proofpoint.

KURZVORSTELLUNG

Absichern von Gesundheitsdienstleistern mit Proofpoint

Schutz für Menschen, KI-Agenten und Patientendaten, um sichere und resiliente Versorgung zu gewährleisten

Überblick

Da die Gesundheitsversorgung immer digitaler, dezentralisierter und automatisierter wird, sehen sich Gesundheitsdienst-leister mit einer Angriffsfläche konfrontiert, die sich gleichzeitig in alle Richtungen ausdehnt. Personalmangel führt dazu, dass Mitarbeiter oft keine Zeit haben, um Sicherheitsvorschriften einzuhalten. Cloud-Dienste und vernetzte medizinische Geräte schaffen neue Angriffspunkte. Und KI-gestützte Arbeitsabläufe bringen neue Schwachstellen mit sich.

Bedrohungsakteure haben dies bemerkt und nutzen all diese Veränderungen zu ihrem Vorteil. Sie verstehen, dass Sicherheitsverletzungen im Gesundheitswesen oft von Menschen oder von KI-Agenten ausgehen, die in ihrem Namen handeln. Daher konzentrieren sie sich auf identitäts-zentrierte Angriffe, Social Engineering und den Missbrauch von vertrauenswürdigen Zugriffsrechten.

Proofpoint unterstützt Krankenhäuser, Gesundheitsdienste, Kliniken und integrierte Versorgungsnetzwerke beim Schutz ihrer Mediziner, Mitarbeiter, Systeme und Patienten und sichert das gesamte Ökosystem aus Menschen, KI-Agenten und Daten ab. Unsere integrierten Cybersicherheits- und Compliance-Lösungen reduzieren das Risiko von Datenschutzverletzungen, schützen vertrauliche Daten und unterstützen die zuverlässige und ununterbrochene Patientenversorgung.

Wertvolle Ziele im Gesundheitswesen

Gesundheitsdienstleister gehören heute zu den am häufigsten angegriffenen Unternehmen. Sie arbeiten nicht nur unter enormem Druck, sondern verwalten auch große Mengen hochvertraulicher Daten. Dazu gehören:

- Geschützte Gesundheitsdaten wie Patientenakten, Diagnoseergebnisse und Behandlungsdaten
- Personenbezogene Daten
- Finanz-, Abrechnungs- und Lohn- und Gehaltsdaten

Diese Informationen sind für Angreifer äußerst wertvoll und ihr Verlust ist mit hohen Kosten verbunden. Ein Verstoß kann zu Geldstrafen, Rechtsverfahren, Reputationsschäden und zur Beeinträchtigung der Versorgung und Sicherheit von Patienten führen.

Gesundheitsdienstleister stehen auch vor branchenspezifischen Herausforderungen:

- Das medizinische Fachpersonal benötigt schnellen und ununterbrochenen Zugriff auf Systeme.
- Die Kommunikation enthält häufig vertrauliche und zeitkritische Informationen.
- Die Versorgungsteams arbeiten mit Krankenhäusern, Kliniken, Laboren und externen Parteien zusammen.
- Rechtliche Überprüfungen, Audits und Untersuchungen sind üblich.

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die Menschen und Daten an agentenbasierten Arbeitsplätzen schützt.

E-Mail und Cloud-basierte Collaboration-Tools sind für die koordinierte Patientenversorgung unerlässlich, stellen jedoch auch die wichtigsten Einfallstore für Cyberangreifer dar.

Laut dem *Verizon Data Breach Investigations Report 2025* gehen 60 % aller Datenschutzverletzungen mit einer menschlichen Komponente einher.

Herausforderungen bei der Cybersicherheit für Gesundheitsdienstleister

Bei der Modernisierung ihrer Abläufe sehen sich Gesundheitsdienstleister mit einer Reihe wachsender Risiken konfrontiert.

Absicherung von klinischen und Patientendaten

Gesundheitsdienstleister müssen Gesundheitsdaten, personenbezogene Daten und Finanzdaten in E-Mails, auf Cloud-Plattformen und auf Endpunkten schützen. Jede Sicherheitsverletzung kann zu Verstößen gegen HIPAA, HITECH, Datenschutz-vorschriften und PCI DSS-Compliance-Vorgaben sowie zu kostspieligen Rechtsstreitigkeiten führen.

Reduzierung der Insider-Risiken in klinischen Umgebungen

Das Insider-Risiko ist in allen Bereichen erhöht. Die allgemeine Personalfluktuation ist hoch – hinzu kommen die Schichtteams, die aus ständig wechselnden Mitarbeitern, Auftragnehmern und Assistenzärzten bestehen. Gleichzeitig besteht ein allgemeiner Zugang zu elektronischen Patientenakten. Versehentliche Datenkompromittierungen, die Weitergabe von Zugangsdaten und der Missbrauch von Zugriffsrechten können gleichermaßen zu meldepflichtigen Sicherheitsverletzun-gen führen.

Abwehr von Bedrohungen durch Nachahmung und Kontoübernahmen

Gesundheitsdienstleister sind auf ein komplexes Ökosystem von Drittanbietern wie Laboren, Geräteanbietern, Zulieferern, Versicherern und Behörden angewiesen. Angreifer nutzen diese vertrauenwürdigen Beziehungen per Business Email Compromise (BEC), Nachahmung von Anbietern und Anmeldedaten-Phishing aus. Gemeinsam genutzte Postfächer und Service Konten sind dabei besonders attraktive Ziele.

Schnelle Reaktion auf hochentwickelte Bedrohungen

Sicherheitsteams erhalten eine überwältigende Anzahl an Warnmeldungen. Manuelle Überprüfungen lassen sich jedoch nicht einfach skalieren, vor allem dann nicht, wenn Angriffe hunderte Anwender erreichen oder von scheinbar vertrauenswür-digen Identitäten ausgehen.

Vorbereitung auf eine Cloud-basierte Pflegeumgebung

Mediziner greifen zunehmend aus dem Homeoffice auf Systeme zu und nutzen dabei häufig ihre privaten Geräte. Es ist nicht mehr praktikabel, den gesamten Datenverkehr über lokale Sicherheits-kontrollen zu leiten. Für effektive Sicherheit benötigen Teams einen Überblick darüber, wer wie und warum auf vertrauliche Daten zugreift.

Ein personen- und agentenzentrierter Ansatz für die Sicherheit im Gesundheitswesen

Gemeinsam bilden Menschen und Agenten die operative Ebene der Gesundheitsversorgung. Mediziner und Mitarbeiter leiten die Behandlungs- und Geschäftsprozesse ein, erhalten inzwischen aber auch Unterstützung durch nichtmenschlichen Agenten. Dazu gehören:

- Gemeinsam genutzte Postfächer und Service-Konten
- Cloud-Identitäten und APIs
- Automatisierte Arbeitsabläufe und KI-gestützte Systeme
- Vernetzte medizinische Geräte
- Klinische und geschäftliche Anwendungen wie Epic

Deshalb nutzen heutige Cyberangriffe nicht nur die Technologie, sondern zunehmend vertrauens-würdige Personen und Agenten aus.

Leider können herkömmliche Perimeter-basierte Sicherheitslösungen nicht zwischen legitimen Aktionen und schädlichem Verhalten unterscheiden. Dies gilt vor allem dann, wenn Angreifer für ihre betrügerischen Aktivitäten kompromittierte Identitäten anstelle von Malware verwenden.

Proofpoint schützt diese Umgebung durch die Korrelation von Identitäten, Verhaltensweisen und Datenzugriffen sowohl für Menschen als auch für Agenten. Dadurch werden blinde Flecken beseitigt, die Angreifer aktiv ausnutzen.

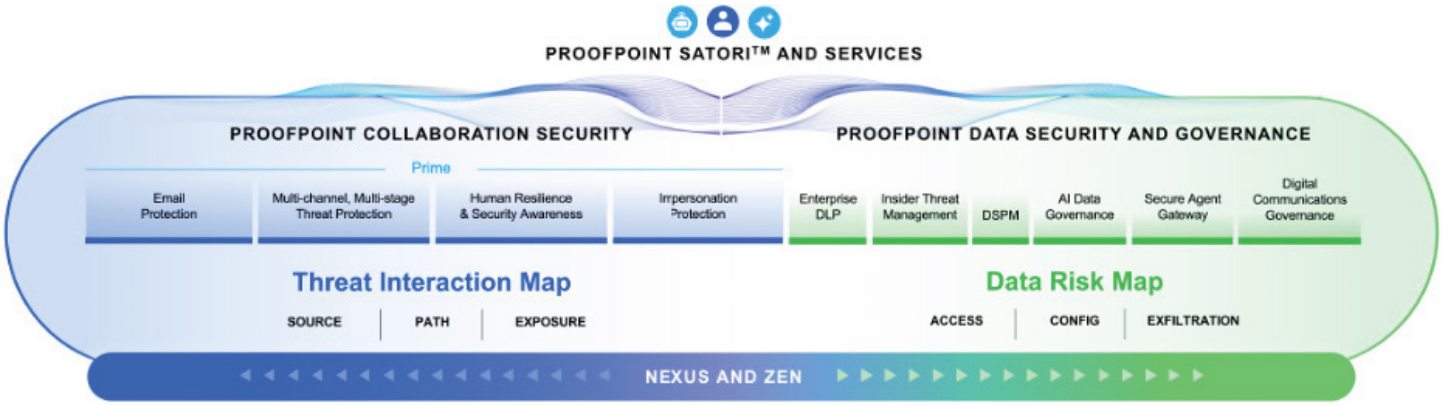


Abbildung 1. Die Proofpoint-Lösungen schützen das gesamte Ökosystem aus Menschen, KI-Agenten und Daten.

Produkte

- Proofpoint Collaboration Security Prime
- Proofpoint Secure Email Relay
- Proofpoint Data Loss Protection (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Satori
- Proofpoint Account Takeover Protection
- Proofpoint Insider Threat Management
- Proofpoint Communications Governance
- Proofpoint ZenGuide

So kann Proofpoint Gesundheitsdienstleister unterstützen

Proofpoint genießt das Vertrauen von 67 % der Fortune 500-Unternehmen im Gesundheitswesen. Nur Proofpoint bietet eine integrierte Plattform, die Menschen, Agenten und Daten gleichermaßen schützt.

In diesem Abschnitt werden die vielen Möglichkeiten erläutert, wie wir helfen können.

Schutz vor Ransomware und anderen hochentwickelten Bedrohungen

Proofpoint Collaboration Security Prime bietet einen umfassenden Ansatz zur Abwehr von Angriffen, die auf Menschen und Agenten abzielen und dazu E-Mails, Collaboration-Tools, Cloud-Anwendungen, Webkanäle und Social-Media-Plattformen missbrauchen. Die Lösung nutzt **Proofpoint Nexus®** für fortschrittliche KI, Verhaltensanalysen und Bedrohungsdaten, um Angriffe über den gesamten Bedrohungs-zyklus hinweg zu blockieren – von vor der Zustellung bis zum Klickzeitpunkt.

Absicherung kritischer E-Mail- und Anwendungskommunikation

Gesundheitsdienstleister sind für wichtige klinische und betriebliche Arbeitsabläufe auf systemgenerierte E-Mails angewiesen, darunter:

- Patientenbenachrichtigungen und Terminerinnerungen
- Pflegekoordinierung und gesundheitliche Warnmeldungen
- Rechnungsbescheide und Finanzkommunikation
- Compliance-, Berichts- und Verwaltungsmitteilungen

Diese Mitteilungen werden häufig in großer Menge von vertrauenswürdigen Anwendungen versendet und müssen folgende Kriterien erfüllen:

- Zuverlässige Zustellung
- Authentifiziert und von den Empfängern als vertrauenswürdig eingestuft
- Sicher und vorschriftenkonform

Proofpoint Secure Email Relay ermöglicht Gesundheitsdienstleistern das sichere Versenden großer Mengen an App-E-Mails, während Patienten, Partner und das Unternehmen gleichzeitig vor Nachahmung und Betrug geschützt sind. Proofpoint Secure Email Relay bietet folgende Vorteile:

- Ermöglicht die DMARC-konforme E-Mail-Zustellung von kritischen Anwendungen wie Epic, ServiceNow und anderen klinischen und geschäftlichen Plattformen
- Schützt systemgenerierte E-Mails vor Spoofing und Missbrauch durch Doppelgänger-Domains
- Gewährleistet Vertrauenswürdigkeit und Integrität in der patientenbezogenen und betrieblichen Kommunikation
- Verringert das Risiko durch kompromittierte oder falsch konfigurierte App-E-Mails

Durch die Absicherung nicht-menschlicher Absender erweitert Proofpoint Secure Email Relay das agentenzentrierte Cybersicherheitsmodell von Proofpoint. Dadurch ist gewährleistet, dass die Kommunikation im Gesundheitswesen vertrauenswürdig, vorschriftenkonform und zuverlässig bleibt.

Sichere Speicherung von Patientendaten

Proofpoint Data Loss Prevention (DLP)-Lösungen verhindern versehentlichen oder böswilligen Datenverlust per E-Mail, Cloud und über Endpunkte, indem sie umfassende Einblicke in das Anwenderverhalten und Inhalte liefern.

Proofpoint Adaptive Email DLP nutzt verhaltensbasierte KI, um normale E-Mail-Versandmuster zu analysieren und Medizinern und Mitarbeitern kontextbezogene Warnungen in Echtzeit zu übermitteln. Die Lösung verhindert fehlgeleitete Nachrichten und Datenkompromittierungen, ohne die Patientenversorgung zu beeinträchtigen.

Proofpoint Data Security Posture Management (DSPM) identifiziert, wo vertrauliche Daten gespeichert sind, welche Menschen und Agenten darauf zugreifen können und wo übermäßige oder riskante Berechtigungen bestehen. Dadurch können Gesundheitsdienstleister ihre Angriffsfläche verringern und KI sowie Automatisierung sicher einführen.

Proofpoint Satori™ erweitert DSPM durch Governance für Echtzeit-Datenzugriffe in Gesundheitseinrichtungen. Proofpoint Satori überwacht und kontrolliert kontinuierlich den Zugriff auf vertrauliche Patientendaten und deckt dabei Cloud-Datenspeicher, Analyseplattformen und KI-Pipelines ab, ohne die klinischen Arbeitsabläufe zu stören.

Proofpoint Satori bietet für Gesundheitsdienstleister folgende Vorteile:

- Erkennung und Klassifizierung vertraulicher Patientendaten und klinischer Daten über Cloud-Plattformen hinweg
- Durchsetzung von Least-Privilege-Zugriffen für Mediziner, Mitarbeiter, Anwendungen und KI-Agenten
- Erkennung und Behebung riskanter oder ungewöhnlicher Datenzugriffe in Echtzeit
- Anwendung richtlinienbasierter Kontrollen, um personenbezogene Gesundheitsdaten zu schützen und gleichzeitig Analysen, Untersuchungen und KI-Innovationen zu ermöglichen

Erkennung von Kompromittierungen und Missbrauch in großem Umfang

Proofpoint Account Takeover Protection und **Proofpoint Insider Threat Management** erkennen verdächtiges Verhalten sowohl bei menschlichen Identitäten als auch bei Agentenidentitäten. Die Lösungen erkennen die Kompromittierung von Anmeldedaten, den Missbrauch von Berechtigungen, laterale Bewegungen und Datenexfiltration. Durch die Korrelation von Identität, Verhalten und Datenbewegungen ermöglicht Proofpoint schnellere und genauere Reaktionen, bevor die Patientenversorgung beeinträchtigt wird.

Vorschriftenkonformität und Bereitschaft für Rechtsstreitigkeiten

Proofpoint Digital Communications Governance-Lösungen vereinfachen die Einhaltung von HIPAA, HITECH und Aufbewahrungsvorschriften. Sie gewährleisten, dass klinische und geschäftliche Kommunikation erfasst, durchsuchbar und für Audits, Untersuchungen und E-Discovery verfügbar ist.

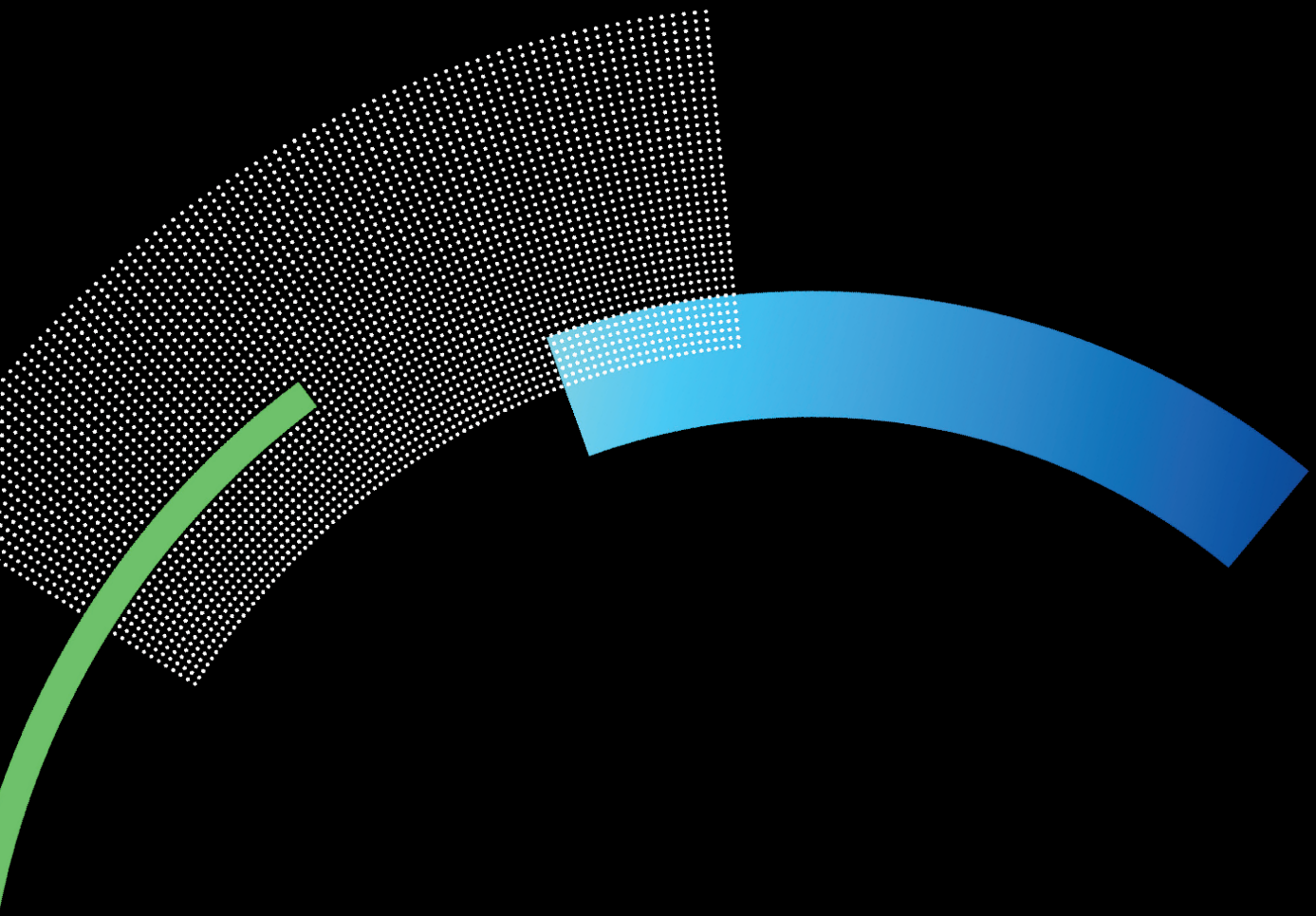
Risikominimierung durch Verhaltensänderung

Proofpoint ZenGuide™ bietet rollenbasierte, risikoorientierte Schulungen zur Sensibilisierung für Sicherheit an, die auf Mediziner und Mitarbeiter zugeschnitten sind. Die Lösung fördert sicheres Verhalten durch die Simulation realer Bedrohungsszenarien im Gesundheitswesen, ohne die Patientenversorgung zu beeinträchtigen.

Fazit

Proofpoint hat schon immer Menschen geschützt. Jetzt erweitert unsere personen- und agentenzentrierte Sicherheitsplattform den Schutz auf jede Interaktion zwischen Menschen, Daten und KI-Agenten. Wir bieten Kontrolle, Compliance sowie reibungslose Möglichkeiten zur Implementierung von Innovationen.

Mit Proofpoint können Gesundheitsdienstleister das Risiko von Datenschutzverletzungen reduzieren, Patientendaten schützen, die Einhaltung von Vorschriften gewährleisten und in einer komplexen Bedrohungslandschaft die zuverlässige und ununterbrochene Versorgung sicherstellen.



proofpoint.

Information zu Proofpoint, Inc. Proofpoint, Inc. ist ein weltweiter Marktführer bei personen- und agentenzentrierter Cybersicherheit und schützt Verbindungen zwischen Anwendern, Daten und KI-Agenten über E-Mail, Cloud und Collaboration-Tools. Proofpoint ist ein vertrauenswürdiger Partner für mehr als 80 Prozent der Fortune 100, über 10.000 große Unternehmen sowie für Millionen kleinerer Firmen und stoppt Bedrohungen, verhindert Datenverlust und sichert die Interaktionen zwischen Anwendern und KI-Workflows ab. Die Collaboration- und Datenschutzplattform von Proofpoint hilft Unternehmen jeder Größe, ihre Mitarbeiter zu schützen und zu unterstützen, damit sie KI sicher und bedenkenlos einsetzen können. Weitere Informationen unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: LinkedIn

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →