proofpoint.

KURZVORSTELLUNG

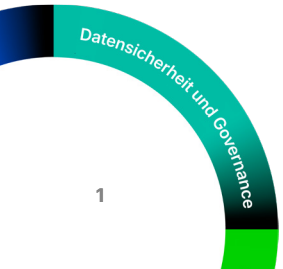
Proofpoint Insider Threat Management

Schützen Sie Ihr Unternehmen vor riskanten Insidern

Wichtige Vorteile

- Schutz vor finanziellen Schäden und Markenschäden, die durch fahrlässig handelnde, schädliche und kompromittierte Insider verursacht werden
- Proaktive Erkennung von riskantem Verhalten durch einen umfassenden und detaillierten Überblick über Verhaltensindikatoren
- Schnellere Untersuchungen mit unwiderlegbaren Beweisen
- Effektive Zusammenarbeit mit Personal- und Rechtsabteilung sowie weiteren Beteiligten
- Schutz der Privatsphäre Ihrer Anwender und Gewährleistung der Objektivität bei Untersuchungen
- Schnelle Rendite durch einfache Bereitstellung und einen ressourcenschonenden Endpunkt-Agenten

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.



Die verteilte Belegschaft arbeitet heute ortsunabhängig. Mitarbeiter, Auftragnehmer und Vertragspartner haben Zugriff auf mehr Daten als je zuvor – und diese können sich auf Geräten, in E-Mails und in der Cloud befinden. Geschäftliche Veränderungen wie Fusionen und Übernahmen, Firmenauflösungen und Umstrukturierungen führen zu Unsicherheit und können Insider-Bedrohungen auslösen. Gleichzeitig fördern geopolitische und wirtschaftliche Spannungen Cyberspionage durch Insider.

Diese Dynamik erhöht das Risiko von Insider-Bedrohungen, die zu Diebstahl von Geschäftsgeheimnissen und geistigem Eigentum, Betrug, Spionage und Systemsabotage sowie zu erheblichen finanziellen, reputationsbezogenen und strategischen Schäden für Unternehmen führen können. Um Insider-Risiken wirksam reduzieren zu können, benötigen Sicherheitsteams kontextbezogene Einblicke in riskantes Verhalten.

Proofpoint Insider Threat Management (ITM) bietet umfassende Transparenz zu fahrlässig handelnden, böswilligen und kompromittierten Insidern und hilft Sicherheitsteams bei der Erkennung von riskantem Verhalten sowie bei der effizienten Untersuchung von Insider-bezogenen Vorfällen. Mit dem personenzentrierten Ansatz von Proofpoint ITM erhalten Sie detaillierte Einblicke in das Verhalten und die Absichten der Anwender. Außerdem können Sie von einer zentralen Konsole aus Richtlinien einrichten, Warnmeldungen triagieren, nach Bedrohungen suchen und auf Vorfälle reagieren. Und mithilfe von Forensik-Beweisen können Sie Fehlverhalten von Insidern schnell und effizient untersuchen.

Je schneller ein Zwischenfall behoben ist, desto weniger kann er Ihrem Geschäft, Ihrer Marke und Ihrem Gewinn schaden.

Proaktive Reduzierung des Sicherheitsrisikos

Umfassender Überblick über personenbezogene Risiken

Bedrohungen durch Insider sind ein allgegenwärtiges und jederzeit mögliches Risiko. Dies macht sie für CISOs auf der ganzen Welt zu einem der größten Cybersicherheitsprobleme. Mit Proofpoint Human Risk Explorer (HRE) und Proofpoint ITM erhalten Sie korrelierte Bewertungen zu Risikosignalen, sodass Sie neue Risiken proaktiv erkennen und beheben können. Proofpoint HRE analysiert mehrere Dimensionen an einem Ort und bietet ein umfassendes Verständnis der personenbezogenen Risiken, darunter Schwachstellen und Verhaltensweisen einzelner Mitarbeiter, die Anfälligkeit für Angriffe, der Umgang mit vertraulichen Daten, das Sicherheitsbewusstsein und die Identität.

Proofpoint HRE nutzt zudem datengestützte Erkenntnisse für Empfehlungen. Wenn ein Anwender riskantes Verhalten zeigt (z. B. eine große Mengen vertraulicher Informationen herunterlädt), können Sie sofort Maßnahmen ergreifen, d. h. strengere Sicherheitskontrollen durchsetzen, gezielte Schulungen zuweisen, die Überwachung verstärken usw. Indem Sie sich zuerst auf besonders riskante Anwender konzentrieren, können Sie die Wahrscheinlichkeit von Vorfällen erheblich reduzieren und Ihre allgemeine Risikolage verbessern.

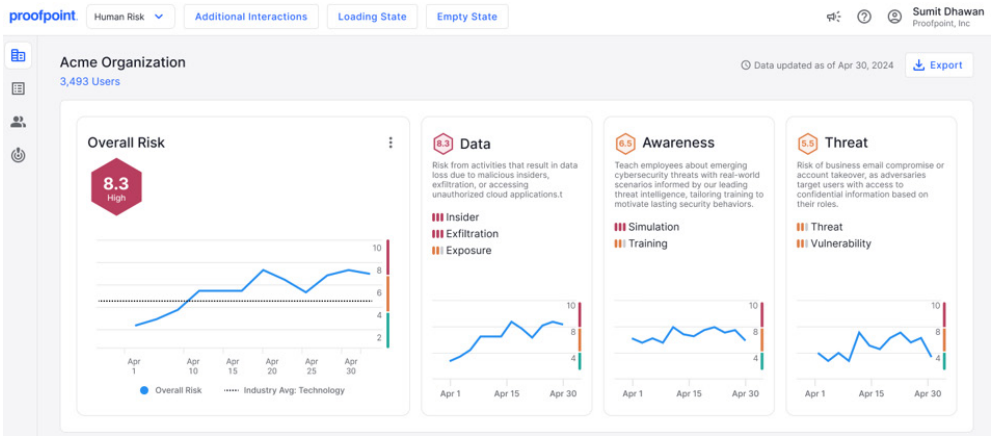


Abb. 1: Mit Human Risk Explorer können Sie das Gesamtrisiko für Ihr Unternehmen leicht verstehen und sehen, wie es im Vergleich zur Branche abschneidet. Wenn Sie weitere Details anzeigen, erhalten Sie Einblicke in Risiken durch Insider, Datenexfiltrationen und Datengefährdungen.

Adaptiver, risikobasierter Ansatz

Um das Insider-Risiko zu reduzieren, identifizieren die meisten Unternehmen Anwendergruppen mit gemeinsamen Risiken, z. B. Einzelpersonen oder Teams, deren Rollen, Verhaltensweisen oder Umstände das Risiko für die Integrität von Systemen und Daten erhöhen können. Zu den üblichen Risikogruppen zählen Mitarbeiter, die das Unternehmen verlassen, neue Mitarbeiter, Anwender mit privilegierten Zugriffen, Führungskräfte, Auftragnehmer, Top Clicker usw.

Was ist aber mit Anwendern, die nicht als riskant bekannt sind? Die meisten Unternehmen müssen und sollten nicht ständig die Telemetriedaten aller Aktivitäten auf den Endpunkten aller Anwender erfassen. Als Alternative dazu bietet Proofpoint einen adaptiven, risikobasierten Ansatz. Dabei nutzen Unternehmen nicht statische, manuelle Richtlinien, sondern solche, die sich basierend auf dem Anwenderverhalten automatisch in Echtzeit anpassen.

Bei einem adaptiven Ansatz passen dynamische Richtlinien die Anwender-überwachung basierend auf dem Verhalten und nicht auf vorgegebenen Risikomerkmalen an. Wenn zum Beispiel ein Anwender, der keiner Risikogruppe angehört, vertrauliche Daten auf ein USB-Laufwerk kopiert, generiert Proofpoint ITM eine Warnung und löst eine verstärkte Überwachungsrichtlinie aus, die für einen festgelegten Zeitraum detaillierte Metadaten und Screenshots erfasst. Dadurch erfolgt eine Überwachung nur bei Bedarf.

Dies gewährleistet den Schutz der Privatsphäre und vereinfacht Benachrichtigungen für Sicherheits-analysten. Mit einem adaptiven, risikobasierten Ansatz sparen Sie Zeit und verbessern die Erkennungsgenauigkeit.

Äußerst stabiler und flexibler Endpunkt-Agent

Für diesen adaptiven, risikobasierten Ansatz verwendet Proofpoint einen einzigen, ressourcenschonenden Endpunkt-Agenten, der vor Datenverlust schützt und detaillierte Einblicke zum Anwenderverhalten bietet. Sie können den Umfang und die Art der erfassten Daten für jeden Anwender und jede Anwendergruppe anpassen. Auf diese Weise können Sie Bedrohungen frühzeitig erkennen, Warnmeldungen effizient untersuchen und schnell darauf reagieren. Gleichzeitig sparen Sie Verarbeitungs- und Speicherkosten. Der Benutzermodus-Agent von Proofpoint verursacht keine Konflikte mit anderen Lösungen und belastet nicht das System, sodass Stabilität, Anwenderproduktivität und Leistung gewährleistet werden.

Echtzeit-Einblicke zu riskantem Verhalten

Detaillierter Überblick über riskante Anwender

Proofpoint bietet einen detaillierten Überblick über die Datenaktivitäten auf Endpunkten, um die Erkennung von riskantem Verhalten zu vereinfachen,

z. B. von Versuchen, vertrauliche Daten auf nicht autorisierte Websites hochzuladen oder in Cloud-Synchronisierungsordner zu kopieren, den Dateityp zu manipulieren (z. B. Dateierweiterungen ändern) oder Dateien mit vertraulichen Daten umzubenennen. Solche Aktivitäten könnten darauf hinweisen, dass Anwender ihre Spuren verwischen. In Verbindung mit zusätzlichem Kontext (z. B. wenn ein Mitarbeiter gekündigt hat und zur Konkurrenz wechselt), können diese Aktivitäten auf einen Hochrisikoanwender hinweisen, der einer weiteren Untersuchung bedarf.

Mit Proofpoint erhalten Sie außerdem einen Überblick über die Anwendungsnutzung und das Surfverhalten im Web. Zu riskanten Verhaltenssignalen zählen die Installation und Ausführung nicht autorisierter Tools, die Durchführung typischer Aktivitäten von Sicherheitsadministratoren, die Manipulation von Sicherheitskontrollen oder der Download schädlicher Software. Die detaillierten Einblicke von Proofpoint helfen bei der Beantwortung der Fragen nach dem Wer, Was, Wo und Wann zu riskanten Aktivitäten. Dank des Kontexts und der Einblicke können Sie bei ungewöhnlichem Verhalten die Absicht des jeweiligen Anwenders besser erkennen.

Inhaltsüberprüfung und Datenklassifizierung

Vertrauliche Daten sind besonders gefährdet, wenn sie freigegeben oder übertragen werden. Proofpoint scannt übertragene Daten und interpretiert Klassifizierungen (z. B. von Microsoft Information Protection, MIP), um sicherzustellen, dass die richtigen Richtlinien angewendet werden.

Mithilfe Ihrer vorhandenen Investitionen in Datenklassifizierung können Sie vertrauliche Geschäftsdaten wie geistiges Eigentum erkennen, ohne dafür einen separaten Workflow für Sicherheitsteams und Endnutzer erstellen zu müssen. In Fällen, in denen die Datenklassifizierung nicht zur Erkennung regulierter Daten und Kundendaten herangezogen werden kann, können Sie die erstklassigen Detektoren von Proofpoint nutzen, darunter Detektoren für den exakten Datenabgleich bei strukturierten Daten (Exact Data Matching, EDM) und für den Abgleich indexierter Dokumente (Indexed Document Matching, IDM) bei unstrukturierten Inhalten wie geistigem Eigentum. Diese erweiterten Methoden verbessern die Erkennungsgenauigkeit und schützen Ihre wichtigsten Informationen.

DATENAKTIVITÄTEN	**VERHALTENSAKTIVITÄTEN**
Warnmeldungen zu Dateninteraktionen und Exfiltrationen, z. B.: • Datei-Upload ins Web • Datei-Kopie auf USB-Gerät • Datei-Kopie in lokalen Cloud-Synchronisierungsordner • Drucken einer Datei • Kopieren/Einfügen von Datei/Ordner/Text • Dateiaktivitäten (Umbenennen, Kopieren, Verschieben oder Löschen) • Dateiverfolgung (Web zu USB-Gerät, Web zu Web usw.) • Datei-Download aus dem Web • Datei-Versand als E-Mail-Anhang • Datei-Download aus E-Mail/von Endpunkt	Verhaltensbezogene Warnungen, z. B.: • Verbergen von Informationen • Nicht autorisierter Zugriff • Umgehung der Sicherheitskontrollen • Leichtfertiges Verhalten • Erstellen eines Backdoor-Trojaners • Urheberrechtsverletzung • Nicht autorisierte Kommunikationstools • Nicht autorisierte Administrationsaufgaben • Nicht autorisierte Aktivitäten von Datenbankadministratoren • Vorbereitung eines Angriffs • IT-Sabotage • Erweiterung von Berechtigungen • Identitätsdiebstahl • Verdächtige GIT-Aktivitäten • Nicht akzeptable Nutzung

Flexibles Regelmodul und Bibliothek mit Warnmeldungen

Mit Proofpoint ITM können Sie neue Regeln und Auslöser erstellen, die auf Ihre Umgebung zugeschnitten sind, oder unsere vorkonfigurierten Bedrohungsszenarien anpassen. Sie können diese Szenarien nach Anwendergruppen, Anwendungen sowie Datum und Uhrzeit ändern oder basierend auf Vertraulichkeit der Daten, Klassifizierungsbezeichnungen, Quellen und Zielen, Übertragungskanälen und Typen anpassen.

Um die Einrichtung zu vereinfachen und den Bereitstellungsaufwand zu reduzieren, umfasst Proofpoint ITM auch sofort einsatzbereite Bibliotheken mit Warnmeldungen bei riskanten Datenbewegungen oder Interaktionen auf Endpunkten. Zusätzlich generiert Proofpoint Warnmeldungen zu verschiedensten riskanten Verhaltensweisen von Insidern. Die Bibliothek zu Insider-Bedrohungen umfasst über 150 Regeln, die auf den Richtlinien des CERT-Instituts und verhaltensbasierter Forschung basieren und die schnelle und einfache Erkennung von riskantem Verhalten ermöglichen.

Verhinderung nicht autorisierter Datenexfiltrationen über Endpunkte

Es reicht nicht immer, riskante Anwender- und Datenaktivitäten zu erkennen – sie müssen auch in Echtzeit blockiert werden.

Mit unserer Lösung können Sie Anwender stoppen, die mit vertraulichen Daten nicht richtlinienkonform interagieren, z. B. indem sie Daten von und zu USB-Geräten übertragen, Dateien mit Cloud-Ordnern synchronisieren, Dateien ins Internet hochladen, Dateien kopieren und einfügen, drucken oder auf mobile Geräte, SD-Karten, Netzwerkfreigaben usw. kopieren. Sie können auch verhindern, dass Anwender vertrauliche Daten über Websites mit generativer KI (GenAI) weitergeben.

Dabei können Sie Ihren Schutz auf der Basis folgender Parameter anpassen: Anwender, Anwendergruppen, Endpunktgruppen, Prozessnamen, USB-Geräte, USB-Seriennummern, USB-Anbieter, Datenklassifizierungen, Ursprungs-URL und Übereinstimmungen bei Inhaltsüberprüfungen.

Vereinfachung und Beschleunigung von Untersuchungen

Zentrale Konsole

Proofpoint hilft Ihnen, Untersuchungen und Reaktionen bei Insider-bezogenen Ereignissen zu vereinfachen. Sie können Telemetriedaten von Endpunkten, E-Mail und Cloud erfassen, sodass Sie einen zentralen Überblick für alle Kanäle erhalten.

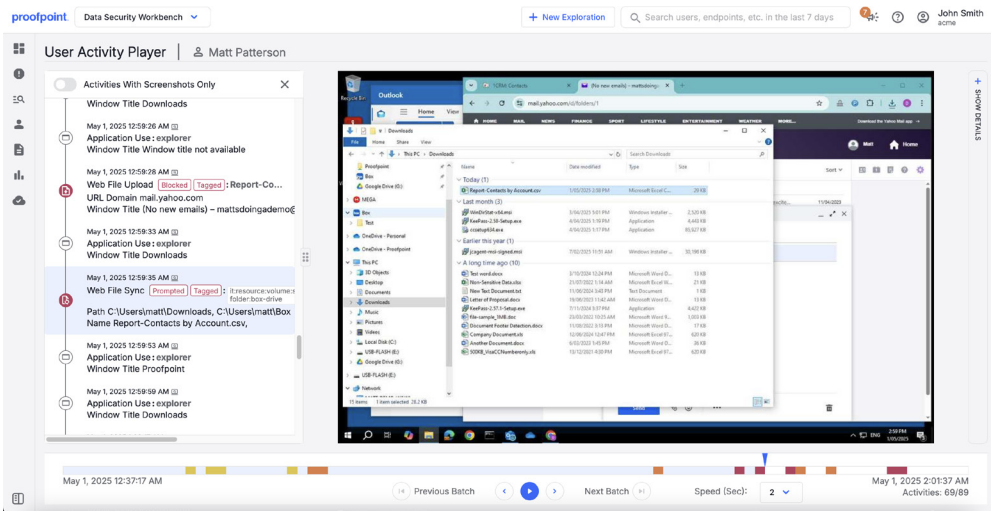


Abb. 2: In der Data Security Workbench sehen Sie in einer Zeitleiste, was vor, während und nach einem Insider-bezogenen Vorfall passiert ist. Für zusätzlichen Kontext und Forensik-Beweise können Sie ganz einfach Screenshots anzeigen.

Die zentrale Konsole, die als Data Security Workbench bezeichnet wird, liefert eine intuitive Visualisierung, damit Sie Aktivitäten überwachen, Warnmeldungen korrelieren, Untersuchungen verwalten, nach Bedrohungen suchen und die Reaktion auf Zwischenfälle koordinieren können. Dank der zentralen Übersicht können Sie außerdem Ihre Betriebskosten senken.

Die leistungsfähigen Such- und Filterfunktionen von Proofpoint unterstützen Sie mit individuellen Datenanalysen proaktiv bei der Bedrohungssuche. Sie können nach riskanten Verhaltensweisen und Aktivitäten suchen, die für Ihr Unternehmen relevant sind, oder auf neue Risiken reagieren. Und mit der KI-gestützten Suche, die Prompts in natürlicher Sprache unterstützt, können Sie Untersuchungen beschleunigen. Ähnlich wie unsere Erkennungsfunktionen können Sie auch eine der mitgelieferten Vorlagen zur Bedrohungssuche anpassen oder Ihre eigene Vorlage erstellen.

Triage-Prüfung von Warnmeldungen

Die Untersuchung und Behebung von Sicherheitswarnungen, die durch Insider ausgelöst werden, ist nicht immer einfach und kann ein langwieriger und kostenintensiver Prozess sein. Zudem sind oft weitere nicht-technische Abteilungen daran beteiligt, z. B. Personal-, Rechts- und Compliance-Abteilungen sowie Geschäftsbereichsleiter.

Bei Proofpoint können Sie zu jeder Warnmeldung Details aufrufen, einschließlich Metadaten und Kontext mit Zeitleistenansichten. Sicherheitsteams können so entscheiden, welche Ereignisse näher untersucht werden müssen und welche gleich wieder geschlossen werden können. Kontextbezogene Erkenntnisse aus der Zeit vor, während und nach einem Insider-Ereignis liefern einen Überblick über die Absichten und dazu, ob der jeweilige Anwender fahrlässig oder böswillig gehandelt hat bzw. kompromittiert wurde. Dies ist für die Entscheidung über die nächsten Schritte von entscheidender Bedeutung.

Funktionen für Workflows und Informationsaustausch erleichtern die funktionsübergreifende Zusammenarbeit. Die Aufzeichnungen über riskante Aktivitäten lassen sich für mehrere Ereignisse in übliche Dateiformate (z. B. PDF) exportieren.

Diese Exporte enthalten Beweise in Form von Screenshots sowie damit verbundenen Kontext. Das erleichtert es nicht-technischen Teams wie der Personal- oder Rechtsabteilung, die Daten forensisch zu untersuchen und fundierte Entscheidungen zu treffen.

Bildschirm-Screenshots für forensische Beweise

Ein Bild kann tausend Worte wert sein. Mit Proofpoint können Sie Screenshots der Anwenderaktivitäten erfassen, um so mit einem klaren und unwiderlegbaren Beweis für schädliches oder fahrlässiges Verhalten zur Entscheidungsfindung bei Personal- und Rechtsabteilungen sowie Managern beizutragen.

Unternehmen mit einer komplexen Sicherheitsinfrastruktur müssen möglicherweise eine zentrale Informationsquelle für alle Systeme pflegen, z. B. Screenshots, Snippets oder Dateien zu Untersuchungszwecken im eigenen Speicher aufbewahren. Proofpoint vereinfacht diesen Schritt mit automatischen Datenexporten in Ihren eigenen und von Ihnen betriebenen Speicher in AWS S3, Microsoft Azure und Google Cloud Platform.

Gleichgewicht von Privatsphäre und Sicherheitsmaßnahmen

Ein erfolgreiches Insider-Risiko-Programm sorgt für ein Gleichgewicht zwischen der Privatsphäre der Anwender und den Datenschutzschutzmaßnahmen und hält dabei die Datenschutzbestimmungen ein. Proofpoint verfolgt einen Ansatz des Datenschutzes durch Technikgestaltung, bei dem der Datenschutz in das Produktdesign einbettet wird. Auf diese Weise können Sie die Rechte Ihrer Mitarbeiter schützen, die Datenschutzgesetze einhalten und Voreingenommenheit bei Untersuchungen verhindern.

Datenspeicherort und Datenspeicherung

Proofpoint unterstützt Rechenzentren in mehreren Regionen, damit Sie die Vorschriften zu Datenschutz und Datenspeicherort einhalten können. Wir verfügen derzeit über Rechenzentren in den USA, in Kanada,

in Europa, in den Vereinigten Arabischen Emiraten, in Australien und in Japan.

Durch das Gruppieren von Endpunkten können Sie kontrollieren, wo die Daten über die jeweiligen Geräte gespeichert werden, indem Sie die Gruppe einem Rechenzentrum zuordnen. Auf diese Weise lassen sich Daten auf einfache Weise geografisch trennen.

Attributbasierte Zugriffsberechtigungen

Um Datenschutzanforderungen einhalten zu können, müssen Sie den Datenzugriff flexibel steuern können. Mit Proofpoint können Sie sicherstellen, dass Sicherheitsanalysten nur die Daten sehen, die sie benötigen, und zum Beispiel den Zugriff eines bestimmten Analysten auf konkrete Anwenderdaten beschränken oder festlegen, dass der Zugriff nur für einen bestimmten Zeitraum möglich ist.

Anonymisierung und Datenmaskierung

Durch die Anonymisierung personenbezogener Daten wird die Privatsphäre der Anwender gewährleistet und Voreingenommenheit bei Untersuchungen vermieden. Proofpoint anonymisiert die erfassten Anwenderdaten. Dabei werden weder die vollständigen Namen noch die Mitarbeiter-IDs der Anwender gespeichert, die Warnmeldungen auslösen. Stattdessen untersuchen Analysten Warnungen auf der Grundlage eindeutiger, anonymisierter Kennungen. Falls die Identität des Anwenders benötigt wird, kann der Sicherheitsanalyst die Deanonymisierung beantragen und ein Administrator kann diese gewähren.

Sie können vertrauliche Daten wie geschützte Gesundheitsdaten und personenbezogene Daten auch per Datenmaskierung schützen. So gewährleisten Sie, dass die personenbezogene Zuordnung in der Benutzeroberfläche nicht möglich ist und nur Personen, die Zugriff auf die Daten benötigen, diese vollständig einsehen können.

Geschäftliche Flexibilität durch eine moderne Architektur

Schnelle und einfache Skalierung

Proofpoint ist eine Cloud-native Lösung, die sich problemlos skalieren lässt und an Ihre sich ändernden Geschäftsanforderungen anpasst. Die Lösung kann pro Mandant hunderttausende Anwender unterstützen und punktet mit schneller Bereitstellung und einfacher Wartung. Dies gewährleistet eine schnelle Rendite. Durch einen API-orientierten Ansatz lässt sich die Proofpoint-Lösung problemlos in Ihr bestehendes Ökosystem integrieren. Zudem vereinfachen Webhooks die Weitergabe von Warnmeldungen an SIEM-Tools (Sicherheitsinformations- und Ereignis-Management) und SOAR-Systeme (Security Orchestration, Automation and Response) und unterstützen so die Identifizierung und Triage von Zwischenfällen.

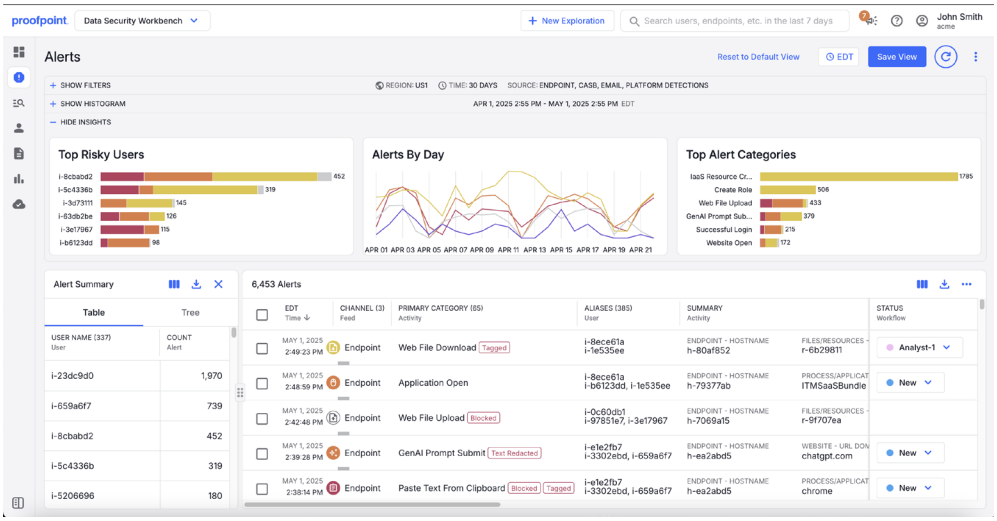


Abb. 3: Die Anonymisierung schützt die Identität der Anwender und trägt dazu bei, die Privatsphäre zu schützen und bei Untersuchungen Objektivität zu gewährleisten.

Unterstützung unternehmensweiter Änderungen

Geschäftliche Veränderungen können zu Unsicherheit führen und so ein ideales Umfeld für Insider-Bedrohungen schaffen. Durch Fusionen und Übernahmen, drohende Entlassungen oder neue Technologien wie generative KI können Insider-Risiken zu einer Insider-Bedrohung werden. Insider-Risiko-Teams benötigen Transparenz und Kontrollen, um Änderungen unterstützen zu können. Proofpoint ermöglicht dies mit einem adaptiven, risikobasierten Ansatz, der proaktive Erkennung und Prävention bietet.

Aufbau und Weiterentwicklung Ihres Programms

Ein wirksames Insider-Risiko-Programm deckt Personen, Prozesse und Technologie ab. Proofpoint kann Sie als vertrauenswürdiger Partner auf Ihrem Weg begleiten, um Ihr Programm zum Erfolg zu führen. Mit unseren Premium-Services stehen Ihnen die Kompetenzen zur Verfügung, die Sie benötigen, um Ihr Programm zu optimieren, Ihre Investitionen optimal zu nutzen und die Zustimmung und Unterstützung Ihrer Verantwortlichen sicherzustellen. Unsere Advisory-Services bieten strategische Beratung und kontinuierliche Services beim Aufbau und bei der Verbesserung Ihres Programms. Und unsere Applied-Services helfen Ihnen, Ihre Technologieinvestitionen zu optimieren, Ihren laufenden Betrieb zu unterstützen und Ihr Insider-Risiko-Programm weiterzuentwickeln.

proofpoint.

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →