PERSONENZENTRIERTE SICHERHEIT

Der Verstärkungseffekt moderner Cybersicherheitsarchitektur

Warum personenzentrierte Sicherheit für eine moderne Schutzstrategie und die Anpassung, Verknüpfung und optimale Nutzung der bestehenden Cybersicherheitsinvestitionen unverzichtbar ist

proofpoint.

proofpoint.

Kurzfassung

CISOs haben heute die wichtige Aufgabe, kritische strategische Investitionen für die Cybersicherheitsarchitektur ihres Unternehmens anzustoßen. Zu den zentralen Säulen heutiger Schutzstrategien gehören Secure Access Service Edge (SASE), Extended Detection and Response (XDR) und Identitätsschutz. Diese Säulen funktionieren aber nicht unabhängig voneinander, sondern müssen miteinander vernetzt sein. Denn nur so können Sie sicherstellen, dass Ihr Unternehmen aktuelle Bedrohungen abwehren kann und für zukünftige Bedrohungen gerüstet ist. Und auch wenn diese Säulen die Basis bilden, decken sie nicht die größte aller Bedrohungen ab: Ihre Anwender und deren Verhalten.

Mit personenzentrierter Sicherheit schließen Sie den Kreis – vom Posteingang zum Endpunkt und von der Identität zu Insider-Bedrohungen. Denn hinter jeder Sicherheitsverletzung steht menschliches Verhalten, sei es aufgrund einer Kompromittierung, aus Fahrlässigkeit oder aus böswilligen Motiven.

Dieses Whitepaper zeigt Ihnen, warum personenzentrierte Sicherheit in einer modernen Cybersicherheitsarchitektur ein zentrales Element ist – und den entscheidenden Unterschied macht.

In diesem Whitepaper erfahren Sie:

- **Warum personenzentrierte Sicherheit eine zentrale Rolle bei der Sicherheitsarchitektur spielt** und wie sie dazu beiträgt, blinde Flecken bei bestehenden Schutzmaßnahmen zu beseitigen sowie personenbezogene Risiken an digitalen Arbeitsplätzen zu erkennen.
- **Welche Vorteile die Proofpoint Human-Centric Security-Plattform bietet.** Das Whitepaper beschreibt, wie Proofpoint als strategische Kontrollebene agiert, die Effektivität Ihrer vorhandenen Sicherheitsinvestitionen steigert und Ihr Unternehmen vor personenbezogenen Bedrohungen schützt.

Jenseits von Perimeter und Einzelprodukten

Viele CISOs versuchen weiterhin, moderne Bedrohungen mit veralteten Modellen abzuwehren, d. h. mit isolierten Kontrollen, fragmentierten Einblicken und Tools, die sich nicht schnell anpassen lassen. Doch die Angriffsfläche hat sich geändert – und unsere Gegenmaßnahmen müssen sich anpassen.

Die neue Realität ist geprägt von Angriffen, die sich gegen Menschen und nicht gegen die Technologie richten. Aufgrund der immer weiter wachsenden digitalen Arbeitsbereiche attackieren Angreifer Ihre Anwender zunehmend per E-Mail und über andere digitale Kanäle wie Messaging- und Collaboration-Tools, Social-Media-Plattformen, Cloud-Anwendungen, Large Language Models (LLMs) und File-Sharing-Dienste. Angreifer können sich auch in vertrauenswürdige Geschäftskommunikation einschleichen und die Beziehungen zu Lieferanten und Kunden massiv stören.

Gleichzeitig gilt: Daten verlieren sich nicht von selbst. Jeder Zwischenfall mit Datenverlust wird durch menschliches Verhalten verursacht. Fahrlässige Anwender gehen falsch mit vertraulichen oder kritischen Daten um, böswillige Anwender verlassen damit das Unternehmen und kompromittierte Anwender werden gehackt, damit die Angreifer an die Daten gelangen. Und in anderen Fällen halten sich Anwender nicht an die Richtlinien für den sicheren Umgang mit Daten.

Die Wahl erstklassiger Tools ist weiterhin wichtig. Doch CISOs müssen sich heute auch auf den Aufbau einer intelligenten, einheitlichen Architektur konzentrieren, die sich kontinuierlich an die Veränderungen in der Bedrohungslandschaft anpasst und sicherstellt, dass diese Tools zusammenarbeiten und bestmöglichen Schutz bieten.

Bei Proofpoint haben wir eine branchenweit einmalige Plattform geschaffen: Die Proofpoint Human-Centric Security-Plattform bietet umfassende, personenzentrierte Sicherheit mit einem Verstärkungseffekt und steigert die Wirksamkeit Ihrer Sicherheitsinvestitionen in den Bereichen E-Mail, Identität, Daten und Zugriffsrechte.

Wir schließen nicht nur Sicherheitslücken. Mit starken Integrationen mit Partnern wie CrowdStrike, Okta, Zscaler, Microsoft, Palo Alto Networks und anderen minimieren wir die Verweildauer, neutralisieren Angriffe früher und entlasten Ihr Sicherheitsteam.

Wenn Sie bislang lediglich unsere E-Mail-Schutzlösung einsetzen, stehen Sie erst am Anfang Ihrer Journey. Willkommen im Zeitalter der Plattform.

proofpoint.

Die zentralen Säulen einer modernen Cybersicherheitsarchitektur

Jeder CISO kennt die zentralen Säulen einer modernen Cybersicherheitsarchitektur: **SASE, XDR, Identität sowie SecOps und Automatisierung**. Wie unten beschrieben, ist jede dieser Säulen unverzichtbar und konzentriert sich auf einen wichtigen Risikobereich. Das Problem dabei: Keine dieser Säulen konzentriert sich auf das größte Risiko der aktuellen Sicherheitslandschaft: Ihre Anwender. **Deshalb ist personenzentrierte Sicherheit die kritischste aller Säulen**.

SecOps und Automatisierung Optimiert die Erkennung, Untersuchung und Reaktion, indem der manuelle Aufwand und isolierte Workflows beseitigt werden. Verkürzt die Reaktionszeiten und sorgt dafür, dass Überlastung durch zu viele Warnmeldungen und ineffiziente Betriebsprozesse der Vergangenheit angehören. Proofpoint automatisiert die Triage von Bedrohungen und die Richtlinienerzwingung mit integrierten Playbooks, die mit Einblicken in personenbezogene Risiken und flexiblen APIs ergänzt werden. Dadurch können Teams in Sicherheitskontrollzentren schneller und präziser agieren.

SASE

Ermöglicht den sicheren und optimierten Zugriff auf Anwendungen und Daten – unabhängig davon, wo sich der Anwender und das Gerät befinden. Behebt das Problem verteilter Belegschaften und gewährleistet Cloud-Zugriffe und die konsistente Richtlinienerzwingung für Remote-Umgebungen. Durch die Integration von Daten zu personenbezogenen Risiken kann SASE den Schutz für besonders riskante Anwender und Verhaltensweisen priorisieren.

Personenzentrierte Sicherheit

Konzentriert sich auf den Schutz der Mitarbeiter, indem sie berücksichtigt, dass Cyberkriminelle heute hauptsächlich Anwender anstelle von Infrastruktur ins Visier nehmen. Die Proofpoint Human-Centric Security-Plattform bietet Schutz vor Phishing, Datenverlust und Kontenkompromittierung mit einer Kombination aus KI-gestützter Bedrohungserkennung und Echtzeit-Hinweisen für Anwender. Um personenbezogene Risiken zu minimieren, identifizieren unsere Nexus- und Zen-Technologien auf einzigartige Weise und zuverlässig riskante Anwender, Verhaltensweisen und Vorfälle.

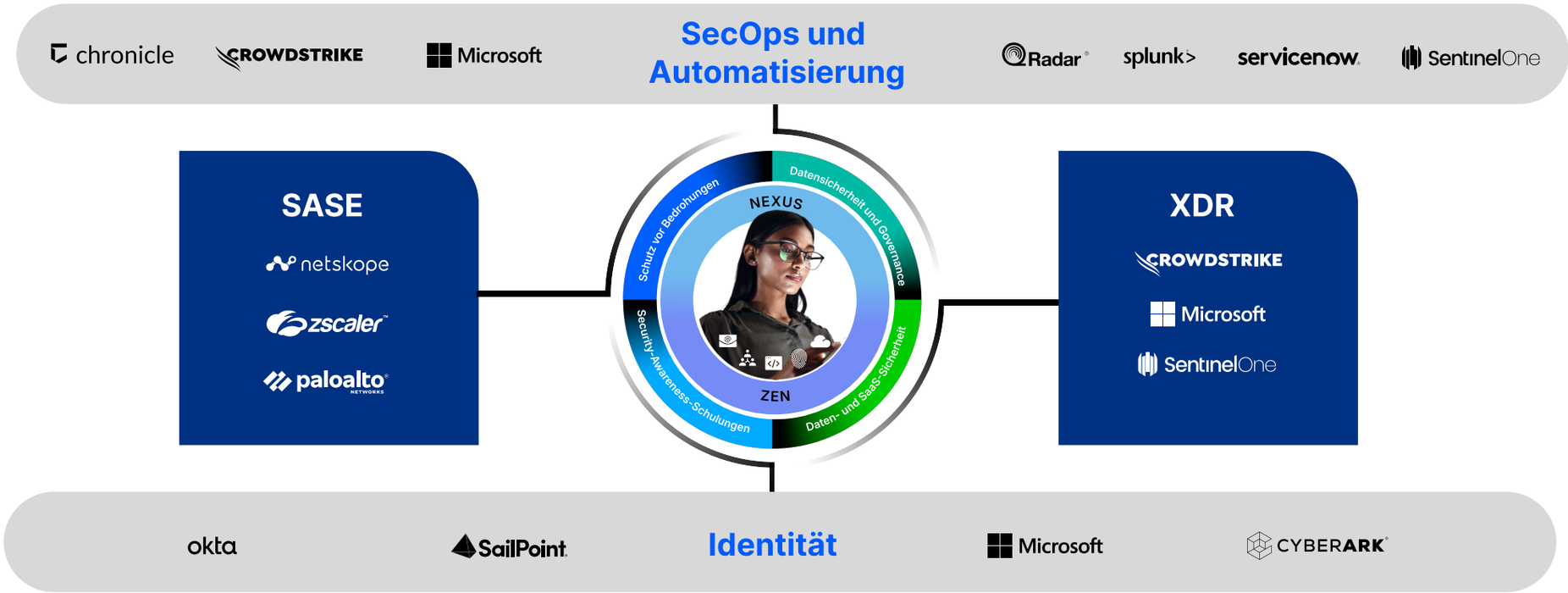
XDR

Vereinheitlicht die Telemetriedaten von E-Mails, Endpunkten, Clouds und Netzwerken und vereinfacht so die Bedrohungserkennung, Untersuchung und Reaktion. Behebt das Transparenzproblem, das durch Silos und langsame Reaktionen entsteht. Die personenzentrierten Telemetriedaten von Proofpoint, z. B. zu den angegriffenen und den riskanten Anwendern, können die XDR-Prozesse mit frühzeitigem und entscheidungsrelevantem Kontext ergänzen.

Identität Schützt Anwenderidentitäten und -zugriffe für lokale und Cloud-Umgebungen, indem Kontoübernahmen, Anmeldedaten-Missbrauch und SaaS-Konfigurationsfehler (Software-as-a-Service) erkannt werden. Behebt das Problem des Identitätswildwuchses und der nicht autorisierten Zugriffe mit kontinuierlicher Überwachung der Berechtigungen, des Login-Verhaltens und riskanter Anwendungskonfigurationen. Durch die von Proofpoint bereitgestellte Transparenz dazu, wer warum auf welche Ressourcen zugreifen kann, können Sicherheitsteams laterale Bewegungen verhindern und das Least-Privilege-Prinzip durchsetzen.

proofpoint.

Personenzentrierte Sicherheit mit Verstärkungseffekt



Die Proofpoint Human-Centric Security-Plattform agiert als strategische Kontrollebene in Ihrer Cybersicherheitsarchitektur und integriert sich mit Ihren vorhandenen Sicherheitsinvestitionen. Dadurch erhalten Sie Daten zu personenbezogenen Risiken und können die Effektivität deutlich steigern.

Unsere Plattform kombiniert Datenklassifizierung, Anwenderabsicht und Bedrohungskontext – und nutzt künstliche Intelligenz, Machine Learning und Echtzeit-Bedrohungsdaten, um Erkenntnisse zu gewinnen und automatische Richtlinienentscheidungen zu vereinfachen.

Dies sind einige der zahlreichen Möglichkeiten, mit denen die **Proofpoint Human-Centric Security-Plattform** sich mit den anderen Säulen Ihrer Architektur integriert, um vollständigen Schutz zu bieten:

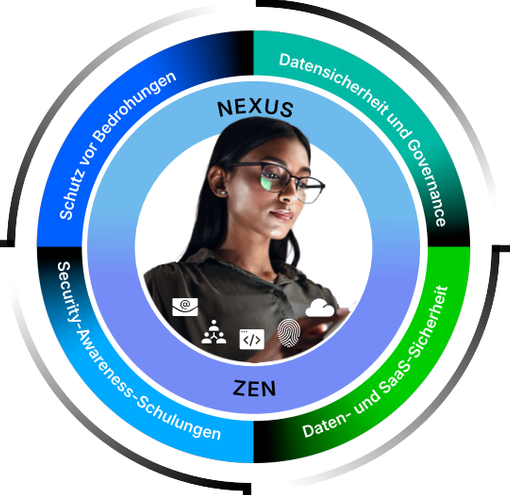
Schnellere, automatisierte Reaktionen

Proofpoint integriert sich mit Plattformen für SIEM (Sicherheitsinformations- und Ereignis-Management) und SOAR (Security Orchestration, Automation and Response), um durch personenbezogene Warnmeldungen und automatisierte Reaktionsmaßnahmen die mittlere Zeit zur Erkennung, Untersuchung und Reaktion zu verkürzen. Die Risikosignale von Proofpoint lösen automatisierte Playbooks in Cortex XSOAR oder Splunk SOAR aus, mit denen Anwender unter Quarantäne gestellt oder Anmeldedaten zurückgesetzt werden. Warnmeldungen, die mit Erkenntnissen aus Splunk und Microsoft Sentinel ergänzt werden, reduzieren die Anzahl der False Positives und beschleunigen die Triage. Proofpoint-Daten zu Bedrohungen und Anwenderverhalten werden an verbundene Systeme weitergegeben, um einheitliche Workflows zu ermöglichen.

SASE und adaptive Zugriffskontrolle

Bei Partnern wie Zscaler und Palo Alto Networks integriert Proofpoint Erkenntnisse zu Bedrohungen und Verhalten, damit Zugriffsrichtlinien in Echtzeit dynamisch angewendet werden können. Das bedeutet, dass gefährdete Anwender eine erweiterte Authentifizierung durchlaufen müssen oder der Zugriff durch Zscaler oder Palo Alto Prisma Access blockiert wird. Böswillige Aktivitäten lösen eine sofortige Richtlinienerzwingung aus.

Das ist Secure Access Service Edge (SASE) auf Basis von personenbezogenen Faktoren und nicht nur Paketen.



XDR beginnt dort, wo Angriffe starten

Phishing ist weiterhin der häufigste Ausgangspunkt. Wir schließen den Kreis mit CrowdStrike, Microsoft Sentinel und SentinelOne. Eine gekennzeichnete E-Mail löst in CrowdStrike oder SentinelOne innerhalb von Sekunden statt Stunden eine Isolierung des Endpunktgeräts aus. Der Anwenderrisikowert und der konkrete Bedrohungskontext aus Proofpoint ergänzen Warnmeldungen in Microsoft Sentinel.

Mit Proofpoint erhalten Sie Transparenz über den ersten Kontakt, sodass Ihr XDR-System über den Start eines Angriffs informiert ist.

Identität und Schutz für privilegierte Zugriffe

Wir tauschen Daten zum Risikokontext mit Okta, CyberArk und SailPoint aus, um dynamische Zugriffskontrollen zu ermöglichen. Dazu identifizieren wir Ihre am stärksten gefährdeten Anwender und geben diese Erkenntnisse an unsere Partner weiter. Bei verdächtigem Verhalten wird Multifaktor-Authentifizierung erzwungen, bei hochriskanten Anwendern werden adaptive Kontrollen und Richtlinien angewendet und bei Erkennung eines kompromittierten Kontos wird der Zugriff widerrufen. Kurz: Durch die Integration ermöglichen wir die Durchsetzung adaptiver, identitätsbezogener Zero-Trust-Kontrollen.

proofpoint.

Ihre nächsten Aktionen sind strategischer, nicht taktischer Natur

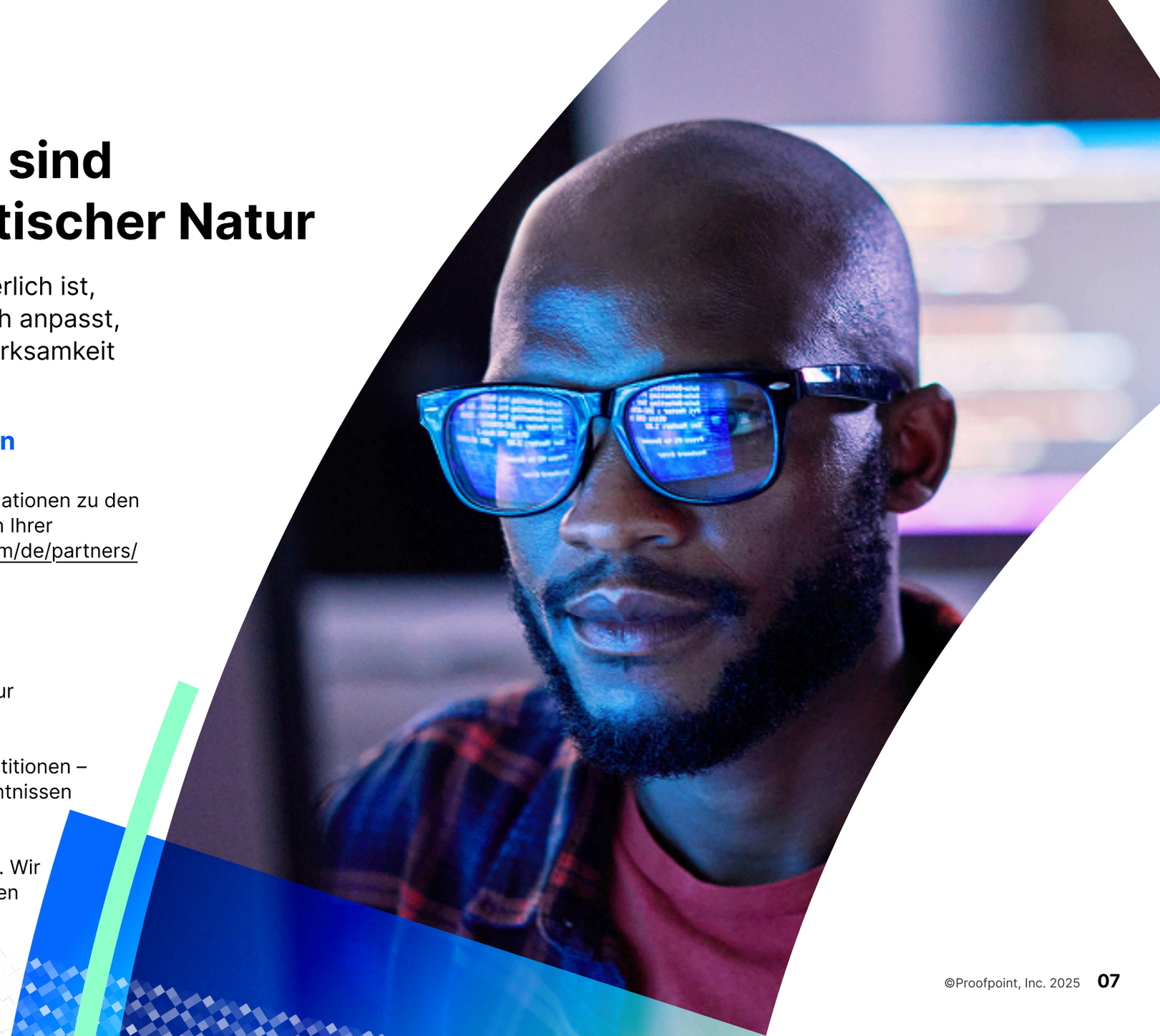
Die Frage lautet nicht, welches Tool jetzt erforderlich ist, sondern wie Sie eine Plattform aufbauen, die sich anpasst, sich mit anderen Systemen verbindet und die Wirksamkeit aller bereits vorhandenen Technologien steigert.

Weitere Informationen zu unseren Integrationen

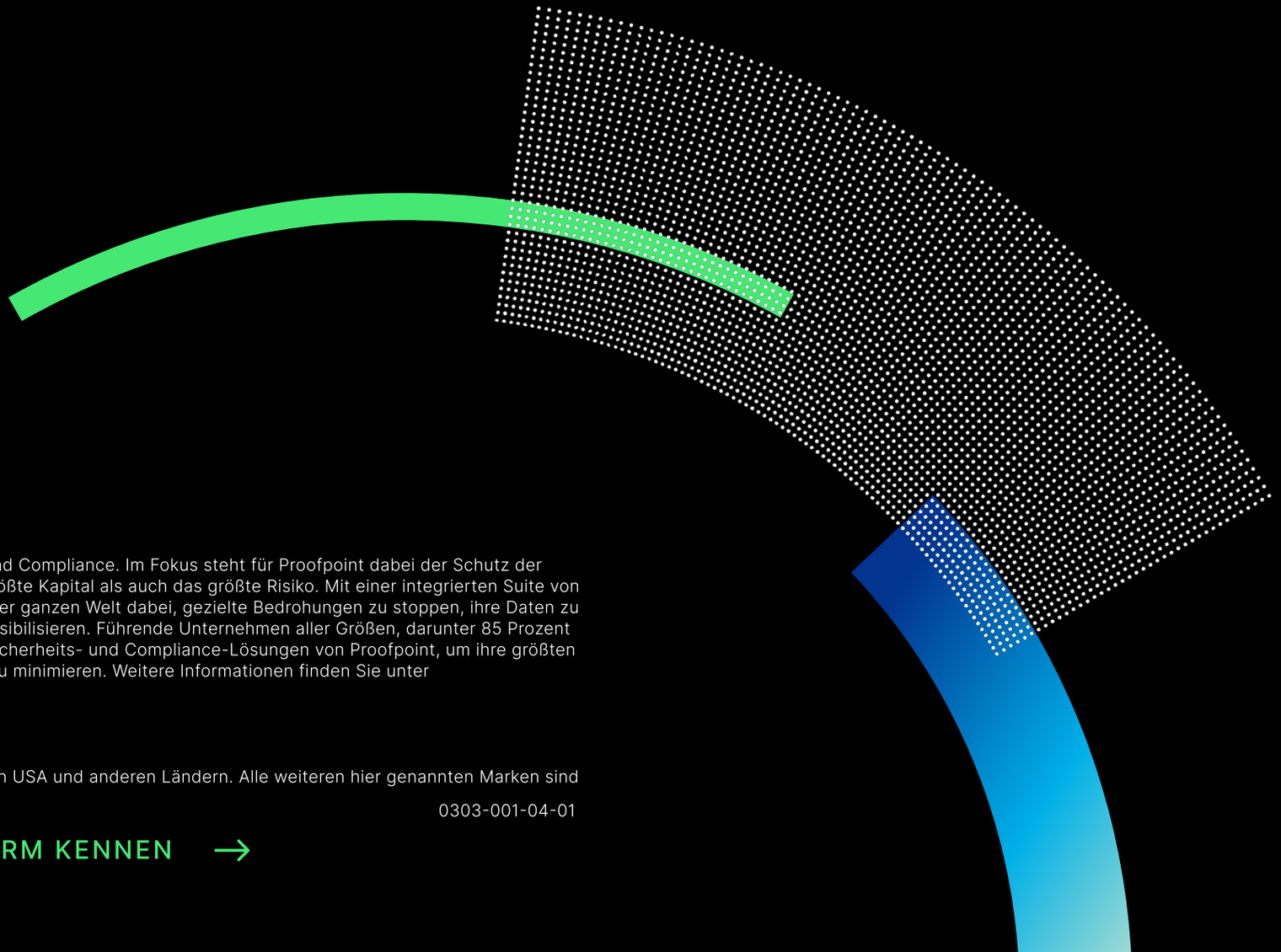
Auf unserer Website finden Sie weitere praxisrelevante Informationen zu den Integrationen zwischen Proofpoint und anderen Komponenten Ihrer Cybersicherheitsarchitektur. Besuchen Sie uns: proofpoint.com/de/partners/technology-alliance-partners.

Kontaktieren Sie Proofpoint

- **Analysieren** Sie, wie gut Ihre aktuelle Sicherheitsarchitektur personenzentrierte Bedrohungen abwehren kann.
- **Erfahren** Sie, wie die Wirksamkeit Ihrer vorhandenen Investitionen – XDR, SASE und Identität – mit unseren einheitlichen Erkenntnissen zu personenbezogenen Risiken gestärkt werden kann.
- **Erleben** Sie unsere plattformgestützte Sicherheit in Aktion. Wir zeigen Ihnen, wie Sie mit personenzentrierten Erkenntnissen hervorragende Sicherheit erzielen.



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

0303-001-04-01

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →