proofpoint.

KURZVORSTELLUNG

Absicherung medizinischer Informationen mit Proofpoint

So schützen Sie Patientendaten vor Insider-Bedrohungen, Datenverlust und Cloud-Risiken

Wichtige Vorteile

- Identifizierung und Minimierung von Risiken, die durch fahrlässige, kompromittierte Anwender oder böswillige Insider entstehen
- Skalierbarer Schutz für alle Elemente der Angriffsfläche, um den wachsenden digitalen Fußabdruck abzusichern
- Verhinderung von Datenverlust durch E-Mails, die Cloud und Endpunkte

10 %

aller Ransomware-Angriffe in den letzten beiden Jahren zielten auf die Gesundheitsbranche ab.

Quelle: SC Media

Gesundheitsdienstleister sind schon seit Langem beliebte Ziele von Cyberkriminellen. Da diese Unternehmen viele verschiedene Arten von Daten wie geistiges Eigentum, Daten zu klinischen Tests, geschützte Gesundheitsdaten und private Finanzdaten verarbeiten, bieten Attacken zahlreiche Möglichkeiten zur Erpressung. Auch die zunehmende Nutzung von Cloud, Remote-Arbeitsplätzen und Telemedizin vergrößert die Angriffsfläche von medizinischen Einrichtungen. Zudem führt der wachsende Arbeitsdruck in der Branche dazu, dass das Risiko durch böswillige ebenso wie durch wohlgesonnene Insider steigt.

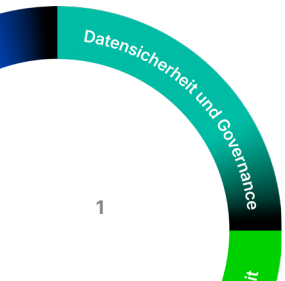
Proofpoint bietet einen personenzentrierten Ansatz, um vertrauliche Daten in verteilten Netzwerken des Gesundheitswesens zu schützen. Unsere Datensicherheitslösungen ermöglichen einzigartige Transparenz und Kontrolle über vertrauliche Daten. Wir unterstützen Sie dabei, Ihre Mitarbeiter und deren vertrauliche Daten vor versehentlicher Offenlegung, Angriffen und Insider-Risiken zu schützen. Unser Schutzschild erstreckt sich auf Cloud-Dienste, E-Mails, Endpunkte und lokale Dateifreigaben, damit Ihr Unternehmen datenbezogene Risiken besser verwalten und gleichzeitig Zeit sowie Betriebskosten einsparen kann.

Eine wachsende Bedrohung

Wie viele Unternehmen speichern auch Gesundheitseinrichtungen Kreditkarten- und andere Finanzdaten. Zusätzlich verarbeiten sie enorme Mengen an personenbezogenen Gesundheitsdaten sowie Daten zu klinischer Forschung und bewahren sogar Daten zu staatlichen Stipendienprogrammen auf. All diese Daten machen sie zu einem lukrativen Ziel für Cyberkriminelle.

Hinzu kommt, dass Gesundheitseinrichtungen inzwischen einen komplexeren digitalen Fußabdruck haben. Immer mehr Gesundheitsdienstleistungen werden in der Cloud gehostet und die wachsende Zahl medizinischer IoT-Geräte (Internet of Things) vergrößert die Angriffsfläche zusätzlich. Gleichzeitig werden durch die modernen Telemedizin-Optionen vertrauliche Daten auch außerhalb des Netzwerkperimeters verwendet, während Mitarbeiter dank hybrider Arbeitsregeln inzwischen oft per Fernzugriff arbeiten können.

Leider folgen Angreifer stets ihren Zielen, sodass in den letzten beiden Jahren 10 % aller Ransomware-Angriffe auf die Gesundheitsbranche abzielten und Cyberangriffe auf den Medizinbereich um 32 % zunahmen.[1] Damit sind diese Zahlen wesentlich höher als für andere Sektoren und Branchen. Zudem sind Datenkompromittierungen im Gesundheitsbereich sehr viel teurer als in anderen Branchen.



1. Shaun Nichols (*SC Media*): *Cyberattacks targeting medial organizations up 32% in 2024* (Cyberangriffe auf medizinische Einrichtungen 2024 um 32 % gestiegen), Februar 2025.

32 %

Cyberangriffe auf den Medizinbereich nahmen in den letzten beiden Jahren um 32 % zu.

Quelle: SC Media

9,77 Mio. $

2024 lagen die durchschnittlichen Kosten einer Kompromittierung von Gesundheitsdaten bei 9,77 Millionen US-Dollar.

Quelle: Ponemon Institute und IBM

2024 lagen die durchschnittlichen Kosten einer Kompromittierung von Gesundheitsdaten bei 9,77 Millionen US-Dollar.[2] Die Kosten können zum Beispiel Lösegeldzahlungen, Maßnahmen zur Systemwiederherstellung, Geldbußen für Compliance-Verstöße sowie Mittel für Rechtsstreitigkeiten und für die Wiederherstellung eines beschädigten Markenrufs umfassen. Darüber hinaus können Systemausfallzeiten oder eine kompromittierte Integrität der Daten negative gesundheitliche Folgen haben und sogar Leben kosten.

Datensicherheitsprobleme

Datensicherheit sollte für Krankenhäuser, Kliniken, Krankenversicherungen und Biotech-Firmen höchste Priorität haben. Schließlich müssen diese Einrichtungen nicht nur ihre eigenen Forschungsdaten und ihr geistiges Eigentum, sondern auch die personenbezogenen Informationen und Gesundheitsdaten sowie Zahlungskartendaten der Patienten schützen. Dabei stehen sie vor zahlreichen Herausforderungen, von denen einige in diesem Abschnitt beschrieben werden.

Ausspionieren elektronischer Gesundheitsdaten und andere Bedrohungen durch Insider verhindern

Gesundheitseinrichtungen gehören zu den stressigsten Arbeitsumgebungen, wodurch auch das Risiko von Bedrohungen durch Insider steigt.

Ein neugieriger Mitarbeiter kann in einer Pause schon mal einen Blick in die Patientenakte eines berühmten Patienten werfen. Dieses Schnüffeln in elektronischen Patientenakten birgt ernsthafte Risiken für die Einrichtung, wenn die Informationen eines zahlungskräftigen Patienten den Weg in die Öffentlichkeit finden. Wohlgesonnene, aber überarbeitete Mitarbeiter könnten unbedacht eine Phishing-E-Mail öffnen oder versehentlich E-Mails mit vertraulichen Daten an die falschen Empfänger senden. Und emotionaler Stress kann sogar zu Insider-Bedrohungen gegen einen Arbeitgeber führen. Wenn das Konto eines vertrauenswürdigen Anwenders durch Anmeldedaten-Diebstahl kompromittiert wird, kann das gravierende Folgen haben, noch bevor der Diebstahl überhaupt bemerkt wird. Deshalb benötigen Sie einen proaktiven Ansatz, der alle diese Bedrohungen verhindert.

Sicherheitsrisiken generativer KI reduzieren

Dienstleister im Gesundheitsbereich setzen zunehmend auf generative KI (GenAI), z. B. um die Produktivität der Klinikmitarbeiter zu steigern, die Einbindung von Patienten und Mitgliedern zu verbessern sowie administrative Prozesse effizienter zu gestalten. Sie nutzen generative KI auch, um die Qualität der Pflege und Patientenversorgung zu optimieren, oder setzen sie außerhalb von klinischen Anwendungen ein, um allgemeine Interaktionen bei der Patientenversorgung zu verbessern. Doch der Einsatz von KI birgt auch neue Risiken. Abgesehen von nicht korrekten oder nicht neutralen Datenausgaben müssen Gesundheitsdienstleister sicherstellen, dass KI-Modelle nicht versehentlich personenbezogene Gesundheitsdaten offenlegen oder missbräuchlich verwenden. Das kann zum Beispiel vorkommen, wenn KI unstrukturierte Daten wie Kliniknotizen verarbeitet. Zudem müssen bei der Integration von GenAI in den Klinikalltag oft komplexe Regulierungshürden überwunden werden.

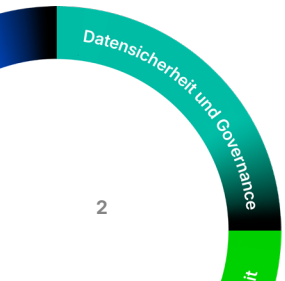
Wachsende Angriffsfläche durch Wechsel in die Cloud schützen

Viele Gesundheitseinrichtungen gingen den Wechsel in die Cloud nur zögerlich an. Inzwischen bieten jedoch fast alle Einrichtungen verschiedene Dienste in Public, Private und Hybrid Clouds an. Durch den Echtzeitzugriff auf Informationen hat sich die Patientenversorgung verbessert und Einrichtungen konnten ihre Abläufe vereinfachen sowie die Anschaffungskosten für IT-Infrastruktur reduzieren. Andererseits hat sich dadurch die Angriffsfläche vergrößert.

Selbst bei lokal gespeicherten elektronischen Patientenakten werden einzelne Informationen daraus immer wieder an anderen Orten aufgerufen, freigegeben und gespeichert. Denken Sie zum Beispiel an mobile Geräte, Endpunkte im Homeoffice, medizinische IoT-Geräte und Cloud-basierte E-Mail-Systeme. Da Gesundheitsdaten nicht mehr ortsgebunden sind, wird der Schutz dieser Daten immer schwieriger.

Mit dem Wachstum der Cloud-Umgebungen steigt auch das Risiko von Anmeldedaten-Diebstahl. Büro-Software und Collaboration-Funktionen werden immer öfter über Cloud-Dienste wie Microsoft 365 und Google Workspace bereitgestellt, was dazu führt, dass Cyberkriminelle diese Services immer häufiger ausnutzen.

2. Ponemon Institute und IBM: *Cost of a Data Breach Report 2024* (Kosten von Datenkompromittierungen 2024).



Produkte

- Proofpoint Adaptive Email DLP
- Proofpoint Enterprise DLP
- Proofpoint Email DLP
- Proofpoint Email Encryption
- Proofpoint Insider Threat Management
- Proofpoint Data Security Posture Management
- Proofpoint Applied Services for Data Security

Datensicherheit in allen Kanälen und Plattformen vereinheitlichen

Gesundheitseinrichtungen nutzen heute zahlreiche Mittel für die Kommunikation und Datenübertragung, darunter Systeme für elektronische Gesundheitsakten wie Epic, Cloud-basierte und lokale E-Mail-Systeme, andere Messaging-Systeme sowie File-Sharing-Dienste. Außerdem verfügen sie über eine Vielzahl an Endpunkten, wie PCs am Ort der Patientenversorgung, hunderte Arten von medizinischen Geräten, Desktop-Computer, Laptops und Mobilgeräte. Viele Mitarbeiter nutzen im Laufe eines Tages mehrere Geräte. Ihre vertraulichen Daten werden auf Servern im Rechenzentrum und in der Cloud gespeichert und regelmäßig zwischen diesen beiden Speicherorten übertragen.

Eine erweiterte Angriffsfläche und zunehmend komplexe Infrastruktur machen integrierte Sicherheitsmaßnahmen noch wichtiger. Für die Datensicherheit bedeutet dies, dass Sie integrierte DLP-Tools (Datenverlustprävention) für E-Mail, Cloud sowie Endpunkte benötigen.

Ein personenzentrierter Ansatz

Ältere Datenschutzansätze konzentrieren sich nur auf die Daten. Informationen gehen jedoch nicht einfach so verloren. Hinter Datenverlusten stehen immer Personen, die einen Fehler machen oder böswillig handeln. Gleichzeitig kommt es bei Cybersicherheit auf Transparenz an. Deshalb müssen Sie die Personengruppen kennen, die für Risiken besonders anfällig sind. Ein personenzentrierter Ansatz analysiert die Dynamik der Individuen, die mit Ihren Daten interagieren.

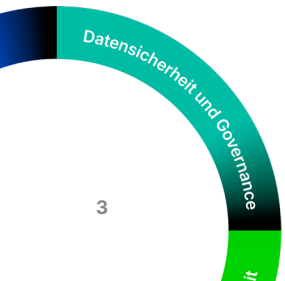
Wie Proofpoint helfen kann

Die einheitliche personenzentrierte Datensicherheitslösung von Proofpoint bietet einzigartige Transparenz. Bei einer Cloud-nativen Plattform können Sie Ihre vertraulichen Daten schützen und sich auf die Personen konzentrieren, die mit ihnen interagieren. Unsere Lösungen berücksichtigen Inhalte, Verhaltensweisen und Bedrohungen und verbinden lokale Datenschutzmaßnahmen mit Cloud-Sicherheitsfunktionen. Dadurch sind Ihre klinischen und nicht-klinischen Mitarbeiter sowie Patienten geschützt – unabhängig davon, wohin ihre Daten übertragen werden.

Das sind die Kernkomponenten unserer einheitlichen Datensicherheitslösung:

Proofpoint Adaptive Email DLP

Proofpoint Adaptive Email DLP kann mithilfe von verhaltensbasierter KI versehentlichen und vorsätzlichen Datenverlust über E-Mails verhindern. Die Lösung analysiert E-Mail-Daten der letzten 12 Monate und lernt auf diese Weise das normale E-Mail-Sendeverhalten Ihrer Mitarbeiter, ihre vertrauenswürdigen Beziehungen und ihren Umgang mit vertraulichen Daten. Dank dieser Analyse kann Proofpoint Adaptive Email DLP ungewöhnliches E-Mail-Verhalten sofort identifizieren. Falls es zu einer fehlgeleiteten E-Mail, einer falsch angehängten Datei oder einer Datenexfiltration kommt, wird den Anwendern eine kontextbezogene Warnmeldung angezeigt, damit sie das Datenverlustereignis umgehend stoppen und verhindern können. Das Eingreifen eines Administrators ist dabei nicht erforderlich.



Proofpoint Enterprise DLP

Die marktführenden DLP-Lösungen von Proofpoint verfolgen einen adaptiven, personenzentrierten Ansatz zur Verhinderung von Datenverlust, der einen umfassenden Überblick über Anwenderverhalten und Inhalte bietet. Dies ermöglicht eine effektive Erkennung und Prävention ernsthafter Datenverlustrisiken. Durch die Integration von Schutzfunktionen, die E-Mail, Cloud und verwaltete sowie nicht verwaltete Endpunkte abdecken, schafft Proofpoint eine Grundlage für moderne DLP-Strategien. Unsere DLP-Lösungen basieren auf einer Cloud-nativen Architektur mit modernen Datenschutzkontrollen und einem äußerst stabilen Agenten. Sie werden automatisch skaliert und lassen sich einfach bereitstellen und warten.

Über eine einheitliche Konsole lassen sich Warnmeldungen zentral verwalten und Zwischenfälle in sämtlichen Kanälen untersuchen. Leistungsstarke Analysefunktionen ermöglichen die schnelle und zuverlässige Bewertung von Datenrisiken, sodass Sie gezielte Maßnahmen ergreifen können.

Proofpoint Email DLP

Proofpoint Email DLP reduziert das Risiko, dass vertrauliche Daten per E-Mail exfiltriert werden, und gewährleistet die Compliance mithilfe richtlinienbasierter Prävention und Verschlüsselung. Die Lösung lässt sich einfach als Add-on zu einer bestehenden E-Mail-Sicherheitslösung oder als Teil eines unternehmensweiten DLP-Ansatzes bereitstellen. Proofpoint Email DLP automatisiert Vorschriften-Compliance mit vorkonfigurierten Detektoren (für Zahlungskartendaten, geschützte Gesundheitsdaten, DSGVO, SOX, HIPAA u. a.). Unternehmenseigene Daten können zudem mithilfe benutzerdefinierter Wörterbücher und KI-gestützter Klassifizierung identifiziert und geschützt werden.

Proofpoint Email Encryption

Proofpoint Email Encryption verschlüsselt E-Mails und Anhänge automatisch und bietet dabei vollständige Transparenz. Im Gegensatz zu herkömmlichen E-Mail-Verschlüsselungsdiensten, müssen Ihre Mitarbeiter ihre E-Mails nicht manuell verschlüsseln – die Verschlüsselung erfolgt automatisch im Hintergrund. Mit Proofpoint Email Encryption sind Ihre vertraulichen E-Mails geschützt. Gleichzeitig können Ihre verbundenen Unternehmen, Geschäftspartner und Anwender problemlos auf abgesicherte Nachrichten auf Computern sowie Mobilgeräten zugreifen.

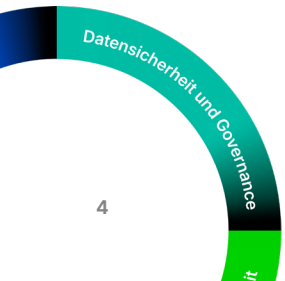
Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) korreliert Anwenderaktivitäten und Datenbewegungen, damit Sicherheitsteams potenzielle Insider-Bedrohungen mit personenzentrierten Verhaltensanalysen erkennen, untersuchen und abwehren können. Dazu bietet die Lösung Funktionen zur Echtzeiterkennung von Datenexfiltrationen, Missbrauch von Berechtigungen und Anwendungen, unbefugten Zugriffen, riskanten versehentlichen Aktionen sowie ungewöhnlichen Verhaltensweisen – einschließlich Optionen zur schnellen Reaktion. Auf diese Weise können Sie Bedrohungen wie das Ausspionieren von elektronischen Patientenakten in zeitleistenbasierten Visualisierungen und Analysen erkennen, verhindern und abwehren.

Sobald eine Insider-Bedrohung erkannt wurde, stellt Proofpoint ITM Workflows und unwiderlegbare Beweise für Fehlverhalten bereit, um die Reaktion auf den Zwischenfall zu beschleunigen. Die Informationen werden durch ressourcenschonende Endpunktsensoren zusammengetragen und anschließend in einer modernen Architektur analysiert, die Skalierbarkeit, Sicherheit und Datenschutz gewährleistet. Proofpoint ITM kann als lokale Lösung oder per SaaS bereitgestellt werden.

Proofpoint Data Security Posture Management

Proofpoint Data Security Posture Management (DSPM) beseitigt die Hauptursache vieler Datenkompromittierungen – blinde Flecken in Datenumgebungen – und priorisiert dabei die Reduzierung des personenbezogenen Risikos für die Datensicherheit. Indem Proofpoint DSPM identifiziert, wo vertrauliche und wertvolle Daten gespeichert sind, wer darauf zugreift und von welchen Risiken die größte Gefahr ausgeht, können Gesundheitsdienstleister Sicherheitslücken schließen, die Angriffsfläche verkleinern und die Compliance automatisieren. Proofpoint DSPM gewährleistet zudem die sichere Nutzung von KI-Tools, indem die Lösung vertrauliche Daten identifiziert, Datenschutzrichtlinien durchsetzt und in Echtzeit Vertraulichkeitsanalysen für KI-Workflows durchführt.



Proofpoint Applied Services for Data Security

Die Gesundheitsbranche kämpft schon seit Jahren mit Personalmangel, wodurch es enorm schwierig ist, die Qualität der Patientenversorgung aufrecht zu erhalten. Da immer weniger Fachkräfte für die Verwaltung von Sicherheitsmaßnahmen zur Verfügung stehen, entscheiden sich immer mehr Gesundheitsdienstleister für Managed Services, die sich um ihre Sicherheitsbelange kümmern. Proofpoint Applied Services for Data Security verstärkt Ihr Team mit unseren weltweit tätigen Datensicherheitsexperten. Wir haben jahrzehntelange Erfahrung und basierend darauf Best Practices und ein Reifegradmodell zur Optimierung Ihres Programms entwickelt. Wir decken Anwendungsverwaltung, Umfang und Richtlinien-Governance, Ereignisanalyse, Zwischenfallverwaltung und Berichte sowie Analysen ab. Dadurch werden Sie vor dem Diebstahl geistigen Eigentums und vor Verletzungen des Patientendatenschutzes bewahrt. Unsere Experten konzipieren, implementieren und betreiben ein Programm, das speziell für Ihre Sicherheits- und Compliance-Anforderungen maßgeschneidert wurde. Wir verwenden hochentwickelte Machine Learning-Techniken wie DLP und ITM sowie menschliche Analysen, um die Sicherheit Ihrer medizinischen Informationen zu gewährleisten. Warnmeldungen werden untersucht und für schnelle Reaktionen auf Kompromittierungsversuche genutzt. Wir helfen Ihnen gern dabei, Ihre Sicherheit zu verbessern und Ihr Team optimal einzusetzen, sodass Sie sich auf andere Themen konzentrieren können.

Fazit

Die letzten Jahre haben alle Gesundheitseinrichtungen vor beispiellose Herausforderungen gestellt. Angesichts von Kostensenkungen, geringeren Rückerstattungen und Fachkräftemangel sind die unruhigen Zeiten jedoch noch nicht vorbei. Gleichzeitig hat sich die Infrastruktur verändert. Die Angriffsflächen sind gewachsen, weshalb Datensicherheitsmaßnahmen vom Rechenzentrum auf mehrere Clouds ausgeweitet werden müssen. Mitarbeiter und Patienten melden sich weiterhin häufig von anderen Orten an und die Anzahl medizinischer IoT-Geräte am Netzwerkrand steigt. Seit fast zwei Jahrzehnten konzentrieren sich Einrichtungen auf die Absicherung des Perimeters. Doch der klassische Perimeter existiert so nicht mehr. Heute ist jeder einzelne Mitarbeiter gleichzeitig Perimeter und Netzwerkrand. Mit den Datensicherheitslösungen von Proofpoint erhalten Sie Echtzeiterkenntnisse zu datenbezogenen Risiken. Sie können Datenverlust verhindern, indem Sie Zwischenfälle priorisieren und darauf reagieren. Außerdem umfasst die Plattform verschiedene Compliance-bezogene und gesetzlich vorgeschriebene Funktionen wie Datenerkennung, -klassifizierung und -verschlüsselung, damit Sie gesetzliche Anforderungen und Branchenstandards erfüllen können. Sie schützen Ihre Einrichtung, indem Sie die Personen schützen, die mit Ihren vertraulichen Informationen arbeiten.

proofpoint.

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune 100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: LinkedIn

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →

0207-005-04-04 6/25