Proofpoint Account Takeover Protection

Erkennung und Reaktion auf Cloud-Kontoübernahmen

Wichtige Vorteile

- Erkennt kompromittierte Microsoft 365-, Google Workspace- und Okta-Konten
- Schützt vor Kontoübernahme-Angriffen, die MFA umgehen
- Beschleunigt Ihre Untersuchungen dank einer zentralen Übersicht aller Aktivitäten nach der Kontoübernahme
- Verkürzt die Angreifer-Verweildauer durch Sperrung von Konten und Erzwingung von Kennwortzurücksetzungen
- Setzt böswillige Änderungen an Postfach-Regeln und MFA-Einstellungen zurück
- Entfernt verdächtige Drittanbieter-Anwendungen

Proofpoint Account Takeover Protection (ATO Protection) ergänzt Proofpoint Targeted Attack Protection (TAP) um Funktionen zur Erkennung kompromittierter Cloud-Konten und zum Schutz Ihrer Cloud-Umgebungen.

Proofpoint ATO Protection ergänzt Proofpoint Targeted Attack Protection (TAP) um Funktionen für Erkennung und Schutz vor kompromittierten Cloud-Konten. Die Lösung nutzt künstliche Intelligenz (KI), korrelierte Bedrohungsdaten sowie Verhaltensanalysen, um verdächtige Aktivitäten zu erkennen. Sie deckt dabei nicht nur die gesamte E-Mail-Angriffskette ab, sondern erkennt auch Änderungen durch Angreifer und entfernt deren Zugriff, indem sie böswillige Manipulationen von Postfach-Regeln und MFA-Einstellungen (Multifaktor-Authentifizierung) zurücksetzt. Sie entfernt auch verdächtige Drittanbieter-Anwendungen und isoliert sowie sperrt verdächtige Dateien.

Proofpoint ATO Protection stellt detaillierte Berichte zu verdächtigen Anmeldungen, angegriffenen Anwendern und betroffenen Systemen sowie Einstellungen bereit. Durch die Integration mit Proofpoint Identity Threat Defense sehen Sie mit einem einzigen Klick die potenziellen Auswirkungen einer Kontoübernahme auf andere Konten und Hosts. Dank dieser Erkenntnisse können Sie Angriffe stoppen, bevor daraus ernsthafte Kompromittierungen werden, die Ihrem Unternehmen schaden.

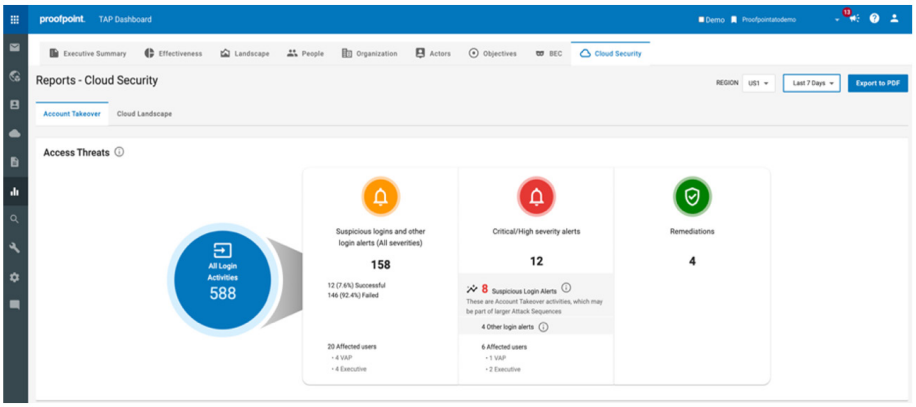
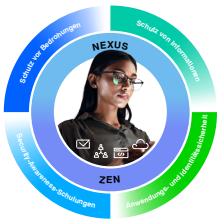


Abb. 1: Proofpoint ATO Protection erkennt verdächtige Anmeldungen, unterstützt mit detaillierten Erkenntnissen die Untersuchung von Bedrohungen und setzt böswillige Änderungen zurück.

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



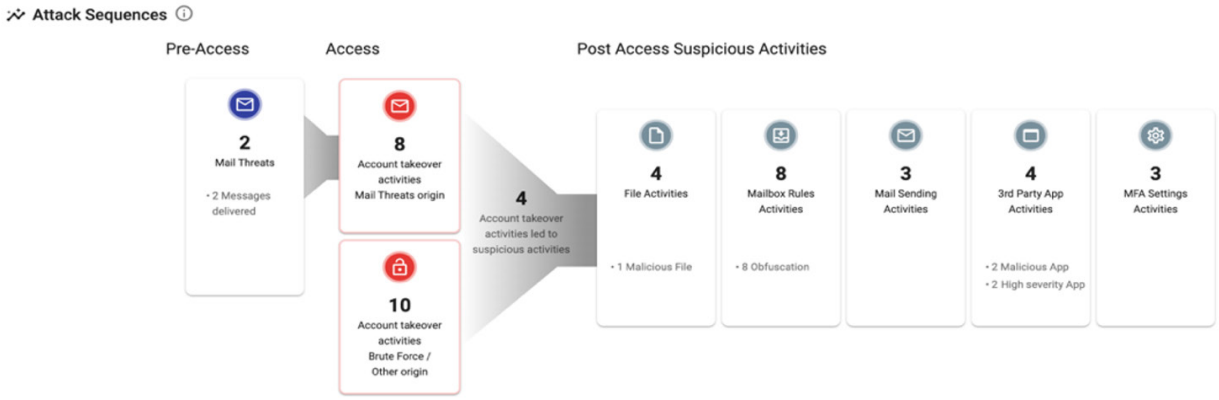


Abb. 2: Der Bericht „Attack Sequence“ (Angriffsablauf) zeigt Bedrohungsaktivitäten der betroffenen Konten vor und nach dem Zugriff.

Verbesserte Erkennung und Transparenz

Proofpoint ATO Protection erkennt kompromittierte Konten und verdächtige E-Mails sowie weitere Aktivitäten in Ihren Cloud-Umgebungen. Die Lösung nutzt Bedrohungsdaten von mehr als 40 Millionen Anwendern aus tausenden Unternehmen und kombiniert diese Informationen mit KI sowie Verhaltensanalysen, um ungewöhnliche Aktivitäten in Ihrer Umgebung zu erkennen. Durch diese Kombination von Techniken werden zudem False Positives reduziert, sodass Sie darauf vertrauen können, dass die Erkennungen korrekt sind und ein genaues Bild aller Aktivitäten in den angegriffenen Konten liefern.

Sobald eine Kontoübernahme erkannt wird, gibt Proofpoint ATO Protection Warnungen im TAP-Dashboard aus. Eine Zeitleiste des Angriffs zeigt Übernahmeaktivitäten, Datei- und E-Mail-Vorgänge, Änderungen an Postfach-Regeln sowie MFA-Einstellungen und die Installation von Drittanbieter-Anwendungen.

Beschleunigte Untersuchungen

Proofpoint ATO Protection zeigt Ihren Sicherheitsanalysten die Ursache einer Kontoübernahme und empfiehlt Maßnahmen zur Reduzierung weiterer Risiken. Diese Informationen sind in das TAP-Untersuchungssystem integriert, sodass diese Erkenntnisse die Informationen von Proofpoint TAP ergänzen. Eine Zeitleiste des Angriffs zeigt die übernommenen Konten, wobei jedes Ereignis angeklickt und untersucht werden kann.

Dadurch sehen Sie, wie das Konto angegriffen wurde und wo sich die Angreifer befinden. Zudem erfahren Sie, ob andere Anwender von ähnlichen Bedrohungen betroffen sind. Erweiterte Analysen liefern detaillierte Zeitleisten von Aktivitäten für Anwender, IP-Adressen, Domains und weitere Attribute. Diese umfangreichen Erkenntnisse helfen Ihnen, weitere Risiken für Ihr Unternehmen zu bewerten.

Automatisierte Reaktion

Proofpoint ATO Protection erkennt böswillige Änderungen an Postfach-Regeln und MFA-Einstellungen und setzt diese zurück. Angreifer ändern oft Postfach-Regeln, um sich in Ihrem System zu verbergen und es zu überwachen, bevor sie interne Phishing-Maßnahmen oder andere Angriffsschritte durchführen. Zudem entfernt Proofpoint ATO Protection auch schädliche Drittanbieter-Anwendungen. All diese Aktionen tragen dazu bei, den Schaden für Ihr Unternehmen zu minimieren und den Zeitaufwand für die Untersuchung und Abwehr von Bedrohungen zu verkürzen. Wenn Ihre Untersuchung andere schädliche Aktivitäten aufdeckt, können Sie die übernommenen Konten beheben und sogar Dateien entfernen, die Angreifer zu einem Anwenderkonto hinzugefügt haben.

„Proofpoint Account Takeover Protection“ war bisher „Proofpoint TAP Account Takover“.

MEHR ERFAHREN

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