Proofpoint Targeted Attack Protection

고급 위협 보호 및 가시성 확보

주요 이점

- 지능형 위협이 받은 편지함에 도달하기 전에 탐지, 분석 및 차단
- Very Attacked People™ 및 전반적인 보안 위험을 식별하기 위한 고유한 통찰력 확보
- Proofpoint 위협 인텔리전스를 활용하여 위협으로부터 보호하고 공격에 대한 자세한 포렌식 수신
- URL 격리 및 보안 인식 교육을 통해 적응형 보안 제어 제공
- VAP가 회사 이메일을 통해 알려지지 않은 웹사이트를 자신 있게 탐색하는 동시에 URL 및 웹 기반 공격으로부터 웹사이트를 보호할 수 있습니다. 이 기능은 솔루션 번들의 일부입니다.

공격의 90% 이상이 이메일에서 시작되며[1] 이러한 위협은 항상 진화하고 있습니다. Proofpoint TAP(Targeted Attack Protection)는 사용자를 표적으로 삼는 지능형 위협을 탐지, 분석 및 차단하는 혁신적인 접근 방식을 제공합니다. 또한 이러한 위협에 대한 고유한 가시성을 제공하여 대응을 최적화할 수 있습니다.

TAP는 알려진 이메일 공격과 이전에 본 적이 없는 이메일 공격을 모두 차단합니다 다형성 멀웨어, 무기화된 문서, 자격 증명 피싱 및 기타 지능형 위협을 탐지하고 차단합니다. 클라우드 앱 활동을 모니터링하여 의심스러운 로그인, 광범위한 파일 공유, 위험한 타사 애플리케이션 등을 식별합니다. 또한 가장 표적이 되는 사람들을 식별하고 보호하는 데 필요한 통찰력을 제공합니다.

BEC, URL, 첨부 파일 및 클라우드 기반 위협으로부터 보호

TAP는 정적 및 동적 기술을 모두 사용하여 새로운 공격 패턴을 지속적으로 탐지하고 이에 적응합니다. Proofpoint는 행동, 코드 및 프로토콜을 조사하는 다양한 접근 방식을 사용하여 잠재적인 위협을 분석합니다. 이를 통해 잠재적으로 피해를 입히기 전에 공격 사슬 초기에 위협을 탐지할 수 있습니다.

TAP는 BEC(비즈니스 이메일 사기 공격) 및 공급업체 계정 침해 위협으로부터 보호합니다. 이러한 유형의 공격에는 악성 페이로드가 없는 경우가 많으므로 공격을 식별하려면 샌드박싱을 뛰어넘는 정교한 탐지 기술이 필요합니다. Proofpoint의 위협 인텔리전스인 Nexus 위협 그래프는 TAP를 강화합니다. 이메일, 클라우드, 네트워크, 엔드포인트 및 소셜 네트워킹 소스 전반에 걸쳐 1조 개의 데이터 포인트를 수집, 분석 및 상호 연관시킵니다. Advanced BEC Defense 엔진은 풍부한 위협 데이터를 기반으로 구축 및 훈련되었습니다. 실시간으로 학습하고 위협 환경의 변화에 신속하게 대응할 수 있습니다.

Proofpoint는 샌드박싱을 사용하여 다양한 공격을 연구합니다. 공격에는 악성 첨부 파일과 URL을 사용하여 멀웨어를 설치하거나 사용자가 민감한 정보를 공유하도록 속이는 것이 포함됩니다. 또한 분석가 지원 실행을 활용하여 탐지 및 인텔리전스 추출을 극대화합니다.

클라우드 공격을 보다 잘 이해할 수 있도록 TAP는 클라우드 앱의 위협과 위험을 감지하고 이를 자격 증명 도난 및 기타 이메일 공격으로 연결합니다. Proofpoint의 기술은 위협을 탐지할 뿐만 아니라 머신 러닝을 적용하여 각 공격에 사용되는 패턴, 동작 및 기술을 관찰합니다. 이러한 통찰력으로 무장한 TAP는 향후 공격을 더 빠르게 포착할 수 있도록 학습하고 적응합니다.

Advanced BEC Defense

Advanced BEC Defense는 BEC 및 공급업체 계정 침해 위협으로부터 보호합니다. 다음을 포함하여 메시지 내의 모든 세부 사항에 대한 포괄적인 분석을 수행합니다.

- 헤더 포렌식
- 원래 IP 주소
- 발신자 및 수신자 관계
- 평판 분석
- 심층적인 콘텐츠 분석

또한 Advanced BEC Defense는 공격자 기술, 위협 관찰 및 메시지 샘플에 대한 자세한 가시성을 제공합니다. 이는 사용자가 표적이 되는 방식을 이해하는 데 도움이 됩니다.

URL Defense

TAP URL Defense는 멀웨어 및 자격 증명 피싱을 포함한 URL 기반 이메일 위협으로부터 보호합니다. 이메일 트래픽 패턴을 기반으로 의심스러운 URL을 식별하고 샌드박스 처리하는 고유한 예측 분석 기능을 제공합니다. 받은 편지함에 도달하는 모든 URL은 투명하게 다시 작성됩니다. 이를 통해 모든 장치나 네트워크에서 사용자를 보호합니다. URL을 클릭할 때마다 실시간 샌드박싱도 수행됩니다.

Attachment Defense

TAP Attachment Defense는 첨부 파일을 통해 전달되는 알려진 위협과 알려지지 않은 위협에 대한 보호 기능을 제공합니다. 광범위한 파일 형식, 비밀번호로 보호되는 문서, URL이 삽입된 첨부파일 및 Zip 파일에 숨겨진 위협으로부터 보호합니다.

TAP Account Takeover

TAP Account Takeover는 전체 이메일 계정 탈취 공격 사슬에 대한 가시성과 방어 기능을 제공합니다. 그래픽 공격 시퀀스 타임라인은 손상된 계정과 의심스러운 활동에 대한 조사 속도를 높이는 데 도움이 됩니다. 어떤 종류의 메일 위협이 계정을 표적으로 하는지 확인할 수 있습니다. 공격자가 계정에 액세스하는 경우 해당 계정을 보호하기 위해 시정 조치를 취할 수 있습니다. 또한 이메일 및 클라우드 환경 전반에 걸쳐 악의적인 메일함 규칙 변경, 악용된 타사 앱, 데이터 유출 문제를 해결합니다. TAP Account Takeover는 Microsoft 365, Google Workspace 또는 Okta와 호환됩니다.

SaaS Defense

TAP SaaS Defense는 의심스러운 로그인 활동을 밝힙니다. 여기에는 비정상적인 로그인 위치, 과도한 로그인 시도 및 실패가 포함됩니다. 또한 알려진 악성 IP 주소로부터의 연결이 너무 많은 경우에도 플래그를 지정합니다. 내부 및 외부의 노출도가 높은 파일 공유 이벤트에 대한 가시성을 얻을 수 있습니다. 이를 통해 지난 30일 동안 민감한 데이터가 유출되었을 수 있는 시기를 확인할 수 있습니다. TAP SaaS Defense는 조직에서 사용 중인 중요하고 심각도가 높은 타사 애플리케이션을 탐지합니다. Microsoft 365 또는 Google Workspace와 호환됩니다.

Isolation for VAP

TAP URL Isolation for VAP는 URL 및 웹 기반 공격으로부터 VAP(Very Attacked People™)를 보호하도록 설계되었습니다. 실시간 피싱 탐지 기능을 제공하고 알려지지 않은 위험한 URL로부터 사용자와 허용된 클릭을 보호하는 데 도움이 됩니다. Proofpoint의 격리된 브라우저 솔루션을 사용하면 VAP는 조직이 안전하다는 사실을 알고 회사 이메일을 통해 자신 있게 웹사이트에 액세스할 수 있습니다.

위협 및 표적에 대한 깊은 통찰력과 가시성 확보

Proofpoint는 이메일, 클라우드, 네트워크, 소셜 미디어와 같은 다양한 위협 벡터에 대한 가시성을 확보하고 있습니다. 이러한 가시성은 전 세계 115,000명이 넘는 고객으로부터 얻은 것입니다. 수집된 데이터는 Proofpoint Nexus Threat Graph로 전달됩니다. 여기서 위협 환경에 대한 가시성을 높이기 위해 상호 연관됩니다. 위협 및 캠페인에 대한 자세한 실시간 정보를 제공하는 TAP Threat Insight 대시보드를 통해 이를 확인하고 다른 중요한 통찰력을 수집할 수 있습니다. 이 데이터를 통해 광범위한 공격과 표적 공격 모두를 파악할 수 있습니다. 영향을 받은 사용자, 공격 스크린샷, 심층적인 포렌식 등 위협에 대한 세부 정보를 확인할 수 있습니다.

Very Attacked People

Proofpoint Attack Index는 VAP를 식별하는 데 도움이 되므로 보안 팀은 조직의 주요 표적을 식별할 수 있습니다. 지수는 조직 내 개인에게 전송된 모든 위협의 가중치 종합 점수입니다. 위협의 정교함, 공격 표적의 확산 및 초점, 공격 유형, 전체 공격 규모를 기준으로 0~1,000점의 위협 점수를 매깁니다. VAP를 더 잘 이해함으로써 위협을 차단하는 가장 효과적인 방법의 우선순위를 정할 수 있습니다.

회사 차원 Attack Index

Attack Index는 회사 차원에서 적용할 수도 있으며 다른 산업과 비교하여 전반적인 회사 위험을 비교할 수도 있습니다. 이 보고서는 CISO와 보안 팀이 회사에 대한 공격을 업계 전반의 동료에 대한 공격과 비교하여 이해하는 데 도움이 됩니다. 공격 빈도와 위협 유형에 대해 다룹니다. 이러한 통찰력을 통해 고유한 공격 환경에 따라 보안 제어의 우선순위를 지정할 수 있습니다.

위협 행위자 통찰력

사람들이 계속해서 표적이 되면서 고객이 공격을 실행하는 위협 행위자에 대한 전체적인 그림을 파악하는 것이 더욱 중요해지고 있습니다. Proofpoint의 위협 연구원들은 수년 동안 행위자에 대한 데이터를 선별해 왔으며 이 인텔리전스는 TAP 대시보드에 표시됩니다. 고객은 자신을 표적으로 삼는 위협 행위자, 표적이 되는 사람, 사용되는 전술과 기법, 위협 행위자로부터 시간이 지남에 따라 형성되는 추세를 파악할 수 있습니다. 이를 통해 조직은 직원을 보다 효과적으로 보호하기 위해 추가 보안 및 교정 제어의 우선순위를 결정할 수 있습니다.

자세한 정보

자세한 내용은 **proofpoint.com**을 참조하십시오.