und sicherzustellen, dass relevante Inhalte einbezogen werden (erfordert die Classification-Option)
- **Bedienfreundlich**: Benutzermodell besteht aus einer Reihe von geprüften Gruppen (z. B. Händlerschalter, Zweigstellen), denen jeweils ein Eigentümer/Prüfer zugeordnet ist, der regelmäßige Überprüfungen vornimmt
- **Effektive Stichprobennahme**: Selektive Suche und Stichprobennahme, um Elemente zur Überprüfung zu finden
- **Benutzerdefinierte Suche**: Manuelle oder automatische Suche/Stichprobennahme, mit der Möglichkeit, Textblöcke von den Suchergebnissen auszuschließen (zum Beispiel E-Mail-Haftungsausschlüsse)
- **Optionen „Intelligent Review“ und „Classification“**: Einsatz von maschinellem Lernen, um auf der Grundlage früherer Entscheidungen vorherzusagen, was Überprüfer als relevant oder irrelevant ansehen. Einbeziehung von KI zur Spracherkennung und Stimmungsanalyse
- **Tagging**: Element-Tagging während der Überprüfung für Relevanz und Nutzung integrierter Eskalations-Workflows als Reaktion auf dringende Warnungen
- **Rollenbasierter Zugriff** (siehe Abbildung 5): Erstellung und Modifizierung von rollenbasierten und granularen Funktionen auf Anwendungs- und Abteilungsebene
- **IR**: Automatische Klassifizierung von Elementen basierend auf früheren Aktionen von Überprüfern. Es handelt sich um eine vollständige, passive Lernmaschine, die immer aktiv ist und nicht manuell trainiert werden muss

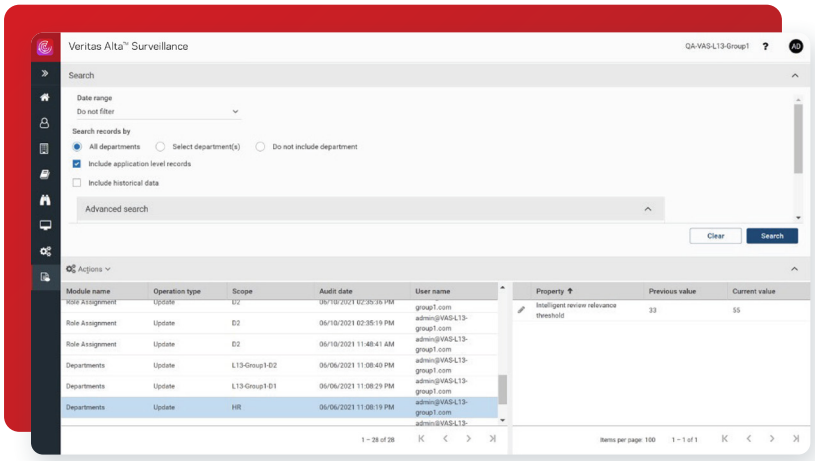

Abbildung 5. Granulare, rollenbasierte Zugriffskontrollen

Überprüfungspriorisierung nach Kategorie

Die Anwendung von Kontext auf archivierte Inhalte optimiert den Prozess der Compliance-Überprüfung. Analysieren Sie alle aufgenommenen Inhalte und bestimmen Sie anhand der optionalen Ergänzung Veritas Alta™ Classification, welche Inhalte in die Überprüfung aufgenommen werden. Verwenden Sie für einfachere und effektivere Überprüfungen Klassifizierungsrichtlinien, um Nachrichten nach Kategorie zu kennzeichnen. Dies stellt sicher, dass sich die Überprüfer Inhalte mit hoher Priorität anstatt irrelevante Nachrichten (z. B. Junk-Mails und abgelehnte Nachrichten) ansehen.

Intuitiver, ereignisgesteuerter Workflow

- Verwalten und schnelles Überprüfen von Suchergebnissen anhand von Beziehungen, Lexikontreffern, Metadaten und Übereinstimmungen mit Klassifizierungsrichtlinien, um den Überprüfungsprozess zu strukturieren
- Überprüfen und Markieren einzelner Elemente oder Ergebnissätze mit anpassbaren Kennzeichnungen
- Eskalieren einzelner Elemente oder Ergebnissätze zur weiteren Überprüfung durch festgelegte Supervisoren
- Exportieren von Falldetails und überprüfter Inhalte in Veritas™ eDiscovery Platform
- Massenüberprüfung – Zuweisen des Prüfstatus an mehrere Nachrichten gleichzeitig mit einer einzigen Aktion

Über Veritas

Veritas Technologies ist ein weltweit führender Anbieter im Bereich Multi-Cloud-Datenmanagement. Über 80.000 Kunden – darunter 95 Prozent der Fortune Global 500 – vertrauen darauf, mit den Lösungen von Veritas den Schutz, die Wiederherstellbarkeit und Compliance ihrer Daten zu gewährleisten. Wir stehen für skalierte, zuverlässige Produkte, welche die Widerstandsfähigkeit bieten, die unsere Kunden im Fall von Cyberangriffen wie Ransomware benötigen. Kein anderer Anbieter erreicht unsere Leistungsfähigkeit mit Unterstützung für mehr als 800 Datenquellen, über 100 Betriebssystemen, über 1.400 Speicherzielen und über 60 Clouds. Unterstützt von der Cloud Scale Technology setzt Veritas heute seine Strategie für ein autonomes Daten-Management um, die den operativen Overhead reduziert und gleichzeitig einen größeren Mehrwert bietet. Hier erfahren Sie mehr: www.veritas.com/de/de. Folgen Sie uns auf Twitter: @veritastechllc.

VERITAS

Veritas (Deutschland) GmbH
Theatinerstr. 11, 8. Etage
80333 München
Tel.: 0800-724 40 75
veritas.com/de/de

Die weltweiten Kontaktinformationen finden Sie hier:
veritas.com/de/de/company/contact

V0988 01/23