proofpoint.

Proofpoint Account Takeover Protection

클라우드 계정 탈취 감지 및 대응

주요 이점

- 손상된 Microsoft 365, Google Workspace 및 Okta 계정 감지
- MFA를 우회하는 계정 탈취 공격으로부터 방어
- 계정 탈취 후 활동에 대한 집중식 보기로 조사 가속화
- 계정을 일시 중단하고 암호를 강제 재설정하여 공격자 체류 시간 줄이기
- 악의적인 메일함 규칙 및 MFA 설정 변경 되돌리기
- 의심스러운 타사 응용 프로그램 제거

Proofpoint Account Takeover Protection(ATO Protection)은 Proofpoint Targeted Attack Protection(TAP)을 확장하여 손상된 클라우드 계정을 탐지하고 클라우드 환경을 보호합니다.

ATO Protection은 Targeted Attack Protection(TAP)을 확장하여 손상된 클라우드 계정을 탐지하고 보호합니다. ATO Protection은 AI(인공지능), 위협 인텔리전스와의 상관관계 및 행동 분석을 활용하여 공격 사슬(attack chain) 전반에 걸친 의심스러운 활동을 탐지합니다. 공격자가 수행한 사기 공격 후 변경을 감지하여 공격자의 액세스 권한을 제거합니다. 악의적인 메일함 규칙 및 다단계 인증(MFA) 설정에 대한 업데이트를 되돌립니다. 또한 의심스러운 타사 응용 프로그램을 제거하고 의심스러운 파일을 격리하고 제거합니다.

ATO Protection은 의심스러운 로그인, 공격된 사용자와 영향을 받은 시스템 및 설정이 포함된 세부 보고서를 제공합니다. Proofpoint Identity Threat Defense와 통합하여 다른 계정 및 호스트에서의 계정 탈취로 인한 잠재적 영향을 간편하게 볼 수 있습니다. 이러한 인사이트를 확보하면 공격이 심각한 유출로 변하기 전에 방지하여 귀하의 비즈니스를 보호할 수 있습니다.

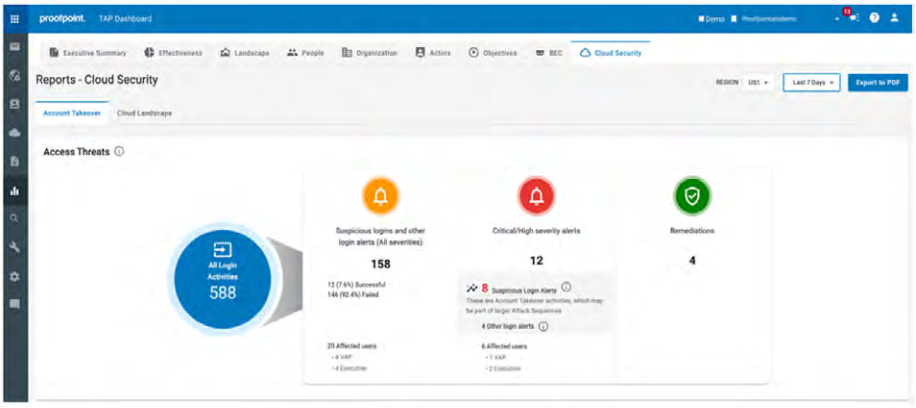
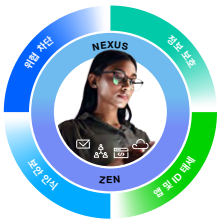


그림 1: ATO Protection에서는 의심스러운 로그인을 탐지하여 위협을 조사하고 악의적인 변경을 되돌리는 데 도움이 되는 상세 인사이트를 제공합니다.

이 솔루션 세트는 Proofpoint의 통합 Human-Centric Security 플랫폼의 일부이며 사람에게서 비롯되는 위험 중 네 가지 주요 영역을 완화합니다.



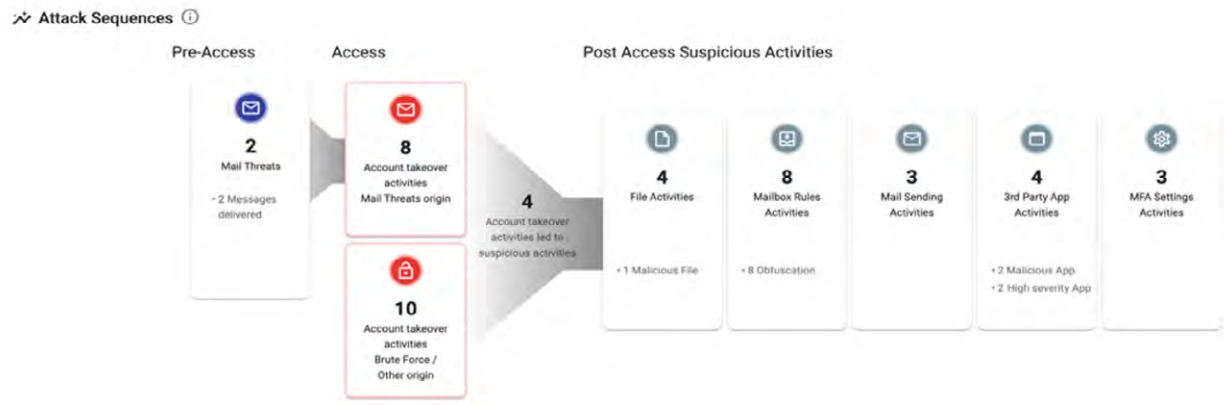


그림 2: 공격 시퀀스(Attack Sequence) 보고서는 영향을 받은 계정에 대한 액세스 전과 후의 위협 활동을 보여 줍니다.

탐지 및 가시성 향상

ATO Protection은 클라우드 환경에서 손상된 계정 및 의심스러운 이메일과 기타 활동을 탐지합니다. ATO Protection은 수천 개의 조직에 걸쳐 모니터링되는 4000만 명 이상의 사용자가 제공하는 위협 인텔리전스를 활용합니다. 이 정보를 AI 및 행동 분석과 결합하여 사용자 환경에서의 비정상적인 활동을 탐지합니다. 이러한 기술 결합은 오탐지로 판명된 경보를 줄입니다. 정확한 탐지에 대해 확신하고 공격된 계정의 모든 활동을 명확하게 확인합니다.

계정이 탈취되면 ATO Protection은 TAP 대시보드에 경보를 추가합니다. 공격 타임라인으로 계정 탈취 활동, 파일 및 이메일 활동, 메일함 규칙 및 MFA 설정 변경 사항 및 추가 타사 앱 추가를 확인합니다.

조사 가속화

ATO Protection을 통해 보안 분석가에게 계정 탈취 원인 및 향후 위험 제한 방법을 보여줄 수 있습니다. 이 정보는 TAP 조사 시스템 및 프로세스와 통합됩니다. 이를 통해 TAP에서 제공하는 접근 방식을 보완하는 인사이트를 확보할 수 있습니다.

공격 타임라인은 탈취된 계정을 보여 줍니다. 타임라인에서 각 이벤트를 클릭하여 조사할 수 있습니다.

계정이 공격된 방식과 공격자의 위치를 확인할 수 있습니다. 유사한 위협의 피해를 입은 사용자에 대해 알아볼 수도 있습니다. 고급 분석은 사용자, IP 주소, 도메인 및 기타 특성에 대한 상세 활동 타임라인을 제공합니다. 이러한 풍부한 인사이트로 사용자 조직에 대한 향후 위험을 평가할 수 있습니다.

자동화된 대응

ATO Protection은 악의적인 메일함 규칙 및 MFA 설정 변경을 감지하고 되돌립니다. 공격자는 내부 피싱을 시작하거나 다른 공격 단계를 수행하기 전에 메일함 규칙을 변경하여 시스템에 숨겼다가 모니터링하는 경우가 많습니다. 또한 ATO Protection은 악의적인 타사 앱도 제거합니다. 이러한 모든 활동은 사용자 조직에 대한 피해를 제한하고 위협 조사 및 대응 시간을 줄입니다. 사용자 조사에 기타 악의적 활동이 있는 경우 탈취된 계정을 수정할 수 있습니다. 또한 공격자가 사용자 계정에 추가한 파일을 제거할 수도 있습니다.

"Proofpoint Account Takeover Protection"의 이전 이름은 "Proofpoint TAP Account Takover"입니다.

자세히 알아보기

자세한 내용은 **proofpoint.com**을 참조하십시오.