CLOUDFLARE

솔루션 요약

Cloudflare + Microsoft 365 피싱 방어

안전한 작업 영역의 커뮤니케이션을 위한 자율적인 멀티 채널 보호 기능 제공

레거시 게이트웨이를 버리고 피싱 보호 기능 업그레이드하기

2000년대 초, 라우팅과 이메일 필터링에 관해 증가하는 요구에 대응하기 위해 보안 이메일 게이트웨이(SEG)가 도입되었습니다. SEG는 여러 해 동안 성공적으로 임무를 수행해 왔지만, SEG는 근본적인 설계 때문에 빠르게 커지는 피싱 위협의 범위와 정교함을 따라잡을 수 없었습니다.

원래 온프레미스 서버용으로 구축된 수동 규칙 집합과 정책을 지속해서 업데이트하면 SEG를 유지 관리하는 데 드는 시간과 노력만 늘어납니다. 이는 비용과 복잡성의 증가를 가져올 뿐이며, 비즈니스 이메일 손상(BEC) 공격 등 가장 위험한 위협을 잡아내기에는 여전히 미흡합니다. 오버헤드 증가와 효율성 감소의 원인은 다음과 같습니다.

- **새롭게 등장하는 피싱 전술 및 zero-day 위협** - 최신 피싱 공격은 정적 필터와 기존 제어를 회피하기 위해 점점 더 교묘한 전술을 채택하고 있습니다. 따라서 손상 지표가 알려지지 않은 새로운 위협을 SEG가 차단하기가 어렵게 됩니다.
- **복잡한 배포** - SEG가 새롭게 등장하는 위협에 적응하도록 하려면 광범위한 구성과 지속적인 조정이 필요하며, SEG의 기능을 완전히 활용하려면 여러 추가 모듈이 필요합니다.
- **시간이 걸리는 사고 대응** - 의심스럽거나 악의적인 활동이 배포된 SEG 제어 기능을 우회하는 경우, 인터페이스와 워크플로우의 패치워크로 인해 조사 및 대응 프로세스가 길어지고 까다로워질 수 있습니다.

효율이 좋은 로우 터치 보호 기능 배포

하이브리드 근무 인력과의 커뮤니케이션 및 협업을 위해 조직에서 지속해서 Microsoft 365를 채택함에 따라, Microsoft의 기본 보안 기능을 활용하는 동시에 머신 러닝 기반 솔루션과의 상호 보완적인 통합으로 가장 위험한 위협을 자동으로 차단하고 격리시키는 것이 아주 중요해졌습니다. 이러한 전략은 피싱 위험을 비약적으로 감소시킬 뿐만 아니라 워크플로우도 간소화하여 지속적인 보안 관리에 드는 시간과 노력을 최소화합니다.

91%

피싱 이메일로 시작되는 사이버 공격의 비율[1]

#1

사기를 저지르고 액세스를 확보하기 위한 공격 벡터[2]

$500억

지난 10년간 BEC 공격으로 발생한 손해[3]

$488만

2024년 데이터 유출로 인한 평균 비용[4]

1. 2020 Deloitte 조사
2. Microsoft SIR Report
3. 2023 FBI IC3 PSA
4. 2024 IBM Cost of a Data Breach

Microsoft의 이메일 보안 기능

SEG 중복을 제거하여 위험 및 비용 절감

분석가들은 기능을 통합하여 중복되는 기능을 최소화하면 조직의 비용과 복잡성을 줄이는 데 도움이 된다는 것에 동의합니다. 그러나 분석가들은 또한 조직에서 모든 사용 사례를 충족하는지 확인하기 위해 기본 기능을 신중하게 평가할 것을 권고합니다.

Microsoft에서는 필수적인 이메일 보안 기능을 계속해서 구축해 나가면서 SEG와의 기능 중복이 늘어났고, 이로 인해 조직에서는 E3 또는 E5 라이선스에 이미 포함되어 있는 기능을 활용하여 보안 운영을 간소화할 기회를 얻게 되었습니다. 이러한 변화를 통해 조직에서는 복잡하고 비용이 많이 드는 SEG 배포를 없애고 해당 예산의 일부를 가장 위험한 피싱 위협에 효과적으로 대응하는 경량 솔루션 통합에 사용할 수 있습니다.

Cloudflare Email Security는 머신 러닝 위협 분석 사용으로 Microsoft 365를 보강하여 BEC 및 멀티 채널 공격 감지를 자동화하는 통합 로우 터치 솔루션을 제공합니다.

SEG 기능이 중복되는 영역에는 다음이 포함됩니다.

- **이메일 위생**
  스팸 및 대량 메시지에 대한 규칙 기반 정책과 알려진 맬웨어에 대한 서명 기반 감지 기능을 제공합니다.
- **URL 및 첨부 파일 보호**
  모든 이메일 링크에 대한 기본 재작성 및 첨부 파일에 대한 샌드박싱 기능을 제공합니다.
- **조사 및 위협 추적**
  이메일 검색, 사고 조사 및 상관관계, 추적, 복원을 제공합니다.
- **정보 보호**
  이메일, 파일, 엔드포인트에 대한 암호화, 아카이빙, DLP 정책을 제공합니다.
- **인식 및 훈련**
  최종 사용자를 위한 피싱 공격 시뮬레이션 및 훈련을 제공합니다.

Exchange Online 보호

모든 요금제에 포함되어 있으며 대량, 스팸, 맬웨어를 필터링하는 필수 이메일 위생 기능을 제공합니다.

- 스팸 방지
- 서명 기반 맬웨어 보호

Microsoft Purview (DLP)

구성 가능한 데이터 손실 방지 규칙 및 시행. Microsoft Information Protection과 통합됨.

- 이메일 및 파일을 위한 DLP
- 팀을 위한 DLP
- 엔드포인트를 위한 DLP

Defender for O365 Plan 1

악의적 링크 및 첨부 파일에 대한 기본적인 보호를 위한 추가 보안 제어 기능.

- 안전한 링크(URL 재작성)
- 안전한 첨부 파일(샌드박싱)
- 내부 이메일 보호

Defender for O365 Plan 2

Plan 1의 모든 기능 및 위협 추적, 조사, 훈련, 대응을 위한 추가적인 기능을 포함.

- 위협 추적
- 도메인 간 사고 상관관계
- 사이버 공격 시뮬레이션 훈련

E3 라이선스

E3 라이선스 + 규제 준수

E3 라이선스 + 규제 준수 + 보안

E5 라이선스

● 완전 ● 제한적 ● 없음

		SEG	M365	Cloudflare
위협 방지	허용/차단 목록	●	●	●
	알려진 악의적 발신자	●	●	●
	알려진 악의적 URL/첨부 파일	●	●	●
	스팸/대량 필터링	●	●	●
	머신 러닝(콘텐츠 분석)	●	●	●
	Zero-Day 맬웨어/랜섬웨어	●	●	●
	악의적 링크	●	●	●
	URL 재작성(클릭 시간 분석)	●	●	●
	적응형 링크 격리	●	●	●
	비즈니스 이메일 손상(BEC)	●	●	●
	직원 가장	●	●	●
	벤더 가장	●	●	●
	직원 손상(ATO)	●	●	●
	벤더 손상	●	●	●
	DMARC 관리	●	●	●
	악의적 애플리케이션 감지(OAuth 피싱)	●	●	●
	웹 콘텐츠 보안	●	●	●
	보안 인식 및 훈련	●	●	●
위협 대응	직관적인 단일 인터페이스	●	●	●
	자동화된 위협 분류	●	●	●
	빠른 검색 및 조사	●	●	●
	자동 철회	●	●	●
	온디맨드 보고	●	●	●
	관리형 감지 및 대응 서비스	●	●	●
데이터 보호	암호화	●	●	●
	아카이빙	●	●	●
	이메일 DLP	●	●	●
	클라우드 DLP(협업 애플리케이션)	●	●	●
	네트워크 DLP	●	●	●

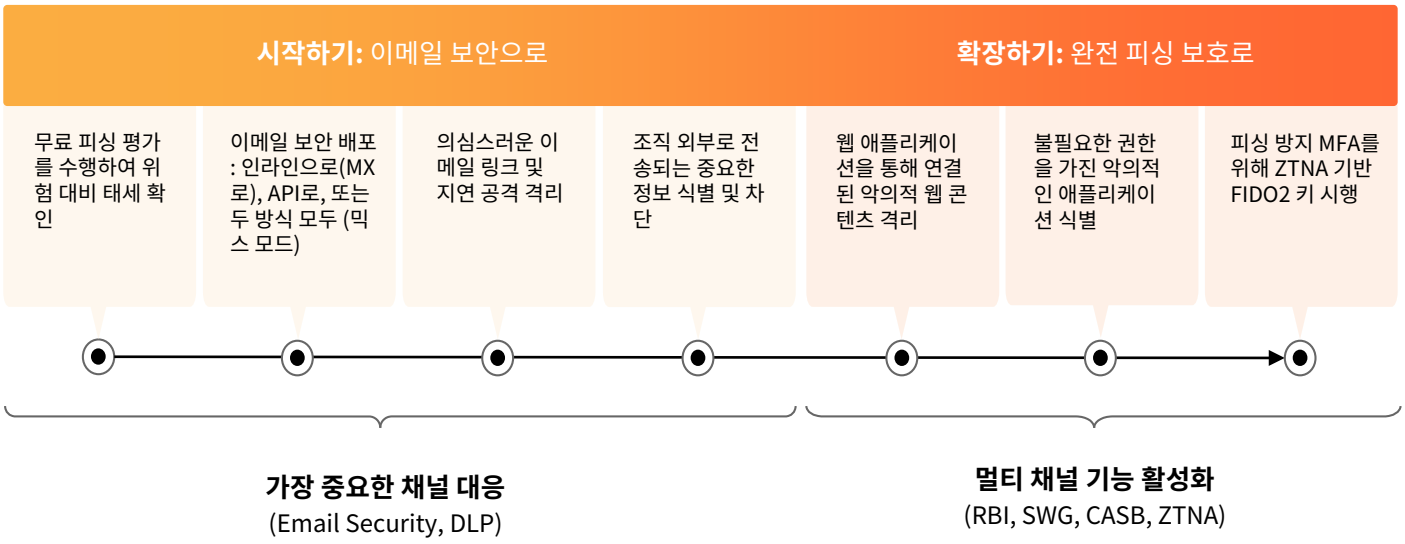
이점

완벽한 멀티 채널 보호

피싱 캠페인이 이메일을 넘어 빠르게 확장되면서, 조직에서 빠르고 간단한 경로로 완전한 멀티 채널 보호를 제공하는 피싱 솔루션을 구현하는 것이 그 어느 때보다도 시급해졌습니다.

조직에서는 Cloudflare의 통합 보안 플랫폼을 사용하여 먼저 업계 최고의 이메일 보안을 배포하여 가장 중요한 피싱 채널에 빠르게 대처한 후, Zero Trust 서비스를 쉽게 활성화하여 모든 채널에 보호 기능을 확장함으로써 알려진 신흥 피싱 위협을 효과적으로 차단할 수 있습니다.

- **효율이 좋은 로우 터치 보호 기능:**
  업계 최고의 감지 기능을 사용하여 최소한의 조정만으로 피싱 위협을 최소화합니다.
- **더 큰 통합, 더 낮은 비용:**
  모든 피싱 사용 사례를 해결하는 완전 통합 단일 플랫폼으로 지출을 줄입니다.
- **빠른 배포, 손쉬운 관리:**
  즉각적인 보호를 보장하는 동시에 지속적인 관리에 필요한 시간과 노력을 줄입니다.



평가 및 비교

현재 사용하고 있는 이메일 보호 기능을 평가하고 어떤 위협을 놓치고 있는지 확인

몇 분 동안 무료 레트로 스캔을 실행하여 지난 14일 동안 어떤 피싱 위협이 들어왔는지 확인하거나, PRA(피싱 위험 평가)를 요청하여 받은 편지함에서 피싱을 받고 있는지 모니터링하세요. 즉시 사용 가능하며 조정이 필요 없는 다른 공급자와 비교해보고 어떤 이메일 보안 솔루션이 가장 빠르고 가장 간편한 보호 기능을 제공하는지 평가해 보세요.

레트로 스캔 실행 | PRA 요청