Advanced Email Security

지능형 이메일 위협으로부터 보호하고, 운영을 간소화하며 인력 위협과 위협 환경에 대한 실행 가능한 가시성을 확보

제품

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Email Isolation
- Proofpoint Browser Isolation
- Proofpoint Security Awareness Training
- Proofpoint Email Fraud Defense
- Proofpoint Internal Mail Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

주요 이점

- 악의적 URL, 첨부파일 및 랜섬웨어가 포함되어 있거나 이메일 사기를 시도하는 위협 차단
- 통합 워크플로를 통해 사용자가 제출한 메시지 또는 전송 후 활성화된 메시지 자동 수습
- 인력, 위협 및 공급업체나 클라우드 위험과 같은 기타 인사이트에 대한 뛰어난 가시성 확보
- DMARC 정책을 간편하게 배포하고 인증을 빠르고 안전하게 적용하여 신뢰할 수 있는 도메인을 도용하는 사기 이메일 차단
- 사용자를 교육하고 역량을 강화하여 사이버 보안 위협에 대한 강력한 방어선 구축

이메일은 현대 비즈니스의 기본적인 기능이며, 1순위 위협 벡터이기도 합니다. 또한 피싱 공격에서 비즈니스 이메일 사기 공격(BEC), 공급망 공격, 랜섬웨어 및 클라우드 계정 침해에 이르는 이메일 공격은 계속 진화하고 있습니다. 따라서 이러한 벡터를 위협으로부터 효과적으로 보호하려면 상당한 노력이 필요하며, 이는 가장 규모가 크고 복잡한 조직에서도 마찬가지입니다. Proofpoint가 도움을 드릴 수 있습니다.

Fortune 100대 기업, Fortune 1000대 기업 및 Global 2000대 기업 중 점점 더 많은 기업들이 이러한 위협에 대처하기 위하여 다른 어떤 지능형 이메일 보안 공급업체보다 Proofpoint를 신뢰합니다. 당사의 솔루션은 이러한 문제에 대처하기 위해 인라인 및 API 접근 방식을 사용합니다. 이를 통해 수신 및 발신 메시지를 완벽하게 보호할 수 있습니다. 단지 기본 보안 솔루션에서 누락된 이메일에만 집중하지 않습니다. 통합된 계층적 접근 방식을 통해 위협을 더 빠르고 정확하게 탐지하여 공격이 성공할 위험성을 줄입니다. 최고의 탐지 조합과 확장 가능한 플랫폼을 통해 운영 효율을 개선할 수 있습니다. 그리고 실행 가능한 인사이트를 활용해 직면한 위험을 더 효과적으로 이해할 수 있습니다. 선제적 조치를 실행하여 보다 빠르고 효과적으로 대응할 수도 있습니다.

지능형 위협 탐지 및 차단

신뢰할 수 있는 효능 확보

Proofpoint의 위협 인텔리전스 및 탐지를 통해 가양성을 최소화하면서 정교한 위협에 대해 강력한 방어를 구축할 수 있습니다.

Proofpoint는 평판, URL 재작성과 예측 및 클릭 시간 샌드박싱을 사용해 첨부 파일이나 URL을 통해 들어오는 페이로드 위협을 탐지합니다. CAPTCHA, 암호 보호, 렌더링이 과도한 사이트, 리디렉터 및 파일 공유 사이트 같은 회피 및 난독화를 뚫을 수 있는 탐지 기능이 내장되어 있습니다.

또한 Nexus Threat Graph의 AI(인공지능) 및 ML(머신 러닝) 모델을 사용하여 BEC 같이 페이로드 없는 공격을 탐지합니다. AI/ML 모델은 공급업체 위험, 협업 제품군의 사용자 신호, 콘텐츠 자연어 처리, 수신자 관계 및 의도 등의 신호를 평가합니다. 기준 데이터와 컨텍스트 데이터를 통해 악의적일 수 있는 이메일을 빠르게 파악할 수 있습니다. 해당 데이터는 당사의 위협 인텔리전스 및 기타 표적 탐지 엔진과 원활하게 작동합니다. 이를 통해 가양성을 최소화할 수 있습니다.

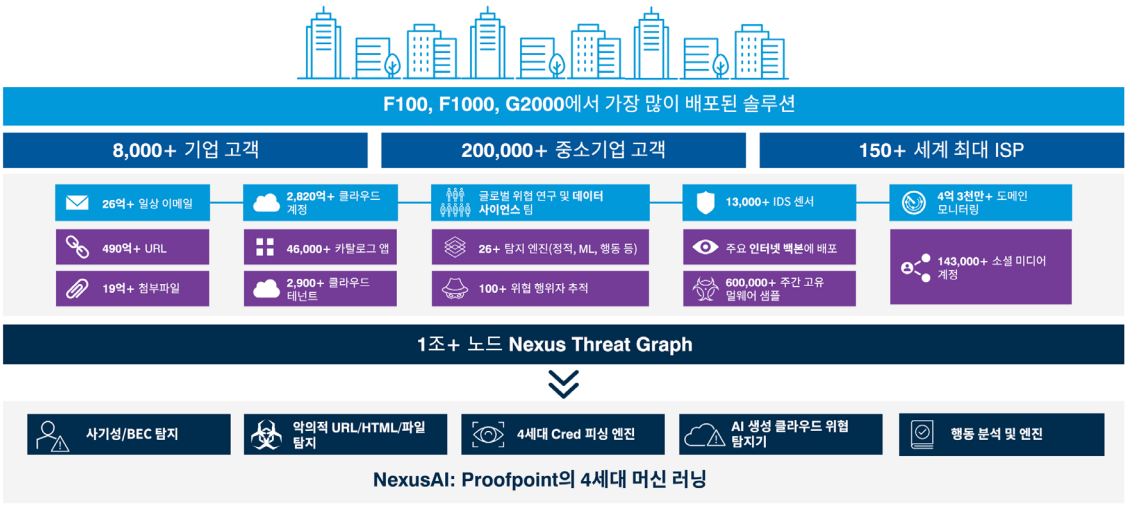

그림 1: Nexus Threat Graph.

지금과 같은 사람 중심 위협 환경에서 사용자가 가장 큰 자산일 뿐만 아니라 가장 큰 위험이기도 합니다.

Proofpoint는 다중 계층 콘텐츠 분석, 평판 분석 및 샌드박싱을 통해 이메일을 분석합니다. 이러한 방식으로 다양한 형태의 멀웨어 및 랜섬웨어를 포함한 지능형 이메일 위협이 사용자를 공격하기 전에 위협을 효과적으로 차단합니다. 또한 악성 URL을 탐지하고 차단하기 위한 예측 및 클릭 시간 URL 샌드박싱을 제공합니다. URL 재작성을 통해 네트워크 또는 장치에서 사용자를 보호할 수 있습니다. 메시지가 전송 이후 무기화되었는지 여부를 탐지할 수도 있습니다.

이메일 및 브라우저 격리를 통한 안전한 클릭

Proofpoint 이메일 및 브라우저 격리는 사용자가 웹사이트, 개인 웹 메일 및 회사 이메일에 안전하게 액세스할 수 있는 안전한 환경을 제공합니다. 공격자는 공급업체 계정을 손상시키듯 사용자의 시스템에 액세스하기 위해 다양한 전술과 위협 벡터를 사용합니다. 예를 들어 개인 이메일 또는 보호되지 않는 채널을 통해 사용자를 표적으로 삼을 수 있습니다. 격리를 통해 업로드 및 다운로드를 비활성화할 수 있습니다. 웹사이트가 실시간으로 분석되는 동안 데이터 입력을 제한할 수도 있습니다. 이러한 과정이 몇 초 이내에 이루어집니다. 이 기술은 자격 증명 도난과 멀웨어 또는 랜섬웨어를 방지하기 위해 계층을 추가합니다. 특히 오염된 URL이 포함된 전송 후 피싱 이메일 방지에 효과적인 기술입니다.

이메일 인증을 통한 이메일 사기 방지

이메일 인증은 보호 계층을 추가합니다. 이 방법이 BEC처럼 멀웨어가 없는 사기성 위협을 방지하는 데 효과적인 것은 입증된 사실입니다. 그러나 합법적인 이메일을 차단할 수 있다는 위험성 때문에 조직은 DMARC 표준을 채택하고 적용하기를 주저합니다.

Proofpoint는 합법적인 메일 흐름을 차단하지 않고도 DMARC를 완벽하게 배포하고 적용할 수 있도록 지원합니다. 신뢰할 수 있는 도메인을 사용하여 도메인 스푸핑 및 사기 이메일로부터 보호합니다. 회사의 이메일 ID를 보호하는 동시에 Proofpoint 게이트웨이에서 사기 이메일을 차단합니다. 아울러 도메인과 유사한 악성 도메인을 포함한 모든 사기성 위협을 하나의 창에서 확인할 수 있습니다. 사용된 전술이나 표적이 된 사람과 무관하게 가시성을 확보할 수 있습니다. Virtual Takedown 서비스를 사용하면 사기성 유사 도메인 이메일 공격이 발생하기 전에 선제적으로 공격을 방지할

수 있습니다. Proofpoint는 배포의 모든 단계를 안내하는 숙련된 컨설턴트를 통해 DMARC 구현 과정을 단순화합니다. 당사는 고객과 함께 모든 신뢰할 수 있는 발신자(타사 발신자 포함)를 식별하여 인증이 제대로 이루어지도록 보장합니다. Proofpoint는 해당 프로세스를 바탕으로 Fortune 1000대 기업 중 1/3 이상의 기업에 도움을 제공했습니다. 당사는 가장 정교한 구성의 작업이 가능합니다.

내부 이메일 보호 및 신속한 위협 방지

내부 이메일 보호의 중요성은 수신 이메일 보호에 못지않습니다. 공격자는 손상된 계정을 사용하여 피싱, BEC 또는 멀웨어를 전송합니다. 당사는 내부 이메일에서 URL 및 첨부파일 형식의 악의적 콘텐츠를 스캔합니다. 악의적 내부 이메일이 탐지되면 자동으로 끌어와 격리할 수 있습니다. 다른 사용자가 이미 이메일을 수신한 후 다른 사람에게 전달한 경우에도 마찬가지입니다. Proofpoint는 또한 손상되었을 가능성이 있는 모든 계정을 알려주는 보고서를 제공합니다. 이를 통해 해당 계정에 신속한 조치를 취할 수 있습니다.

공격 및 인적 공격 표면에 대한 가시성 확보

위험을 더 효과적으로 완화하고 관리자와 이사회에 전달하려면 다음 내용을 숙지해야 합니다.

- 가장 위험한 상태의 사용자 및 해당 사용자가 표적이 되는 방식
- 위협 환경 인사이트, 목표, 행위자 및 트렌드
- 공급업체 및 클라우드 위험 인사이트 같은 기타 신호

Proofpoint는 이 모든 것을 포함한 다양한 기능을 제공합니다.

당사의 플랫폼 접근 방식을 활용하면 데이터 사일로 없이 사람 중심의 위험을 전체적으로 파악할 수 있습니다. 당사는 사용자가 정교한 위협에 더욱 선제적으로 대응할 수 있도록 지원합니다.

사람 중심 인사이트를 통한 위험 해결

지금과 같은 사람 중심 위협 환경에서 사용자는 가장 큰 자산일 뿐만 아니라, 가장 큰 위험이기도 합니다. 당사는 표적화된 공격과 인적 공격 표면에 대한 뛰어난 가시성을 제공합니다.

조직에 가장 큰 위험을 초래하는 사람이 누구이며 그 이유가 무엇인지 알려드립니다. 당사의 VAP(Very Attacked People™) 보고서를 통해 가장 표적이 되고 있는 사용자들을 확인할 수 있습니다. Top Clickers 보고서에서 실제 악의적 메시지를 클릭한 사용자가 누구인지 확인할 수 있습니다. 대시보드에서 VIP를 입력하고 추적할 수 있습니다. 이러한 인사이트를 확보하면 위험에 처한 사용자가 위험을 우선시하고 완화하도록 적응 제어를 구현할 수 있습니다. 이러한 제어에는 표적의 보안 인식, 브라우저 격리 및 다단계 인증이 포함될 수 있습니다.

컨텍스트에 대한 위협 중심 인사이트 확보

Proofpoint는 위협 및 캠페인에 대한 자세한 포렌식 정보를 실시간으로 제공합니다. 심층 위협 분석을 통해 공격을 받은 사람과 공격의 기원 및 형태에 대한 모든 정보를 확인할 수 있습니다. 당사는 공격의 목표도 식별합니다. 예를 들어 공격의 목표가 데이터 유출인지, 랜섬웨어 설치인지 사기 행위의 실행인지 등을 판별할 수 있습니다. 당사는 이메일 공격과 의심스러운 로그인 사이의 연관성을 확인하며, 이를 통해 계정 침해를 더욱 효과적으로 확인하고 차단할 수 있습니다. 플랫폼에서 동료와의 비교를 통해 사용자가 받는 위협 유형과 목표에 대한 포괄적인 벤치마킹을 확인할 수 있습니다.

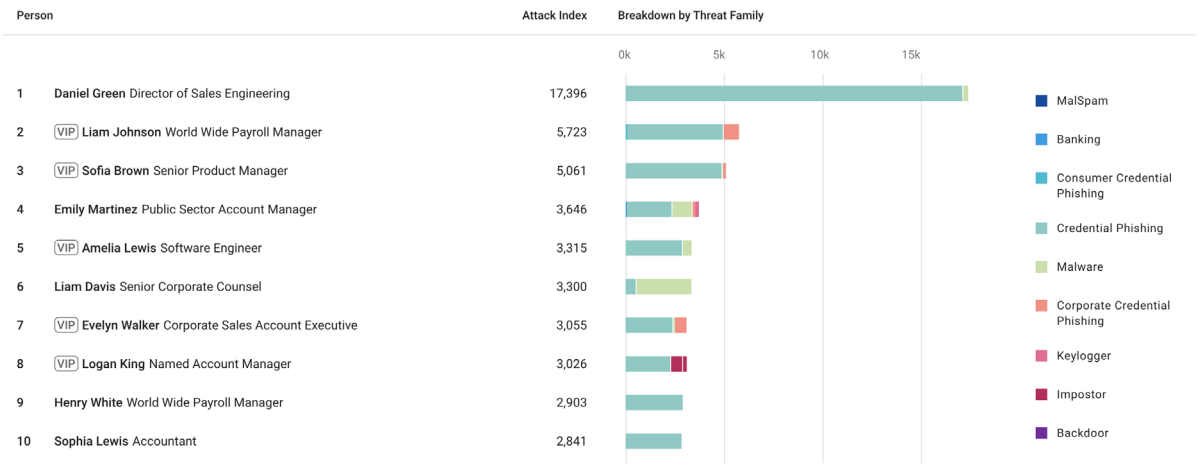

그림 2: Proofpoint의 VAP(Very Attacked People) 보고서는 가장 위험한 상태의 사용자와 위협 유형을 제공합니다.

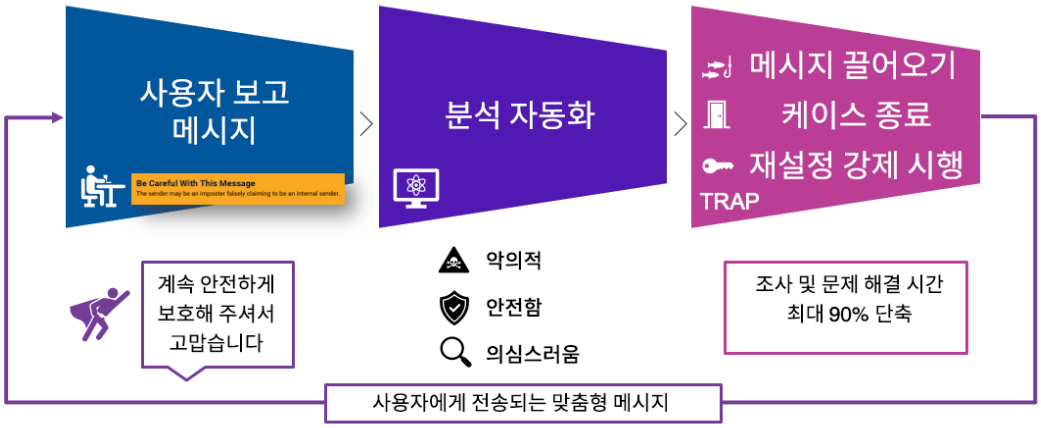

그림 3: Proofpoint의 자동화된 악용 메일함 솔루션 CLEAR(Closed-Loop Email Analysis and Response)

공급업체 및 클라우드 손상 위험 인사이트 통합

Proofpoint는 손상 및 공급업체 위험에 대한 가시성을 제공합니다. 이러한 공격 벡터 전반에 대한 가시성을 바탕으로 복잡한 공격에 철저하게 대응할 수 있습니다. Nexus Supplier Risk Explorer를 통해 잠재적으로 손상된 공급업체와 이들이 사용자에게 이메일 전송 시 사용하는 도메인을 자동으로 식별합니다. 내장된 SaaS Defense 기능을 사용하면 잠재적으로 손상된 사용자와 악의적 또는 유출된 파일 및 위험한 타사 애플리케이션에 대한 인사이트를 얻을 수 있습니다.

운영 효율성 개선

많은 조직이 보안 팀의 인력 부족 또는 업무 부담을 경험해 왔습니다. 이러한 팀에서는 서로 소통이 되지 않는 다양한 보안 공급업체 및 제품을 관리하는 경우가 많습니다. 당사는 중요한 위협에 집중하며 위협 탐지 및 문제 해결을 자동화하는 통합 솔루션을 제공합니다. 이러한 방식을 사용하면 보안 팀이 경쟁 솔루션을 사용했을 때보다 비교적 적은 내부 리소스로 문제를 해결할 수 있으므로 시간과 비용을 절감할 수 있습니다.

악의적 이메일 자동 끌어오기

Proofpoint는 사고 대응에서 수동 작업과 추측에 따른 작업을 배제합니다. 이는 위협을 더욱 빠르고 효율적으로 해결하는 데 도움이 됩니다. 당사는 오염된 URL이 포함된 전송 후 피싱 이메일을 제거합니다. 손상된 내부 계정의 원치 않는 이메일을 원클릭 또는 자동으로 제거할 수도 있으며, 이는 다른 사용자가 전달하거나 수신한 경우에도 동일하게 적용됩니다. 또한 당사의 Nexus Threat Graph는 경고를 제공하고 자동으로 포렌식 데이터를 수집하고 비교합니다. 이를 통해 위협에 대한 실행 가능한 보기를 얻을 수 있습니다. 사용자는 이러한 접근 방식을 통해 이메일 문제 해결 시간을 최대 90% 절감할 수 있습니다.

악용 메일함 프로세스 간소화

Proofpoint는 악용 메일함 프로세스를 간소화하고 IT 오버헤드를 줄일 수 있도록 지원합니다. 사용자는 원클릭으로 간편하게 의심스러운 메시지를 신고할 수 있습니다. Email Warning Tag 또는 PhishAlarm® 이메일 보고 추가 기능을 사용해 직접 신고할 수 있습니다. 신고된 메시지가 악의적이라고 판단되면 해당 메시지와 다른 복사본이 자동으로 격리되도록 할 수 있습니다. 사용자는 해당 메시지가 악의적이라는 사실을 알리는 맞춤화된 이메일을 수신하게 됩니다. 이렇게 하면 이후 비슷한 메시지를 더 활발하게 신고하도록 할 수 있습니다. 관리자는 사용자 행동에 대한 심도 있는 보고를 얻고 동료에 대해 벤치마킹된 악의적 메시지 신고의 정확성도 확보할 수 있습니다.

위협 기반 교육을 통한 행동 변화

최신 이메일 위협은 사람이 있어야만 활성화되는 경우가 많습니다. 그러나 사이버 보안 방어의 구축에서 직원이 약점이 될 이유는 전혀 없습니다. 보안을 의식하는 직원은 오히려 사이버 공격에 대한 강력한 방어선이 될 수 있습니다.

Proofpont는 VAP 또는 Top Clickers에 대응할 수 있도록 지원합니다. 해당 항목에 대해 수집된 데이터는 보안 인식 플랫폼에 자동으로 통합됩니다. 해당 데이터를 사용하여 플랫폼은 더욱 표적화되고 영향력 있는 교육 프로그램을 운영합니다. Proofpoint 위협 인텔리전스의 실제 피싱 시뮬레이션을 사용하므로 시기 적절하고 관련성 높은 교육 경험이 구현됩니다. 시뮬레이션에 등록한 사용자에게는 적시 지침이 제공됩니다. 사용자는 이후 특정 교육에 자동으로 등록될 수 있습니다. 또한 Report Suspicious 기능이 포함된 Email Warning Tag가 사용자에게 제공됩니다. 해당 태그는 특정 이메일과 연관된 위험에 대한 간단한 맞춤형 설명과 시각 자료를 제공하며 태그에서 바로 메시지를 신고할 수 있습니다. 이를 통해 사용자는 더욱 합리적인 결정을 내릴 수 있습니다. 해당 기능은 모든 장치 및 애플리케이션에서 원활하게 작동합니다.

이메일을 통한 데이터 손실 방지

이메일은 수신 위협 및 발신 데이터 손실 양측에 대한 1순위 위협 벡터입니다. 따라서 민감한 데이터를 보호하고 이메일에서 발생하는 데이터 손실을 방지해야 합니다. Proofpoint는 이메일 커뮤니케이션 중의 의도적이고 우발적인 데이터 손실을 방지할 수 있도록 즉시 사용 가능한 가시성 및 시행을 제공합니다.

DLP(데이터 유출방지) 및 암호화가 긴밀하게 통합되어 있으며, 정보 및 클라우드 보안 플랫폼에서 중앙 집중적으로 관리할 수 있습니다. 새로운 통합 경고 관리자를 통해 즉시 사용 가능한 데이터 탐색을 맞춤화하여 우려되는 DLP 위반을 조사 및 보고할 수 있습니다. 당사는 최적화된 워크플로와 문제 해결 기능을 통해 운영을 간소화합니다. 구조화된 데이터와 비구조화된 데이터의 기밀 데이터를 분석합니다. 미세 조정된 정책 및 사전 구축된 사전도 제공합니다. 이는 규정 준수 및 데이터 프라이버시 법에 의해 보호되는 데이터를 자동으로 식별합니다. 아울러 이는 수동 작업을 줄이는 동시에 PCI DSS, SOX, HIPAA, GDPR 등 다양한 산업 분야의 데이터 보호 규칙을 준수하는 데 유용합니다. 암호화와 결합하면 이메일의 민감한 데이터를 자동으로 암호화하도록 고유의 정책을 정의하고 사용자 지정할 수 있습니다. 이러한 방식을 사용하면 민감한 데이터 교환을 간편하게 관리하고 보호할 수 있습니다.

요약

Proofpoint Advanced Email Security는 이메일을 표적으로 삼는 위협을 효과적으로 차단할 수 있습니다. 공격 및 가장 자주 공격을 받은 사람에 대한 실행 가능한 가시성을 제공합니다. 솔루션:

- 지능형 위협이 전달되기 전에 차단
- 인력 위험, 위협 및 인사이트에 대한 뛰어난 가시성 제공
- 효과적이고 자동화된 위협 대응을 통한 운영 효율성 개선
- 사용자에 대한 교육 및 역량 강화를 통해 강력한 방어선 구축
- 이메일을 통한 데이터 손실 방지

자세한 정보

자세한 내용은 **proofpoint.com**을 참조하십시오.