proofpoint.

DSPM: Schutz von geschützten Gesundheitsdaten, Forschungsdaten und geistigem Eigentum beginnt mit Transparenz

Gesundheits- und Life-Science-Unternehmen digitalisieren die Gesundheitsversorgung, die Bearbeitung von Abrechnungsdaten und die Arzneimittelentwicklung mit einem hohen Tempo und führen gleichzeitig KI-Agenten ein, um Abläufe und Forschung zu beschleunigen. Da vertrauliche Daten jedoch über Cloud-Plattformen, Partner-Ökosysteme und autonome KI-Systeme verteilt sind, sehen sich Sicherheitsteams mit zunehmenden Transparenzlücken und regulatorischem Druck konfrontiert.

„Gesundheits- und Life-Science-Unternehmen verzeichnen ein explosionsartiges Wachstum unstrukturierter Daten – von klinischen Unterlagen und Abrechnungsdaten bis hin zu Forschungsergebnissen und KI-Modellen. Ein Großteil dieser Daten ist äußerst vertraulich und wird innerhalb komplexer Ökosysteme oft zu freizügig weitergegeben."

– Derek Maki
Senior Vice President, Leiter des Bereichs Datensicherheitsprodukte, Proofpoint

Jahrelang setzten Gesundheitsanbieter, Versicherer und Life-Science-Unternehmen für den Schutz von Patienten- und Forschungsdaten auf Perimeter-Sicherheitsmaßnahmen, DLP-Tools (Datenverlustprävention) und SIEM-Plattformen (Sicherheitsinformations- und Ereignis-Management). Diese Tools wurden für eine Zeit entwickelt, in der Daten ausschließlich innerhalb von Krankenhausnetzwerken, Unternehmensrechenzentren und kontrollierten Forschungssystemen blieben.

Gesundheitsdaten sind heute jedoch überall.

Elektronische Patientenakten werden zwischen Leistungserbringern und Kostenträgern ausgetauscht. Abrechnungsdaten werden über Drittanbieter-Administratoren weitergeleitet. Die Daten aus klinischen Studien werden an Auftragsforschungsinstitute (CROs) und Forschungspartner weitergegeben. Geistiges Eigentum im Pharmabereich befindet sich in Multi-Cloud-Umgebungen. KI-Modelle werden anhand riesiger Mengen strukturierter und unstrukturierter Daten trainiert.

Durch diese digitale Beschleunigung ist eine kritische Transparenzlücke entstanden.

„Gesundheits- und Life-Science-Unternehmen verzeichnen ein explosionsartiges Wachstum unstrukturierter Daten – von klinischen Unterlagen und Abrechnungsdaten bis hin zu Forschungsergebnissen und KI-Modellen", sagt Derek Maki, Senior Vice President und Leiter des Bereichs Datensicherheitsprodukte bei Proofpoint. „Ein Großteil dieser Daten ist äußerst vertraulich und wird innerhalb komplexer Ökosysteme oft zu freizügig weitergegeben."

Vertrauliche Daten (darunter geschützte Gesundheitsdaten, personenbezogene Daten, Genomdaten, Zahlungsdaten und proprietäre Forschungsergebnisse) werden häufig in SaaS-Anwendungen, Cloud-Speichern, Collaboration-Plattformen und hybriden Umgebungen gespeichert. Dateien können falsch konfiguriert oder allgemein zugänglich sein und es kann vorkommen, dass sie an externe Parteien weitergegeben werden, ohne dass man sich dessen voll bewusst ist.

Im Kern geht es um eine einfache Tatsache: Sie können das Vertrauen der Patienten, bahnbrechende Forschungsergebnisse und die Einnahmen nicht schützen, wenn Sie nicht wissen, wo sich Ihre vertraulichen Daten befinden.

Datentransparenz in Healthcare-Ökosystemen – von der Diagnose bis zur Behandlung

Um wieder die Kontrolle zu erlangen, setzen Gesundheitsunternehmen auf Data Security Posture Management (DSPM) – ein modernes Framework, das kontinuierlich vertrauliche Daten identifiziert, Zugriffsrisiken analysiert und Behebungsmaßnahmen priorisiert.

„Angesichts der Datenmengen, die bei Anbietern, Krankenkassen und Life-Science-Unternehmen anfallen, ist es unglaublich schwierig zu wissen, wo sich die sensibelsten Daten befinden", erklärt Maki. „Mit DSPM können Unternehmen Datenspeicher mit hohem Risiko identifizieren, feststellen, wer Zugriff darauf hat, und sich auf die wichtigsten Risiken konzentrieren."

DSPM scannt kontinuierlich die Umgebung, um Folgendes zu erkennen:

- Patientenakten mit zu freizügigen Freigabeeinstellungen
- Falsch konfigurierte Cloud-Speicher, die geschützte Gesundheitsdaten enthalten
- Übermäßige Zugriffe auf Abrechnungs- und Finanzsysteme
- Ungeschützte klinische Forschungsdaten
- Offen gelegtes geistiges Eigentum und vertrauliche Datensätze, einschließlich solcher, die für das Training von KI verwendet werden

Anstatt Teams mit Warnmeldungen zu überhäufen, liefert DSPM Kontext und kombiniert die Vertraulichkeit der Daten, das Zugriffsrisiko und die Bedrohungswege, um echte Risiken zu priorisieren.

Für Sicherheitsteams, die Compliance-Anforderungen wie HIPAA, HITRUST, PCI DSS, FDA-Vorgaben und globale Datenschutzbestimmungen einhalten müssen, ist diese Transparenz von entscheidender Bedeutung.

„Anbieter, Kostenträger und Pharmaunternehmen stehen alle vor derselben Herausforderung: einer massiven Datenflut und begrenzten Sicherheitsressourcen", sagt Maki. „Um Patientendaten, Forschungsergebnisse und Einnahmen schützen zu können, benötigen Sie eine Priorisierung der Risiken."

„Anbieter, Kostenträger und Pharmaunternehmen stehen alle vor derselben Herausforderung: einer massiven Datenflut und begrenzten Sicherheitsressourcen. Um Patientendaten, Forschungsergebnisse und Einnahmen schützen zu können, benötigen Sie eine Priorisierung der Risiken."

– Derek Maki
Senior Vice President, Leiter des Bereichs Datensicherheitsprodukte, Proofpoint

Absicherung der wachsenden Anzahl von KI-Agenten bei Gesundheits- und Life-Science-Unternehmen

Überall im Gesundheitswesen werden KI-Agenten in klinische Arbeitsabläufe, die Bearbeitung von Abrechnungsdaten, die Arzneimittelforschung und Plattformen für Patienteninteraktionen integriert. Diese Agenten greifen auf riesige Mengen an geschützten Gesundheitsdaten, Forschungsdaten, Finanzunterlagen und geistigem Eigentum zu – oft über mehrere Cloud-Umgebungen hinweg. Im Gegensatz zu herkömmlichen Anwendern sind für KI-Agenten folgende Aktivitäten typisch:

- Selbstständiges Arbeiten
- Dynamischer Abruf von Daten
- Parallele Interaktionen mit mehreren Systemen
- Erstellen neuer, komplexer Datenflüsse
- Hinzufügen nicht-menschlicher Identitäten zu Zugriffsmodellen

Dadurch entsteht eine neue Risikoebene, deren Überwachung vielen Einrichtungen im Gesundheitswesen Schwierigkeiten bereitet.

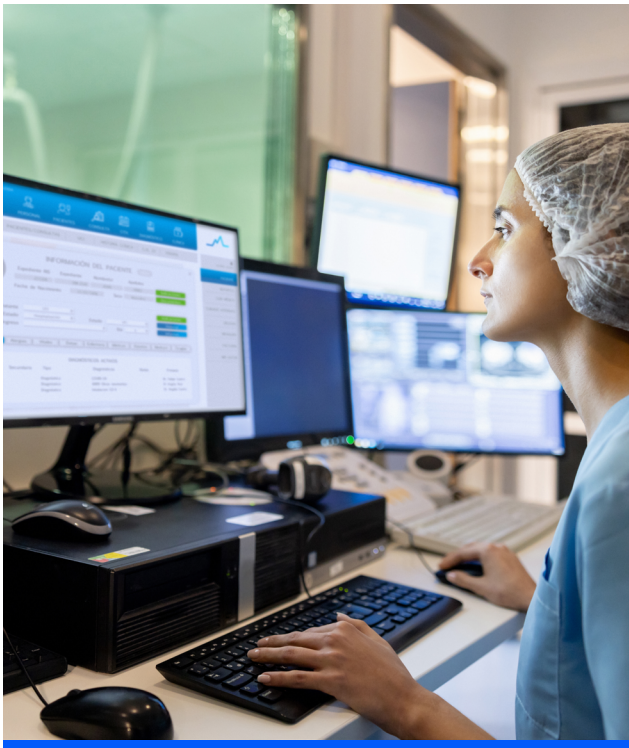
„Einrichtungen im Gesundheitswesen setzen zunehmend KI-Agenten ein, um Effizienz und Innovation voranzutreiben“, erklärt Maki. „Doch diese Agenten benötigen umfassenden Zugriff auf vertrauliche Daten. Ohne einen klaren Überblick darüber, auf welche Daten sie zugreifen, wohin diese Daten übertragen werden und wie sich die Zugriffsrechte entwickeln, setzen sich Unternehmen erheblichen und oft nicht erkennbaren Risiken aus.“

KI-Modelle, die auf Patientenakten, Abrechnungsdaten oder genomischen Forschungsdaten trainiert wurden, können unbeabsichtigt regulierte Informationen offenlegen. KI-Service-Konten mit zu weitreichenden Berechtigungen können indirekte Angriffswege zu Patientendaten oder proprietären Arzneimittelforschungsdaten eröffnen.

Durch die Erfassung von Identitäten (einschließlich nicht-menschlicher Identitäten und Service-Konten) sowie der Vertraulichkeit der Daten und der Zugriffsrisiken unterstützt Proofpoint DSPM Unternehmen im Gesundheitswesen bei folgenden Aufgaben:

- Feststellen, wo KI-Agenten übermäßige Berechtigungen haben
- Verstehen, welche vertraulichen Datensätze zum Trainieren oder Betreiben von KI verwendet werden
- Erkennen übermäßiger Datenfreigaben und falsch konfigurierter KI-Konten
- Visualisieren der durch Automatisierung entstandenen indirekten Zugriffspfade
- Reduzieren des Risikos von Datenkompromittierungen durch KI

„Im Zeitalter der KI-gestützten Gesundheitsversorgung ist die Transparenz hinsichtlich des Zugriffs durch nicht-menschliche Akteure genauso wichtig wie die Transparenz hinsichtlich des Zugriffs durch Menschen“, fügt Maki hinzu. „DSPM bietet Unternehmen die nötigen Kontextdaten, damit sie sicher Innovationen einführen und gleichzeitig das Vertrauen der Patienten sowie geistiges Eigentum schützen können.“



„Im Zeitalter der KI-gestützten Gesundheitsversorgung ist die Transparenz hinsichtlich des Zugriffs durch nicht-menschliche Akteure genauso wichtig wie die Transparenz hinsichtlich des Zugriffs durch Menschen. DSPM bietet Unternehmen die nötigen Kontextdaten, damit sie sicher Innovationen einführen und gleichzeitig das Vertrauen der Patienten sowie geistiges Eigentum schützen können.“

– Derek Maki
Senior Vice President,
Leiter des Bereichs
Datensicherheitsprodukte,
Proofpoint

Vorteile von Proofpoint DSPM: Intelligenter Schutz für das Gesundheits- und Life-Science-Unternehmen

Proofpoint DSPM wurde speziell für stark regulierte Branchen mit komplexen Ökosystemen wie dem Gesundheitswesen entwickelt. Anstatt den operativen Aufwand zu erhöhen, bietet die Lösung schnelle Transparenz und ermöglicht eine messbare Reduzierung des Risikos.

- **Schnelle, agentenlose Bereitstellung**
  Proofpoint lässt sich über eine API mit Microsoft 365, Google Workspace, AWS und anderen Cloud-Plattformen verbinden – ganz ohne Agenten und mit minimalen Betriebsunterbrechungen. Einrichtungen im Gesundheitswesen können damit beginnen, vertrauliche Daten in klinischen, unternehmensinternen und Forschungsumgebungen schnell zu identifizieren und zu klassifizieren.

- **Umfassende, skalierbare Erkennung**
  Der Proofpoint One-Pass Scanner identifiziert und klassifiziert geschützte Gesundheitsdaten, personenbezogene Daten, Zahlungsdaten, proprietäre Forschungsergebnisse, Daten aus klinischen Studien und andere vertrauliche Informationen in SaaS-, PaaS-, IaaS-, lokalen und hybriden Umgebungen – unter Einhaltung der Vorgaben zum Datenspeicherort.

- **Transparenz zu KI-Agenten und nicht-menschlichen Identitäten**
  Proofpoint erfasst und analysiert nicht-menschliche Identitäten (darunter KI-Agenten, Service-Konten und Automatisierungs-Workflows), um übermäßige Berechtigungen, Kompromittierungen vertraulicher Daten und indirekte Zugriffspfade zu identifizieren, die durch maschinengesteuerte Prozesse entstehen.

- **Visualisierung von Angriffspfaden und Zugriffsrisiken**
  Durch die Darstellung von Zugriffs- und Angriffspfaden wird deutlich, wie Identitäten, Berechtigungen und Datenspeicher miteinander verknüpft sind. Außerdem werden indirekte Zugriffspfade zu Patientenakten, Abrechnungssystemen und Forschungsdatenbanken sichtbar.

- **Automatisierte Behebung und Durchsetzung**
  Proofpoint ermöglicht die Erstellung von DLP-Richtlinien mit einem Klick, sodass Sie über Proofpoint DLP übermäßige Berechtigungen widerrufen können. Außerdem integriert sich die Lösung mit Tools wie ServiceNow, Jira und Slack, um geführte Behebungs-Workflows zu ermöglichen.

Ein intelligenterer Ansatz zum Schutz von Patientendaten, Forschung und Innovation

Gesundheits- und Life-Science-Unternehmen müssen ein Gleichgewicht zwischen Innovation, strikter Einhaltung gesetzlicher Vorschriften und dem Vertrauen der Patienten finden.

„Ohne eine genaue Datenklassifizierung ist es nicht möglich, die von HIPAA vorgeschriebenen Sicherheitsvorkehrungen durchzusetzen, klinische Forschung zu schützen oder geschützte Daten zur Arzneimittelentwicklung abzusichern“, sagt Maki. „Proofpoint automatisiert die Klassifizierung, sodass Einrichtungen im Gesundheitswesen die richtigen Kontrollmaßnahmen implementieren können, ohne die Innovation auszubremsen.“

In einer Branche, in der schon eine einzige Datenschutzverletzung die Gesundheitsversorgung beeinträchtigen, die Forschung verzögern oder das Vertrauen der Patienten untergraben kann, sind Klarheit und Kontrolle nicht mehr nur wünschenswert, sondern unverzichtbar.

Proofpoint DSPM bietet die Transparenz, Priorisierung und Automatisierung, die Einrichtungen im Gesundheitswesen benötigen, um die wichtigsten Ressourcen zu schützen.

Proofpoint DSPM unterstützt Unternehmen bei folgenden Aufgaben:

- Erfassung und Schutz von geschützten Gesundheitsdaten in verteilten Systemen
- Schutz der proprietären Arzneimittelforschung und klinischer Daten
- Governance der KI-Agenten-Zugriffe auf vertrauliche Datensätze und Reduzierung der Risiken durch nicht-menschliche Identitäten
- Reduzierung der Wahrscheinlichkeit von Datenschutzverletzungen und finanziellen Risiken
- Einhaltung der HIPAA-, HITRUST- und weltweiten Compliance-Anforderungen
- Quantifizierung der Risiken basierend auf der Vertraulichkeit der Daten und Erkenntnissen zur Wahrscheinlichkeit von Datenschutzverletzungen

„Ohne eine genaue Datenklassifizierung ist es nicht möglich, die von HIPAA vorgeschriebenen Sicherheitsvorkehrungen durchzusetzen, klinische Forschung zu schützen oder geschützte Daten zur Arzneimittelentwicklung abzusichern. Proofpoint automatisiert die Klassifizierung, sodass Einrichtungen im Gesundheitswesen die richtigen Kontrollmaßnahmen implementieren können, ohne die Innovation auszubremsen.“

– Derek Maki
Senior Vice President, Leiter des Bereichs Datensicherheitsprodukte, Proofpoint

Weitere Informationen

Erfahren Sie, wie Gesundheits- und Life-Science-Unternehmen mit Proofpoint vertrauliche Daten im großen Maßstab erkennen, klassifizieren und kontrollieren können.