proofpoint.

KI bei Proofpoint

KI bietet neue und innovative Möglichkeiten für Anwender, ihre Arbeit zu erledigen. Sie hilft aber auch Bedrohungsakteuren, ihre eigene Produktivität zu steigern. Ihre Taktiken, Techniken und Prozesse (TTPs) werden durch KI verstärkt, sodass sie mehrstufige und kanalübergreifende Angriffe im globalen Maßstab durchführen können. Diese Bedrohungen umgehen häufig herkömmliche Sicherheitsmaßnahmen und sind für Anwender kaum zu erkennen.

Die Risiken gehen jedoch nicht nur von externen Angriffen aus. Datenkompromittierungen sind zunehmend die Folge alltäglicher Verhaltensweisen von Anwendern innerhalb des Unternehmens. Hier kann KI helfen. Sie kann den Datenfluss überwachen, riskantes Verhalten im Kontext erkennen und entlastet SOC-Teams (Security Operations Center) dadurch erheblich.

Der Einfluss von KI auf die Arbeit entwickelt sich weiter – und Proofpoint bietet branchenweit führenden KI-gestützten Schutz für unsere Kunden. Durch die Kombination kontinuierlicher KI-gestützter Innovationen mit hervorragenden Bedrohungsdaten bleiben unsere Lösungen Bedrohungsakteuren einen Schritt voraus, sodass Unternehmen ihre vertraulichen Daten schützen und in einer zunehmend KI-gestützten Welt ihre Sicherheit gewährleisten können.

94 %

Proofpoint stellte im Jahr 2025 eine Zunahme der E-Mail-Bedrohungen gegen unsere Kunden um 94 % fest.

Wie Bedrohungsakteure Angriffe mithilfe von KI skalieren

Proofpoint hat die Auswirkungen von KI in den Händen von Bedrohungsakteuren direkt beobachtet. Im Jahr 2025 stellte Proofpoint im Vergleich zum Vorjahr eine Zunahme der E-Mail-Bedrohungen gegen unsere Kunden um 94 % fest. Die Bedrohungslandschaft wird immer raffinierter und umfasst inzwischen KI-Prompt-Injection, E-Mail-Bombing und den Missbrauch legitimer Dienste.

Bedrohungsakteure nutzen KI auf verschiedene Weise zur Verstärkung ihrer Aktivitäten:

- **Verstärkung:** KI ermöglicht Bedrohungsakteuren die Durchführung komplexerer Angriffe auf einer breiteren Angriffsfläche. In diesem Jahr haben wir tausende E-Mails beobachtet, die sich an KI-Agenten richteten, damit diese im Namen des Bedrohungsakteurs handeln.

- **Reduzierung der Einstiegshürde:** KI kann 80-90 % der Angriffskette automatisieren, sodass Bedrohungsakteuren mehr Zeit für komplexere Angriffe zur Verfügung steht. Wir haben eine Zunahme bei mehrstufigen und kanalübergreifenden Angriffen beobachtet, bei denen jeweils tausende unerwünschte Nachrichten versendet werden.

- **Erweitertes Targeting:** Vor der Einführung der KI verließen sich Bedrohungsakteure für ihre Angriffe auf vorhersehbare, generische Vorlagen. Mit KI können sie Angriffe erstellen, die für jedes Opfer personalisiert sind. In diesem Jahr haben wir eine Zunahme bei personalisierten Angriffe mit Missbrauch legitimer Dienste festgestellt.

Alle diese Entwicklungen erschweren die zuverlässige Identifizierung von E-Mail-Bedrohungen. Hier können semantische Analysen und andere Methoden helfen, die auf großen Sprachmodellen basieren.

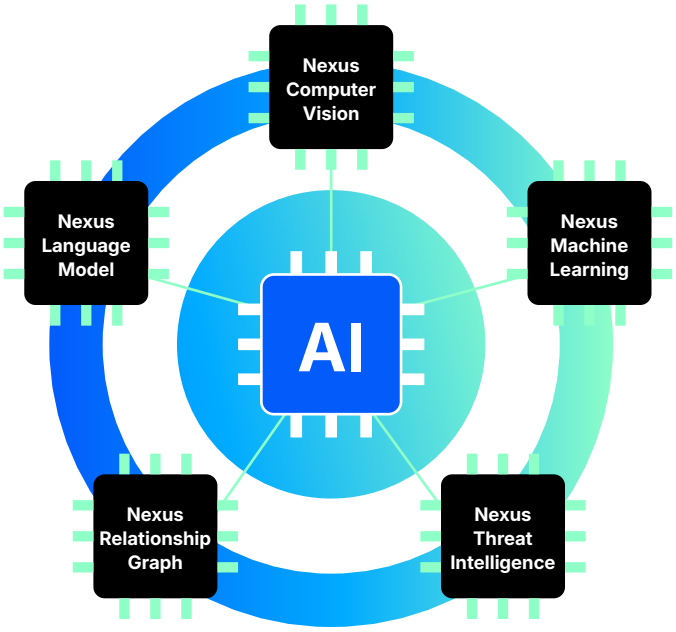
Proofpoint Nexus AI für sichere Zusammenarbeit

Die **Proofpoint Collaboration Security-Lösungen** nutzen unsere Nexus™ AI-Plattform, die einen mehrschichtigen Ansatz zur Bedrohungserkennung verwendet.

KI zur Erkennung und Blockierung von Bedrohungen

Nexus umfasst mehrere KI-gestützten Module, um Angriffe präzise zu erkennen sowie abzuwehren und zusammen eine Erkennungsgenauigkeit von 99,999 % zu erreichen. Dazu werden Machine Learning, Bilderkennung (Computer Vision), Beziehungsdiagramme, Bedrohungsdaten und Sprachmodelle kombiniert.

Die Proofpoint Nexus AI-Modelle verarbeiten jährlich 2,3 Billionen E-Mails, unterstützt von einem Bedrohungsdaten-Team, das über 100 verschiedene Bedrohungsakteurgruppen und mehr als 8.400 aktive Bedrohungskampagnen verfolgt.



Nexus LM™ (Language Model) erkennt BEC- und raffinierte Phishing-Bedrohungen und nutzt hochentwickelte Sprachanalysen (z. B. auf Transaktionssprache, Dringlichkeit, Kontext und Absicht), um versteckte Bedrohungen und unbekannte Datenrisiken aufzudecken.

Nexus RG™ (Relationship Graph) identifiziert subtile Verhaltensänderungen in der Kommunikation Ihrer Anwender, erkennt Abweichungen vom normalen Verhalten, volumetrische Veränderungen sowie die Weitergabe vertraulicher Unternehmensdaten, um das Risiko von Angriffen durch Fehlverhalten zu verringern.

Nexus TI™ (Threat Intelligence) versteht die Taktiken der Angreifer und schützt proaktiv vor neuen Cyberbedrohungen. Dazu identifiziert das Modul mithilfe von Echtzeitdaten neue Angriffstaktiken und Systemschwachstellen und löst Sandbox-Analysen zur Erkennung von verdächtigen URLs und Anhängen aus.

Nexus CV™ (Computer Vision) identifiziert und neutralisiert bildbasierte Bedrohungen. Das Modul kann mithilfe hochentwickelter Bilderkennungstechnologien Bedrohungen erkennen, die in visuellen Elementen verborgen sind, z. B. in Phishing-Websites, QR-Codes, schädlichen Anhängen und gefälschten E-Mails.

Nexus ML™ (Machine Learning) verwendet dynamische und adaptive Lerntechniken wie überwachtes Lernen, unüberwachtes Lernen und Ensemble-Methoden und kombiniert diese Techniken mit prädiktiven Funktionen zur Bedrohungserkennung, um bekanntes Angriffsverhalten abzubilden, sowie unüberwachte Methoden zur Erkennung unbekannter Auffälligkeiten.

Proofpoint Nexus AI für Datensicherheit und Governance

Die leistungsstarken, marktführenden Proofpoint Nexus-Module unterstützen auch unsere Lösungen für **Datensicherheit und Governance**.

KI zur Verhinderung von Datenlecks

Nexus kategorisiert Daten und verfolgt Datenbewegungen – ganz gleich, ob sich die Empfänger innerhalb oder außerhalb des Unternehmens befinden.

Nexus LM™ (Language Model) lernt die realen Geschäftsdokumenttypen (z. B. Abschlussunterlagen, Prognosen oder Produktdesigns) Ihres Unternehmens kennen und wandelt diese erlernten Klassen in einen entscheidungsrelevanten Richtlinienkontext um, sodass vertrauliche Daten auch ohne eine manuelle Anpassung schnell erkannt, priorisiert und geschützt werden.

Nexus RG™ (Relationship Graph) versteht Zusammenhänge und kann dadurch versehentliche und vorsätzliche Datenverluste durch fehlgeleitete E-Mails sowie Datenexfiltrationen verhindern.

Nexus TI™ (Threat Intelligence) schützt vor kompromittierten Konten, die intern und extern Phishing-E-Mails versenden.

Nexus CV™ (Computer Vision) erkennt vertrauliche Inhalte in Bildern in E-Mails und Dokumenten.

Nexus ML™ (Machine Learning) bietet einen umfassenden Überblick darüber, wie Dateien zwischen Repositorys und Zielen erstellt, kopiert, umbenannt, weiter- und freigegeben sowie verschoben werden. Das Modul verknüpft diese Aktivitäten mit einer nachvollziehbaren Zeitleiste zur Herkunft, die schnellere Untersuchungen, ursprungbasierte Kontrollen und auditfähige Nachweise für Datenschutzprogramme unterstützt.

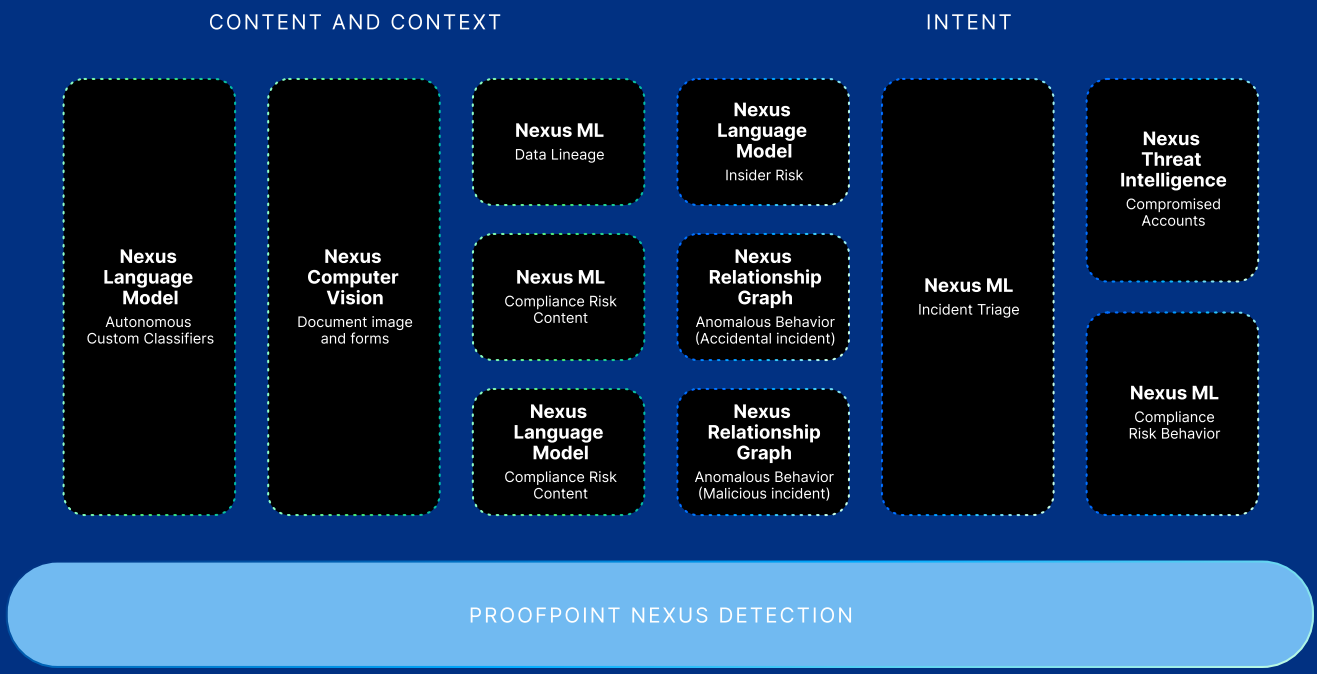


Abb. 1: Proofpoint Nexus unterstützt Lösungen für Datensicherheit und Governance.

Agentenbasierte KI bei Proofpoint

In Bezug auf agentenbasierte KI investiert Proofpoint in zwei wichtige Bereiche.

1. Proofpoint Satori™ Agents

Wir entwickeln KI-Agenten, die sich in bestehende Proofpoint-Lösungen integrieren. Satori-Agenten automatisieren Aufgaben und reduzieren den manuellen Aufwand Ihrer SOC-Teams.

- Der **Abuse Mailbox Agent** automatisiert die manuelle Überprüfung gemeldeter Nachrichten, damit SOC-Teams weniger Zeit für die Unterscheidung zwischen echten Bedrohungen und sicheren E-Mails aufwenden müssen.
- **Der DLP Triage Agent** verwaltet Warnmeldungen und die Aktivitätsüberwachung für Ihre Lösung zur Datenverlustprävention (DLP).
- **Der Phishing Simulation Agent** verwendet KI-Automatisierung, um Sie bei Ihren Security-Awareness-Programmen zu unterstützen und die Resilienz Ihrer Mitarbeiter zu stärken.

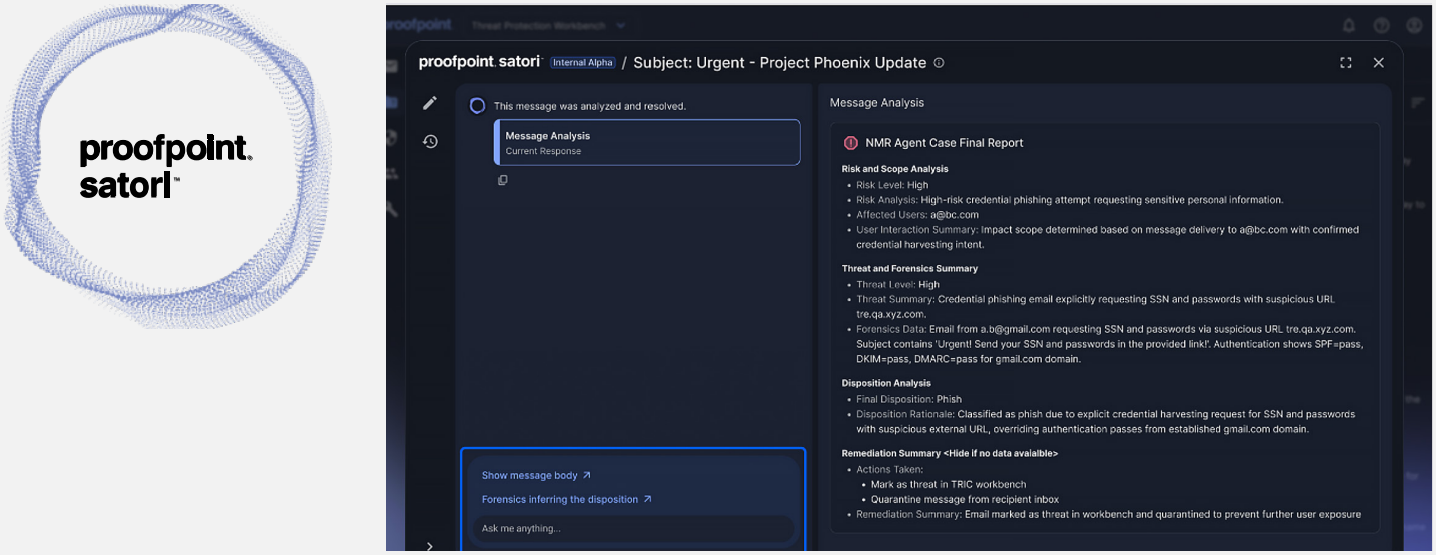


Abb. 2: Der Proofpoint Satori Abuse Mailbox Agent in Aktion.

2: Proofpoint Secure Agent Gateway

Bei der Implementierung agentenbasierter KI-Workflows entstehen in Ihrem Unternehmen Sicherheitslücken. Wir tragen dieser Tatsache Rechnung, indem wir unsere Proofpoint Human-Centric Security-Plattform erweitern, sodass sie auch alle Ihre Agenten schützt.

Proofpoint Secure Agent Gateway schützt Ihre agentenbasierten Workflows und vereinheitlicht die Kontrolle aller Agenten in Ihrer Umgebung.

- **Schützt vertrauliche Daten ,** die bei agentenbasierten Workflows verarbeitet werden.
- **Wird unterstützt von unserer MCP-Technologie** (Model Context Protocol)
- **Kontrolliert den Zugriff auf vertrauliche Daten ,** die von Agenten verwendet werden