PERSONENZENTRIERTE SICHERHEIT

Umsetzen personenzentrierter Sicherheit in der modernen digitalen Arbeitswelt

Wie Sie im Zeitalter der digitalen Transformation mit der umfassenden, mehrschichtigen Proofpoint-Plattform personenzentrierte Sicherheit zum Leben erwecken

proofpoint®

Kurzfassung

Die moderne digitale Arbeitswelt hat unsere Arbeitsweise grundlegend verändert. Unternehmen vertrauen inzwischen der Cloud und Angestellte arbeiten in einem komplexen Mix von Umgebungen zusammen, zu denen u. a. Collaboration- und Messaging-Tools, Social-Media-Plattformen, SaaS-Anwendungen (Software as a Service), Large Language Models (LLMs) und File-Sharing-Dienste gehören.

Diese Transformation ermöglicht schnellere Innovationen und mehr Flexibilität, lässt aber auch viele neue Angriffsflächen für Bedrohungsakteure entstehen. Wissensarbeiter erstellen, speichern und nutzen Daten heute ganz anders, sodass klassische Sicherheitsstrategien, die sich auf den Schutz von Netzwerken und Endpunkten konzentrieren, einfach nicht mehr Schritt halten können. Die Veränderungen erfordern eine moderne Architektur, die zur Arbeitsweise der Unternehmen und ihrer Mitarbeiter passt – und der Tatsache Rechnung trägt, dass Cyberkriminelle heute hauptsächlich Anwender anstelle von Infrastruktur ins Visier nehmen.

Dieses Whitepaper stellt die Proofpoint Human-Centric Security-Plattform vor. Diese branchenweit erste umfassende personenzentrierte Sicherheitsplattform trägt neuen Gegebenheiten Rechnung und rückt die Mitarbeiter in den Fokus der modernen Verteidigungsstrategie.

In diesem Whitepaper erfahren Sie:

- Warum der **Schutz der Mitarbeiter** in der heutigen digitalen Arbeitswelt wichtiger ist als je zuvor
- Für die Lösung welcher **personenzentrierten Probleme** die Proofpoint-Plattform entwickelt wurde
- Wie die **Kerntechnologien** der Architektur Bedrohungen proaktiv erkennen, Anwender in Echtzeit unterstützen und schützen sowie Untersuchungen und Reaktionen vereinfachen

Mitarbeiter als neuer Perimeter: Warum ist personenzentrierte Sicherheit wichtig?

Im Mittelpunkt der Cybersicherheitslandschaft steht heute der Mensch. Inzwischen sind personenzentrierte Bedrohungen wie Phishing, Kontoübernahmen, Insider-Risiken und Datenexfiltration für den Großteil der Sicherheitsverletzungen verantwortlich. Die meisten modernen Angriffe setzen nicht bei technischen Schwachstellen, sondern bei den Mitarbeitern an. Bedrohungsakteure greifen Anwender in der immer komplexeren digitalen Arbeitswelt mit Täuschungs-, Ablenkungs- oder Manipulationsmethoden an.

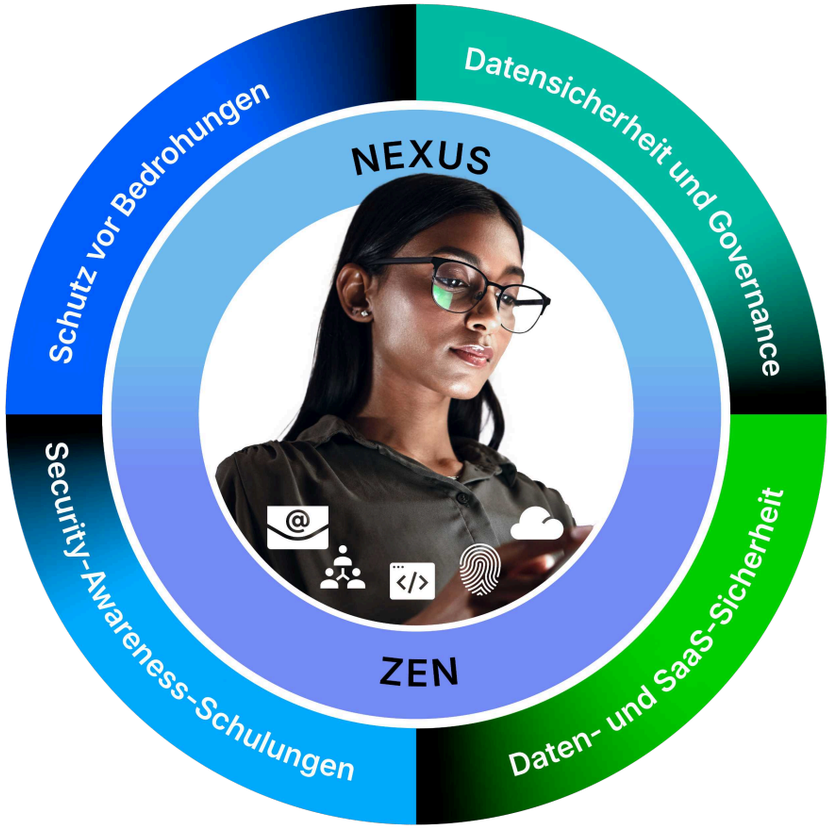
Während sich klassische Sicherheitsmodelle auf den Schutz von Netzwerken und Endpunkten konzentrieren, haben es die modernen Bedrohungen auf menschliche Schwachstellen abgesehen. Mit der Cybersicherheitsplattform von Proofpoint können Unternehmen ihre Mitarbeiter und ihre Daten mit einem personenzentrierten Ansatz schützen. Unsere Plattform umfasst erstklassige Lösungen, die die vier wichtigen Bereiche abdecken: Stoppen von Bedrohungen, Schützen von Informationen, Schulen von Anwendern und Stärken der Daten- und SaaS-Sicherheit.

BEDROHUNGSSCHUTZ

Stoppen von Bedrohungen, die auf Ihre Mitarbeiter abzielen

SENSIBILISIERUNG FÜR SICHERHEIT

Kontinuierliche Schulungen für Ihre Mitarbeiter



DATENSICHERHEIT UND GOVERNANCE

Schutz vor Datenverlust und Kommunikationskontrolle

DATEN- UND SAAS-SICHERHEIT

Schließen von Daten- und SaaS-Sicherheitslücken

Abb. 1: Die Proofpoint Human-Centric Security-Plattform bietet erstklassige Lösungen in vier zentralen Bereichen.

proofpoint.

Eine umfassende, mehrschichtige Plattform

Die umfassende Proofpoint-Plattform basiert auf einer mehrschichtigen Architektur und bietet diese Vorteile:

- **Proaktive Erkennung von Bedrohungen** in allen digitalen Arbeitsbereichen durch moderne KI, Machine Learning, Echtzeit-Bedrohungsdaten usw.
- **Zahlreiche Endnutzer-Kontrollfunktionen,** die Mitarbeiter und Daten in allen Arbeitsbereichen schützen
- **Warnungen, Schulungen und Unterstützung für Anwender,** die die Resilienz gegenüber personenzentrierte Angriffen stärken
- **Vereinfachte Untersuchungen von Bedrohungen und Einleitung von Behebungsmaßnahmen**

Diese Funktionen werden durch drei Kerntechnologien ermöglicht: Proofpoint Nexus, Proofpoint Zen und Proofpoint Threat Protection Workbench. Diese werden in den folgenden Abschnitten im Detail vorgestellt.

proofpoint.

Proofpoint Nexus

KI-gestützte Erkennung und Bedrohungsdatenanalysen

Proofpoint Nexus® ist die Erkennungsschicht der Proofpoint-Architektur und nutzt als einheitliches Erkennungsframework künstliche Intelligenz (KI), Machine Learning und Echtzeit-Bedrohungsdatenanalysen.

Proofpoint Nexus integriert mehrere KI-Modelltypen, die jeweils spezielle Risikoindikatoren in allen Mitarbeiteraktivitäten analysieren, z. B. in E-Mails, Cloud-Anwendungen, Collaboration-Tools und Browsern.

Wichtige Komponenten des Proofpoint Nexus-Erkennungsframeworks

Nexus Threat Intelligence (TI) erfasst kontinuierlich Indikatoren von bekannten und unbekannten Bedrohungsakteuren, Kampagnen und Infrastrukturen, um umfassende Kontextdaten zu Erkennungen zu gewinnen. Diese stehen den Proofpoint-Produkten für die Anpassung an die dynamischen Bedrohungsmethoden zur Verfügung.

Nexus Language Model (LM) nutzt hochentwickelte KI-Sprachmodelle, um den Tonfall, die Dringlichkeit und die linguistische Struktur von Nachrichten zu bewerten, die im Rahmen von Social-Engineering-Angriffen wie BEC (Business Email Compromise) versendet werden.

Nexus Relationship Graph (RG) korreliert Anwenderaktivitäten, Verhaltenshistorie und das Risiko, das von der Position der jeweiligen Anwender ausgeht, um die Wahrscheinlichkeit von riskantem Verhalten bzw. von gezielten Angriffen auf besonders gefährdete Personen zu bewerten.

Nexus Machine Learning (ML) erkennt ungewöhnliches Anwenderverhalten in Messaging- und Collaboration-Tools und achtet auf subtile, aber wichtige Indikatoren für kompromittierte Konten oder Fehlverhalten von Insidern.

Nexus Computer Vision (CV) erkennt Markennachahmungs- und visuelle Betrugstaktiken, indem es das Layout, die Platzierung von Logos und die Nachahmung von Designs analysiert. 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.

Proofpoint Nexus erkennt komplexe Phishing-Angriffe, Diebstahl von Anmeldedaten, Nachahmungsversuche und Ransomware-Kampagnen. In einem realen Fall stellte Proofpoint Nexus die Kompromittierung eines Lieferanten fest, dessen Buchhaltung mit dem Ziel des Rechnungsbetrugs angegriffen werden sollte. Proofpoint Nexus blockierte den Angriff rechtzeitig, nachdem es sprachliche und visuelle Unstimmigkeiten erkannt und mit vorhandenen Bedrohungsdaten aus seinem globalen Datensatz kombiniert hatte.

Proofpoint Nexus bietet auch hervorragenden Schutz für Daten. In einem anderen realen Fall, bei dem ein Mitarbeiter Kundendaten in ein nicht autorisiertes GenAI-Tool einfügte, erkannte Proofpoint Nexus die vertraulichen Daten, erhöhte den Risikowert und blockierte die Aktion.

Proofpoint Nexus analysiert mehr als **2,6 Milliarden E-Mails pro Tag, untersucht täglich über 450 Millionen URLs** und korreliert Indikatoren von hunderten Bedrohungsakteuren. Diese enormen Datenmengen verbessern die Zuverlässigkeit und Reaktionsfähigkeit bei Bedrohungen aller Art.

proofpoint.

Proofpoint Zen

Kontrollpunkte und kontextbezogene Schulungen für Anwender

Proofpoint Zen™ ist die Erzwingungs- und Anwenderschulungsschicht der Proofpoint-Architektur und setzt Sicherheitsrichtlinien direkt am Arbeitsplatz der Anwender durch. Die Kontrollpunkte in der Proofpoint Zen-Suite verwandeln Informationen in Echtzeitschutz und richtlinien-basierte Schulungen, damit Anwender sicherere Entscheidungen treffen können, ohne dass ihre Produktivität darunter leidet.

Wichtige Komponenten der Proofpoint Zen-Suite

Zen for Outlook bettet Sicherheitstools in E-Mail-Workflows ein, um die Anwender als erste Verteidigungslinie zu stärken. Basierend auf den Echtzeit-Bedrohungsdaten von Proofpoint Nexus kann das Plugin den Anwendern bei verdächtigen E-Mails Inline-Warnungen anzeigen. Zudem bietet es eine einfache Möglichkeit, verdächtige Nachrichten zu melden. Außerdem werden bei riskantem Verhalten kontextbezogene Hinweise und bei vertraulichen Daten in ausgehenden E-Mails Warnmeldungen angezeigt.

ZenWeb ist eine ressourcenschonende Erweiterung für Chromium-basierte Browser, die Web-Aktivitäten über SaaS-, File-Sharing- und GenAI-Tools absichert und Anwender vor Phishing-Websites schützt. Durch die Live-Erkennungen der Proofpoint Nexus-Bedrohungsmodelle können Bedrohungen in Echtzeit erkannt und abgewehrt werden, ohne die Produktivität der Anwender zu beeinträchtigen.

Zen Endpoint DLP/Insider Threat Management überwacht das Anwenderverhalten am Endpunkt, um Schutz vor Datenverlust und Insider-Bedrohungen auf Geräteebene zu bieten. Dazu werden die USB-Nutzung, Zwischenablage-Aktivitäten, Dateisynchronisierungsvorgänge sowie das Anwendungsverhalten überwacht und Screenshots von verdächtigen Anwenderaktionen sowie Zeitleisten der Anwenderaktivitäten erstellt.

Zen Cloud API Connectors dehnen die Sicherheit auf Cloud-basierte SaaS-Plattformen wie Microsoft 365, Google Drive, Slack und Box aus, indem Datei-Uploads überwacht, ungewöhnliches Verhalten wie unverhältnismäßige Weitergabe bzw. Freigaben erkannt und benutzerdefinierte Workflows in Okta und SOAR-Tools (Security Orchestration, Automation and Response) ermöglicht werden.

Zen Communications Connectors erfassen die Kommunikation in regulierten Plattformen wie Microsoft Teams, Zoom und Slack zu Archivierungs- und Überwachungszwecken. Dazu werden Nachrichten aus verschiedenen Kanälen in einem einheitlichen Archivformat gespeichert und Integrationen mit Kontrolltools für die Workflows der Personal- und Rechtsabteilungen aufgebaut.

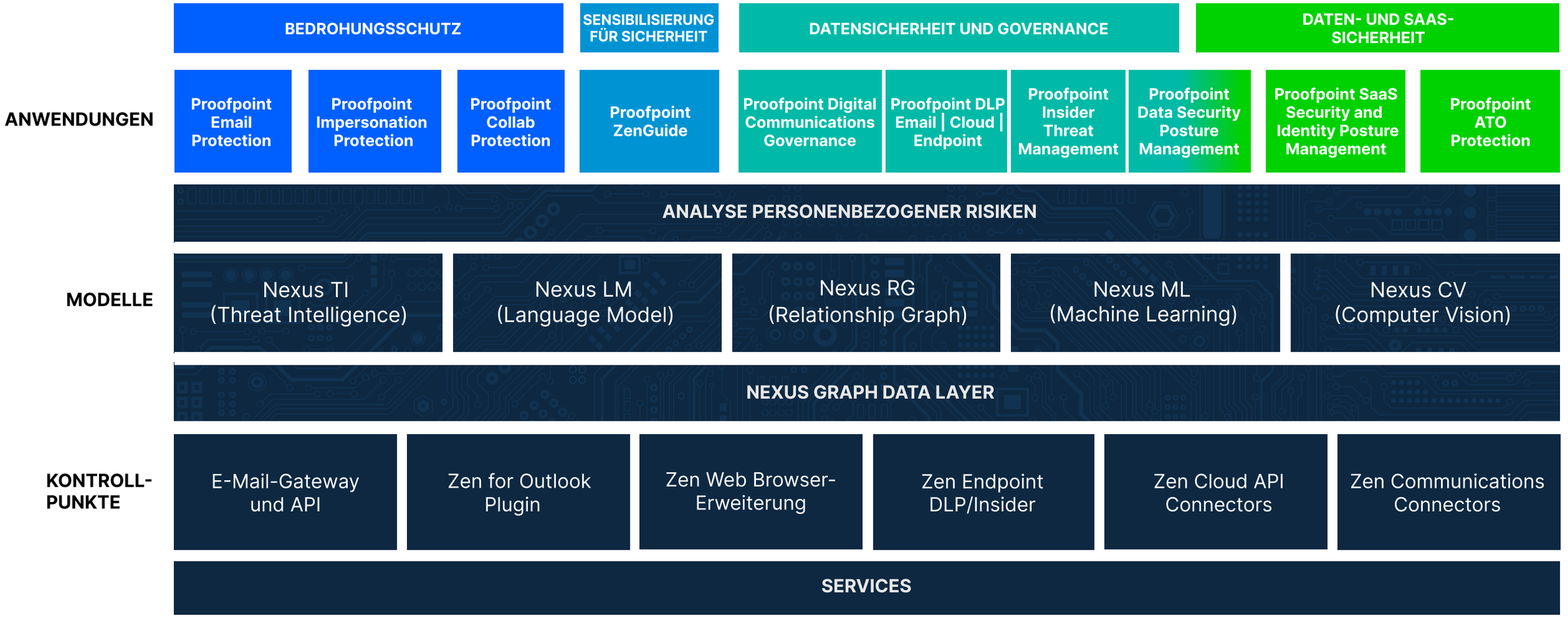


Abb. 2: Die Proofpoint Human-Centric Security-Plattform basiert auf einer mehrschichtigen Architektur. Proofpoint-Produkte (in unseren zentralen Bereichen Bedrohungsschutz, Sensibilisierung für Sicherheit, Datensicherheit und Governance sowie Daten- und SaaS-Sicherheit) nutzen direkt die Funktionen unserer Proofpoint Nexus- und Proofpoint Zen-Technologien.

Proofpoint Threat Protection Workbench

Schnelle Untersuchung und automatisierte Behebung

Wenn Bedrohungen oder Richtlinienverstöße erkannt werden, kommt es auf schnelles Handeln und klare Informationen an. Wenn die Teams in den Sicherheitskontrollzentren (SOCs) mit unterschiedlichen Konsolen arbeiten, zu viele Klicks benötigen und von anderen Teams abhängig sind, verlängern sich die Reaktionszeiten und das Risiko eines erfolgreichen Angriffs steigt.

Die Proofpoint Threat Protection Workbench ist die Untersuchungs- und Automatisierungsschicht der Proofpoint-Architektur. Dank dieser intuitiven, zentralisierten Konsole können Bedrohungen einfacher untersucht und Probleme schneller behoben werden, da Sicherheitsteams Triage, Analysen und Reaktionen durchführen können, ohne durch Toolwechsel oder fragmentierte Daten ausgebremst zu werden.

Sicherheitsteams verwenden die Proofpoint Threat Protection Workbench, um Abuse-Postfächer zu verwalten, Indikatoren zu besonders gefährdeten Anwendern zu eskalieren und Bedrohungskampagnen zu untersuchen. Die Proofpoint Threat Protection Workbench korreliert Proofpoint Nexus-Bedrohungsdaten mit Anwenderverhalten und Richtlinienauslösern, um präzise Warnungen statt unnötig vieler Meldungen auszugeben.

Anwendungsszenarien für Proofpoint Threat Protection Workbench (Beispiele)

- Automatisierte Reaktionen bei Untersuchungen zu Kontoübernahmen
- Klickpfad-Visualisierungen zu angegriffenen Anwendern
- Zusammenfassung komplexer Bedrohungen, die auf mehreren Kanälen aktiv sind

All diese Funktionen entlasten die Analysten und verkürzen die Verweildauer. Für die Reaktion auf Bedrohungen können Analysten direkt entsprechende Playbooks starten oder per API an weitere integrierte Komponenten innerhalb ihres Sicherheitsökosystems eskalieren.

Fazit

Eine speziell entwickelte Architektur für personenzentrierte Sicherheit

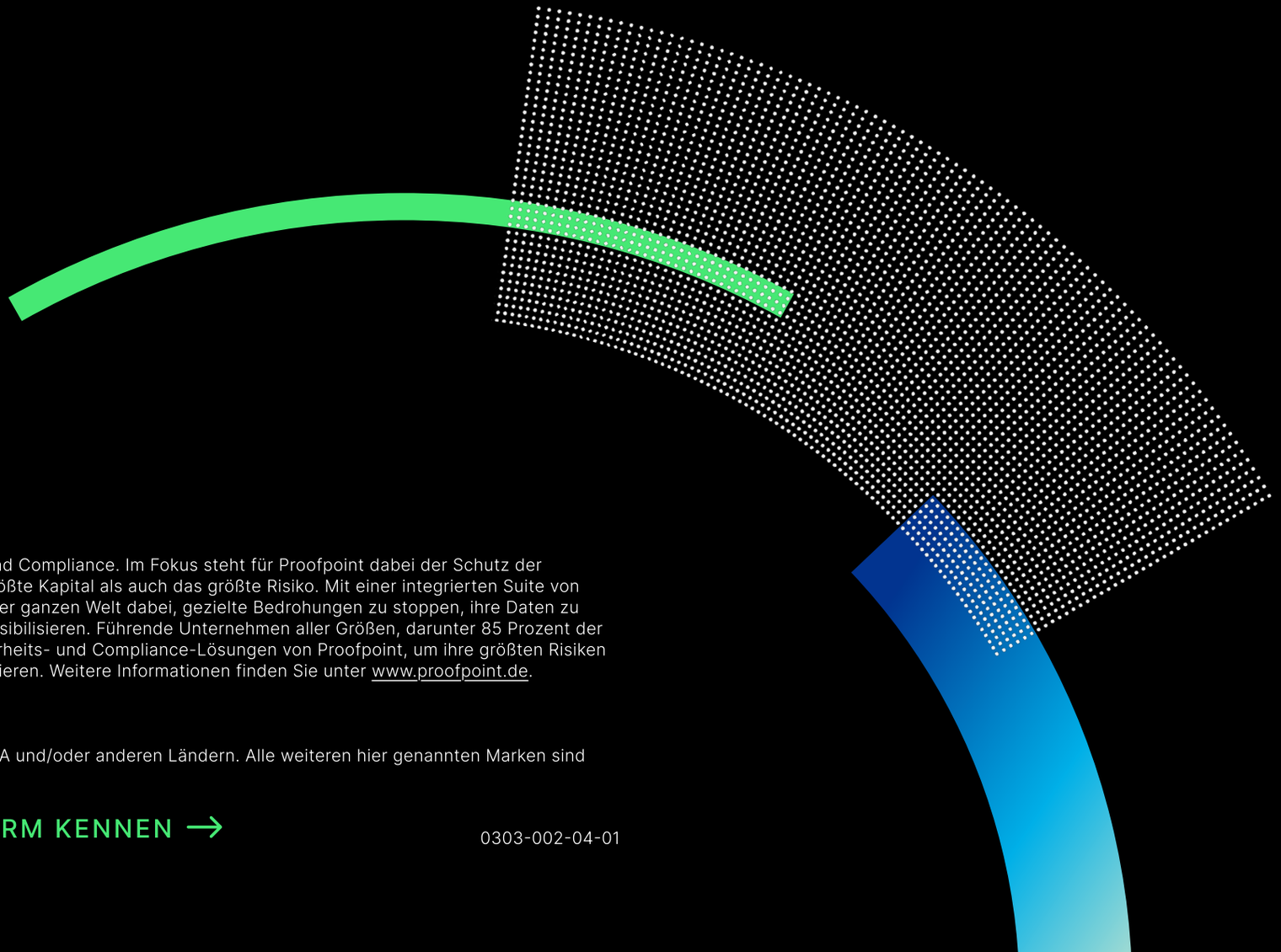
Die Art der Cyberrisiken hat sich verändert. Bedrohungen richten sich nicht nur gegen Systeme, sondern auch gegen Mitarbeiter. Leider haben sich die digitalen Arbeitsplätze schneller weiterentwickelt als die Systeme zum Schutz vor Cyberangriffen. Während Anwender nahtlos zwischen E-Mails, Browsern, Collaboration-Tools und Cloud-Anwendungen wechseln, kann das alte, auf statischen Perimetern und Einheitskontrollen basierende Sicherheitsmodell nicht mehr Schritt halten.

Die Proofpoint-Plattform bewältigt diese Herausforderung, indem sie die Sicherheitsarchitektur an der Arbeitswelt der Mitarbeiter ausrichtet. Mit Proofpoint Nexus erhalten Unternehmen einen KI-gestützten Überblick über personenzentrierte Bedrohungen, der mithilfe einzigartiger Bedrohungsdaten und Verhaltensanalysen gewonnen wird. Mit Proofpoint Zen werden die Anwender im entscheidenden Moment geschützt und unterstützt, ohne ihre Produktivität zu beeinträchtigen. Und die Proofpoint Threat Protection Workbench bietet Sicherheitsteams klarere Einblicke und einfachere Workflows, sodass sie schneller reagieren können.

Statt rein theoretischer Vorteile erhalten Sie mit unserer Plattform eine bewährte Architektur, die in Produktivumgebungen Risiken reduziert und langfristige Resilienz aufbaut. Unternehmen können ihre Workflows sofort schützen und sich auf die nächste Generation personenzentrierter Risiken vorbereiten.

Durch die Kombination von erstklassiger Erkennung, eingebetteten verhaltensbasierten Kontrollen und schnellen, integrierten Behebungsmaßnahmen können wir Ihrem Unternehmen helfen, Risiken genau an der richtigen Stelle zu reduzieren: an der Schnittstelle zwischen Mitarbeitern, Daten und Bedrohungen.

proofpoint.



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 →

0303-002-04-01