Proofpoint Endpoint DLP und Proofpoint ITM

Personenzentrierter Schutz vor Datenverlust und Insider-Bedrohungen auf Endpunkten

Produkte

- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management

Wichtige Vorteile

- Geringeres Risiko durch Datenverlust und Insider-Bedrohungen
- Einfachere Reaktion auf Insider-Zwischenfälle und Richtlinienverstöße
- Schnellere Rendite der Programme zur Abwehr von Insider-Bedrohungen und Vermeidung von Datenverlust

Die verteilte Belegschaft arbeitet heute ortsunabhängig. Mitarbeiter, Auftragnehmer und Vertragspartner haben Zugriff auf mehr Daten als je zuvor – und diese können sich auf Laptops, in E-Mails und in der Cloud befinden. Das Datenverlustrisiko war noch nie so hoch. Doch Daten verlieren sich nicht von selbst. Dazu bedarf es des Menschen.

Anwender, die Daten exfiltrieren, können in drei Kategorien aufgeteilt werden: fahrlässige Anwender, böswillige Anwender und kompromittierte Anwender. Bevor Sie angemessene Richtlinien implementieren können, müssen Sie zunächst den Kontext zu den Verhaltensweisen der Anwender verstehen. Auf diese Weise können Sie auch besser festlegen, wie die bestmögliche Reaktion auf einen Insider-basierten Zwischenfall aussehen sollte.

Proofpoint Endpoint Data Loss Prevention (DLP) und Proofpoint Insider Threat Management (ITM) setzen auf einen personenzentrierten Ansatz zur Verringerung des Risikos durch Datenverlust und Insider-Bedrohungen auf Endpunkten.

Die Lösungen unterstützen IT- und Cybersicherheitsteams wie folgt:

- Identifizierung riskanter Verhaltensweisen und Interaktionen mit vertraulichen Daten durch Anwender
- Erkennung und Verhinderung von Sicherheitszwischenfällen durch Insider und Datenverlust auf Endpunkten
- Schnellere Reaktion auf Zwischenfälle durch Anwender

Proofpoint Endpoint DLP schützt vor Datenverlust durch reguläre Anwender. Proofpoint ITM bietet den gleichen Schutz und zusätzlich einen umfassenden Überblick über Anwenderaktivitäten, um Bedrohungen durch Anwender mit riskantem Verhalten zu verhindern. Beide Produkte sind Teil der Proofpoint Information and Cloud Security-Plattform. Diese umfassende, kontextbezogene und Cloud-native Plattform bietet Transparenz und Einblicke zu allen Kanälen. Sie ermöglicht die Einrichtung von Richtlinien, die Triage von Warnmeldungen und beschleunigt die Reaktion auf Zwischenfälle über eine zentrale Konsole. Dadurch können Sie Datenverlust stoppen und Verstöße durch Insider schnell und effizient untersuchen. Und je schneller ein Zwischenfall behoben ist, desto weniger kann er Ihrem Unternehmen, Ihrer Marke und Ihren Finanzen schaden.

Überwachungen regulärer und riskanter Anwender

Flexibilität mit einem einzigen Endpunkt-Agenten

In der heutigen konkurrenzgeprägten Geschäftswelt müssen Sie in der Lage sein, Insider-Bedrohungen und Datenverlust auf Endpunkten zu vermeiden. Jedoch müssen und sollten die meisten Unternehmen auch nicht ständig die Telemetriedaten aller Aktivitäten auf den Endpunkten aller Anwender erfassen. Wir empfehlen daher einen adaptiven, risikobasierten Ansatz, bei dem ein Teil der Aktivitäten all Ihrer Anwender und alle Aktivitäten nur der Anwender überwacht werden, die ein erhöhtes Risiko darstellen.

Dazu hat Proofpoint einen ressourcenschonenden Endpunkt-Agenten entwickelt, der vor Datenverlust schützt und einen umfassenden Überblick über Anwenderaktivitäten bietet. Mit einer einfachen Änderung der Richtlinienkonfiguration können Sie bestimmen, wie viele und welche Daten für jeden Anwender bzw. jede Anwendergruppe erfasst werden sollen. Dieser adaptive Ansatz hilft Ihnen bei der effizienteren Untersuchung und Reaktion auf Warnmeldungen, ohne dass Sie dafür einen Berg an Daten erfassen müssen.

Bei den regulären Anwendern handelt es sich meist um typische Geschäftsanwender. Da bei ihnen nur ein geringes Risiko besteht, können Sie sie mit Proofpoint Endpoint DLP überwachen, um Einblicke in ihre Datenaktivitäten und den Kontext dieser Aktivitäten zu erhalten. In dieser Lösung lässt sich zum Beispiel mithilfe von Regeln festlegen, dass Warnmeldungen generiert werden, wenn ein Anwender durch Kopieren auf ein USB-Laufwerk oder per Upload in einen Cloud-Synchronisationsordner versucht, vertrauliche Daten zu exfiltrieren.

Mehr Aufmerksamkeit ist bei riskanten Anwendern nötig. Zu ihnen zählen zum Beispiel Mitarbeiter, die das Unternehmen verlassen oder neu eingestellt wurden, externe Auftragnehmer, Inhaber privilegierter Konten und gezielt angegriffene Anwender (z. B. leitende Führungskräfte). Sie benötigen genauere Einblicke, um deren Motive und Absichten zu verstehen. Die Überwachungen sollten vom Verhalten der Anwender und den jeweiligen Umständen abhängen. Proofpoint ITM erfasst Details zu den Aktivitäten dieser Anwender, damit Sie Kontext zu den Absichten vor, während und nach einem Ereignis erhalten.

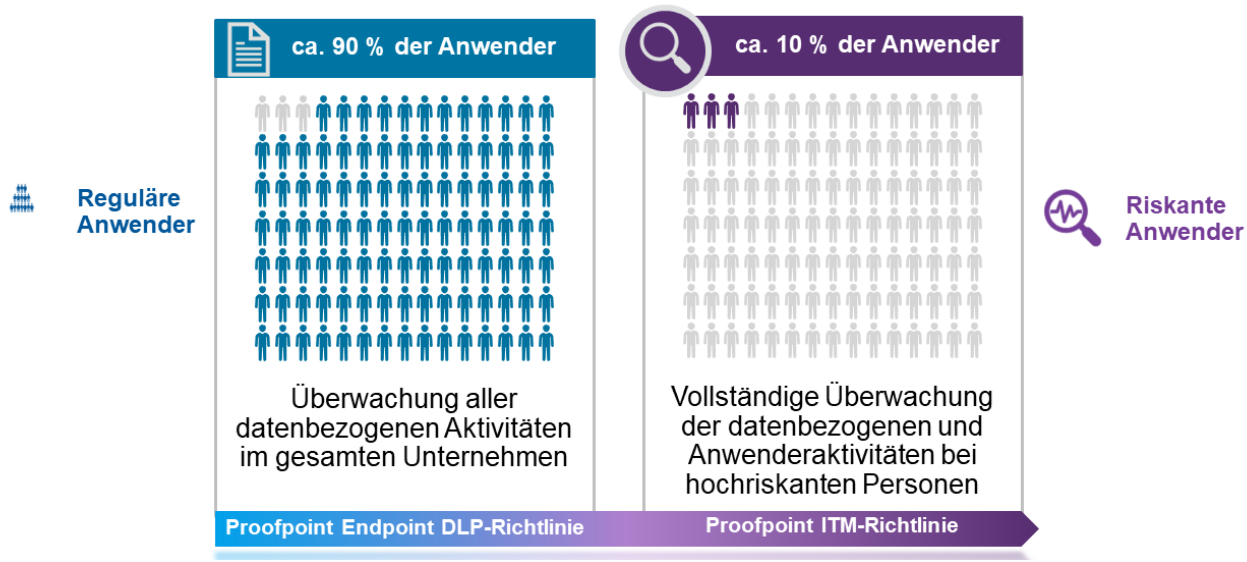

Abb. 1: Mit einem einzigen ressourcenschonenden Endpunkt-Agenten können Sie flexibel reguläre und riskante Anwender überwachen.

Die detaillierten Einblicke von Proofpoint ITM helfen bei der Beantwortung der Fragen nach dem Wer, Was, Wo und Wann zu riskanten Aktivitäten. Mit Kontextinformationen und Erkenntnissen können Sie die Absichten eines Anwenders bei Datenverlust und Richtlinienverstößen besser einschätzen.

Überwachungslisten für Ihre Anwender

Mithilfe intelligenter Überwachungslisten können Sie Anwender basierend auf deren Profil nach Risikotoleranz organisieren und priorisieren. Als Kriterien für die Organisation der Überwachungslisten können dabei die Bedeutung der Anwenderrolle und der Daten dienen, auf die sie zugreifen können, oder aber auch die Anfälligkeit der Anwender für Phishing und andere Social-Engineering-Bedrohungen. Andere mögliche Kriterien sind der Standort der Anwender, Änderungen beim Beschäftigungsverhältnis oder andere personelle bzw. rechtliche Faktoren.

Überblick und Kontext zu Anwender- und Datenaktivitäten

Transparenz zu regulären und riskanten Anwendern

Sowohl Proofpoint Endpoint DLP als auch Proofpoint ITM bieten einen Überblick darüber, wie Anwender mit Daten interagieren. Sie unterscheiden sich jedoch beim Umfang und der Art der erfassten Daten.

Proofpoint Endpoint DLP erfasst Telemetriedaten über die Interaktionen der Anwender mit Daten auf Endpunkten, z. B. wenn ein Anwender den Dateityp ändert, eine Datei mit vertraulichen Inhalten umbenennt oder versucht, vertrauliche Daten zu verschieben (z. B. auf eine nicht autorisierte Website oder in einen Cloud-Synchronisationsordner hochlädt).

Proofpoint ITM bietet einen umfassenderen Überblick über endpunktbasierte Aktivitäten, damit Sie riskante Anwender besser überwachen können. Zusätzlich zu den von Proofpoint Endpoint DLP erfassten Dateninteraktionen erhalten Sie einen Überblick über die Anwendungsnutzung, Bildschirm-Screenshots von Endpunktaktivitäten sowie Informationen zu anderen riskanten Verhaltensweisen, wie die Installation und Ausführung nicht autorisierter Tools oder die Durchführung von Aktivitäten, die normalerweise Sicherheitsadministratoren vorbehalten sind. Die detaillierten Einblicke von Proofpoint ITM helfen bei der Beantwortung der Fragen nach dem Wer, Was, Wo und Wann zu riskanten Aktivitäten. Mit Kontextinformationen und Erkenntnissen können Sie die Absichten eines Anwenders bei Datenverlust und Richtlinienverstößen besser einschätzen.

Durch den personenzentrierten Ansatz bietet Proofpoint im Vergleich zu klassischen Endpunkt-DLP-Tools einen detaillierteren Überblick über die Interaktionen Ihrer Anwender mit vertraulichen Daten. Herkömmliche Endpunkt-DLP-Tools liefern nur dann Einblick in Datenbewegungen, wenn eine Aktion eine Warnmeldung auslöst. Zudem werden die Interaktionen nicht mit Anwendern verknüpft. Scheinbar harmlose Datenaktivitäten, die sich im Kontext gesehen als Teil riskanter Verhaltensweisen herausstellen, würden Sie aufgrund dieser Schwachpunkte nicht bemerken.

Inhaltsüberprüfung und Datenklassifizierung

Vertrauliche Daten können während der Übertragung, also in der riskantesten Phase, erkannt werden. Ermöglicht wird dies durch die Prüfung übertragener Inhalte und das Auslesen von Datenklassifizierungen wie den Microsoft Information Protection-Kennzeichnungen.

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 und bewährten Inhaltsdetektoren aus Proofpoint Cloud App Security Broker (CASB) und Proofpoint Email DLP verwenden. Und mit Proofpoint Intelligent Classification and Protection (ehemals Dathena) können Sie mithilfe künstlicher Intelligenz in Echtzeit automatisch Daten erkennen und klassifizieren.

Sie können Regeln zum Scannen von Inhalten einrichten, um riskantes Verhalten zu erkennen und zu verhindern. Dabei wird eine Warnmeldung generiert, sobald die Lösung nicht richtlinienkonformes Verhalten erkennt, sodass Sie verwertbare Echtzeit-Erkenntnisse erhalten. Die Inhaltsprüfungen werden bei riskanten Anwenderaktivitäten ausgelöst, zum Beispiel bei Web-Uploads oder -Downloads, wenn Anwender Daten auf ein USB-Gerät kopieren, bei einer Synchronisierung mit einer Cloud-Freigabe und wenn ein Dokument aus einer Cloud-Freigabe geöffnet wird.

Erkennung von riskantem Anwenderverhalten und riskanten Dateninteraktionen in Echtzeit

Flexibles Regelmodul

Sie können Regeln und Auslöser erstellen und für Ihre konkrete Umgebung maßschneidern oder unsere vorkonfigurierten Bedrohungsszenarien anpassen. Die Szenarien lassen sich für folgende Parameter anpassen: Anwendergruppen, Anwendungen, Datum/Zeitraum, Vertraulichkeit der Daten, Datenklassifizierungen, Datenquellen und -ziele, Datenbewegungskanäle und Datentypen. Um Konsistenz zu gewährleisten und Aufwand zu sparen, können die für ITM eingerichteten Regeln über die zentrale Richtlinienverwaltung der Plattform auch auf andere Kanäle (z. B. E-Mail, Cloud, Web) angewendet werden.

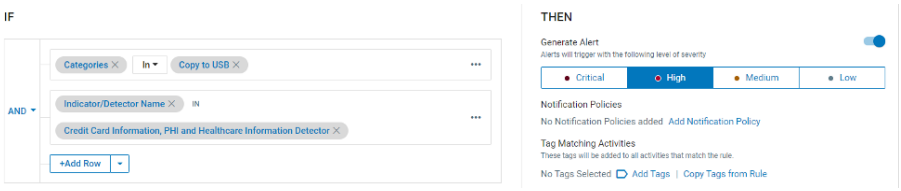

Abb. 2: Einrichtung einer Warnmeldung mit einfachen Wenn-Dann-Aussagen.

Bibliothek mit Warnmeldungen

In Proofpoint Endpoint DLP und Proofpoint ITM sind standardmäßig Bibliotheken mit Warnmeldungen integriert, die die Einrichtung erleichtern und die Amortisierungszeit verkürzen. Proofpoint Endpoint DLP und Proofpoint ITM benachrichtigen Sie bei riskanten Datenbewegungen und Interaktionen auf Endpunkten. Zusätzlich dazu generiert Proofpoint ITM Warnmeldungen zu verschiedensten riskanten Verhaltensweisen von Insidern.

Bibliothek mit Proofpoint Endpoint DLP- und Proofpoint ITM-Warnmeldungen

DATENAKTIVITÄTEN	ANWENDERAKTIVITÄTEN (NUR MIT PROOFPOINT ITM)
Warnmeldungen zu Dateninteraktionen und Exfiltrationen (mehr als 40 Warnungen): • Datei-Upload ins Web • Datei-Kopie auf USB-Gerät • Datei-Kopie in lokalen Cloud-Synchronisierungsordner • Drucken einer Datei • Dateiaktivitäten (Umbenennen, 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	Warnmeldungen zu allen Anwenderaktivitäten auf Endpunkten (mehr als 100 Warnungen): • Verbergen von Informationen • Nicht autorisierter Zugriff • Umgehung der Sicherheitskontrollen • Leichtfertiges Verhalten • Erstellen einer Backdoor • Urheberrechtsverletzung • Nicht autorisierte Kommunikations-Tools • Nicht autorisierte Administrationsaufgaben • Nicht autorisierte Aktivitäten von Datenbankadministratoren • Vorbereitung eines Angriffs • IT-Sabotage • Erweiterung von Berechtigungen • Identitätsdiebstahl • Verdächtige GIT-Aktivitäten • Nicht akzeptable Nutzung

Anwender sind sich häufig nicht bewusst, dass ihr Verhalten riskant ist. Benachrichtigungen bieten jedoch eine einfache Schulungsmethode.

Verhinderung nicht autorisierter Datenexfiltrationen über Endpunkte

Es reicht nicht immer, riskante Anwender- und Datenaktivitäten zu erkennen – sie müssen auch aktiv und in Echtzeit blockiert werden. Mit unserer Plattform können Sie Anwender davon abhalten, mit vertraulichen Daten nicht richtlinienkonform zu interagieren, zum Beispiel:

- Übertragung auf USB-Geräte und von USB-Geräten
- Synchronisierung von Dateien mit Cloud-Ordnern
- Hochladen von Dateien auf nicht autorisierte Websites
- Drucken einer Datei

Passen Sie Ihren Schutz auf der Basis folgender Parameter an: Anwender, Anwendergruppen, Endpunktgruppen, Prozessnamen, USB-Geräte, USB-Seriennummern, USB-Anbieter, Datenklassifizierungen, Ursprungs-URL und Übereinstimmungen durch Inhaltsüberprüfung. Die DLP-Funktionen können auf E-Mail-, Cloud- sowie Web-Anwendungen und den restlichen Teil unserer Information Protection and Cloud Security-Plattform erweitert werden.

Schulung von Anwendern zu riskantem Verhalten

Anwender sind sich häufig nicht bewusst, dass ihr Verhalten riskant ist. Benachrichtigungen bieten jedoch eine einfache Schulungsmethode. Wenn Anwender versuchen, vertrauliche Dateien zu verschieben, können Sie zum Beispiel auf den Verstoß gegen die Unternehmensrichtlinie hinweisen und dazu auffordern, eine Begründung für die Aktion anzugeben. Die Benachrichtigung kann zudem einen Link zur Unternehmensrichtlinie enthalten. Wenn Sie Ihre Mitarbeiter über unsichere Verhaltensweisen informieren, bleiben sie produktiv – und die Sicherheitskontrollen werden dennoch durchgesetzt. Die Benachrichtigungen können an das Risiko, die Funktion und den Standort des Anwenders angepasst werden.

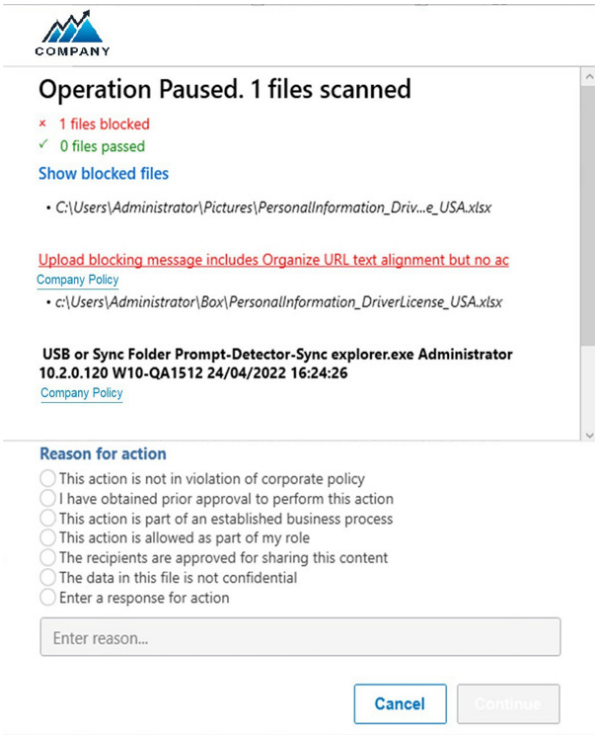

Abb. 3: Benachrichtigung der Endnutzer über riskante Verhaltensweisen und Aufforderung, eine Begründung anzugeben.

Beschleunigte Untersuchung und Behebung von Zwischenfällen

Zentrale Konsole

Da Proofpoint Endpoint DLP und Proofpoint ITM die Information Protection and Cloud Security-Plattform nutzen, werden Untersuchungen und Reaktion zu Insider-bezogenen Ereignissen vereinfacht. Die Plattform erfasst Telemetriedaten von Endpunkten, E-Mail und Cloud, sodass Sie einen zentralen Überblick für alle Kanäle erhalten. Die zentrale Konsole liefert eine intuitive Visualisierung, damit Sie Aktivitäten überwachen, Warnmeldungen korrelieren, Untersuchungen verwalten, nach Bedrohungen suchen und die Reaktion auf Zwischenfälle koordinieren können.

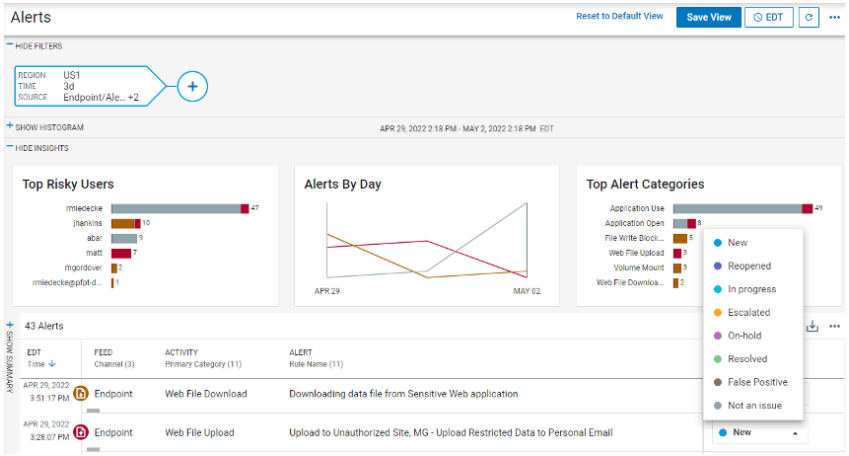

Abb. 4: Anzeige aller Ereignisse und Warnmeldung in einer zentralen Konsole.

Bedrohungssuche per Point-and-Click

Unsere leistungsfähigen Such- und Filterfunktionen unterstützen Sie mit benutzerdefinierten Datenanalysen proaktiv bei der Bedrohungssuche. Sie können nach riskanten Verhaltensweisen und Aktivitäten suchen, die für Ihr Unternehmen relevant sind, oder auf diese Weise auf neue Risiken reagieren. Ähnlich wie unsere Erkennungsfunktionen können Sie auch eine der mitgelieferten Vorlagen zur Bedrohungssuche anpassen oder Ihre eigene Vorlage erstellen.

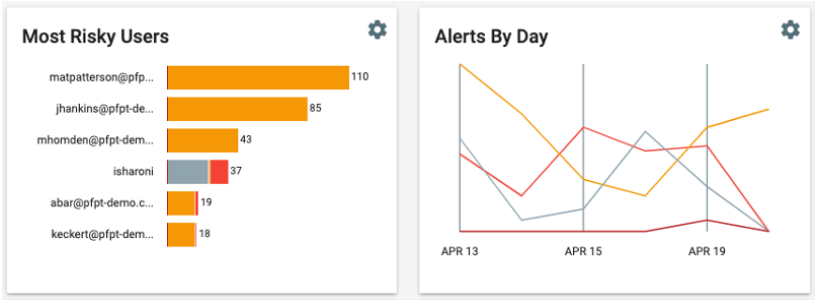

Abb. 5: Suche nach potentiell riskantem oder ungewöhnlichem Verhalten.

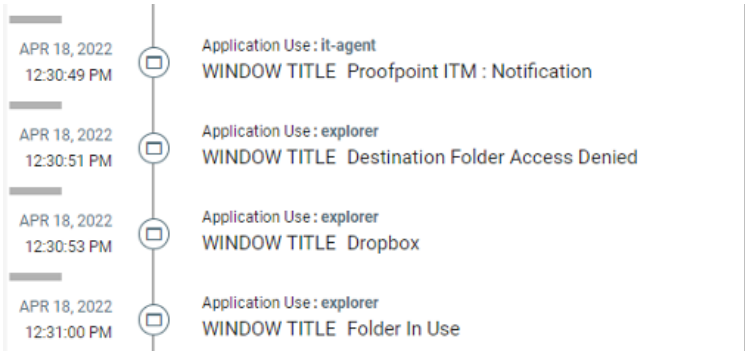

Abb. 6: Durchsuchbare Zeitleistenansicht, die den Verlauf der Anwenderinteraktion mit Daten darstellt.

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 nicht-technische Abteilungen daran beteiligt, z. B. Personal-, Rechts- und Compliance-Abteilungen sowie Geschäftsbereichsleiter.

Bei Proofpoint Endpoint DLP und Proofpoint ITM können Sie zu jeder Warnmeldung Details aufrufen, einschließlich Metadaten und Kontext mit Zeitleistenansichten. Sicherheitsteams können so schneller entscheiden, welche Ereignisse näher untersucht werden müssen und welche gleich wieder geschlossen werden können. Mithilfe von Tags lassen sich Warnmeldungen gruppieren und klassifizieren, um die Koordinierung zu vereinfachen.

Grundlegende 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. Durch Proofpoint ITM enthalten diese PDF-Exporte aus der Plattform Beweise in Form von Screenshots sowie damit verbundenen Kontext. Das erleichtert es nichttechnischen Teams wie der Personal- oder Rechtsabteilung, die Daten forensisch zu untersuchen.

Bildschirm-Screenshots für riskante Anwender

Ein Bild kann tausend Worte wert sein. Proofpoint ITM kann Screenshots von Anwenderaktivitäten erstellen, um so eventuell mit einem klaren und unwiderlegbaren Beweis für schädliches oder fahrlässiges Verhalten zur Entscheidungsfindung bei Personal- und Rechtsabteilungen sowie Managern beizutragen.

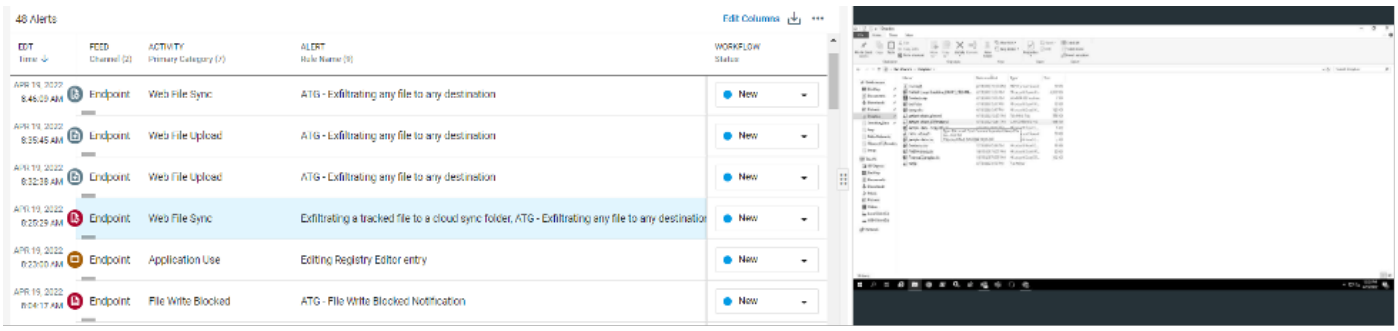

Abb. 7: Zeitleistenansicht von Anwenderaktivitäten mit Screenshot des Anwender-Endpunkts

Einfache Integration in komplexe Sicherheitsumgebungen

Die Information Protection and Cloud Security-Plattform basiert auf Mikroservices. Durch Webhooks, die in unsere Plattform eingebettet sind, können SIEM- und SOAR-Tools die Warnmeldungen von Proofpoint Endpoint DLP und Proofpoint ITM problemlos erfassen und so die Identifizierung und Triage von Zwischenfällen unterstützen.

Unternehmen mit einer komplexen Sicherheitsinfrastruktur müssen möglicherweise eine zentrale Informationsquelle für alle Systeme pflegen. Wir kommen dem entgegen, indem wir für Daten aus Proofpoint Endpoint DLP und Proofpoint ITM automatische Exporte in Ihren eigenen oder von Ihnen gehosteten AWS S3-Storage anbieten.

Erfüllen der Anforderungen an Datenschutz und Compliance

Verwaltung der Datenspeicherung

Für die Information Protection and Cloud Security-Plattform bieten wir die Möglichkeit, Daten in mehreren Regionen zu speichern, damit Sie die Vorschriften zu Datenschutz und Datenspeicherort einhalten können. Wir verfügen derzeit über Rechenzentren in den USA, in Europa, 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 können Kunden die Daten auf einfache Weise geografisch trennen und zum Beispiel Daten zu einem Endpunkt in den USA über eine US-Gruppe verwalten und in einem Rechenzentrum in den USA speichern.

Gewährleistung von Datenschutz mit attributbasierter Zugriffssteuerung

Um Datenschutzanforderungen einhalten zu können, müssen Sie den Datenzugriff flexibel steuern können. Mit Proofpoint Endpoint DLP und Proofpoint ITM können Sie den Zugriff auf einfache Weise verwalten und gewährleisten, dass Sicherheitsanalysten nur die Daten sehen können, die sie für Untersuchungen sehen müssen. Sie können zum Beispiel granulare Richtlinien erstellen und den Zugriff so zuweisen, dass Sicherheitsanalysten in Europa nur Daten zu europäischen Anwendern sehen können, aber keine Daten, die die USA oder den Asien-Pazifik-Raum betreffen. Die Einstellungsmöglichkeiten sind flexibel genug, dass Sie den Zugriff eines bestimmten Analysten auf konkrete Anwenderdaten beschränken oder festlegen können, dass der Zugriff nur für einen bestimmten Zeitraum möglich ist.

Überblick und Kontext für mehrere Kanäle

Proofpoint Endpoint DLP und Proofpoint ITM nutzen das volle Potenzial der Information Protection and Cloud Security-Plattform und bieten einen personenzentrierten Ansatz, um Inhalte, Verhaltensweisen und Bedrohungen zu überwachen. Auf diese Weise können sie Datenverlust stoppen und die Untersuchung von Zwischenfällen vereinfachen. Durch die zentrale Konsole erhalten Sie einen vollständigen Überblick sowie kontextbezogene Erkenntnisse zu mehreren Kanälen, einschließlich Endpunkte, Cloud, E-Mail und Web.

Sie können direkt über die Konsole für alle Kanäle Richtlinien einrichten, Bedrohungen suchen sowie Warnmeldungen untersuchen und darauf reagieren, ohne für die einzelnen Aktivitäten zwischen verschiedenen Tools wechseln zu müssen. Sie haben außerdem die Möglichkeit, Details zu den Metadaten der Warnmeldungen anzuzeigen, um zu verstehen, was vor, während und nach einem Ereignis passiert ist. Die Cloud-native Lösung lässt sich in kürzester Zeit bereitstellen, sodass Sie schnell eine Rendite erzielen können.

Durch die Transparenz und den Kontext der Information Protection and Cloud Security-Plattform können Sie effizienter arbeiten, wertvolle Zeit sparen und Geschäftsunterbrechungen durch Datenverlust und Insider-Bedrohungen minimieren.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.