

Proofpoint Collaboration Security Prime

AI 시대를 위한 완벽하고 지속적인
협업 보안

주요 내용

- 99.999% 효율로 가장 광범위한 위협 차단
- 이메일, 기타 벡터, 또는 침해된 공급업체로부터 시작된 위협인지 여부와 관계없이 몇 분 만에 계정 침해 차단
- 배포 후 6개월 이내에 실제 악성 링크 클릭 40% 감소
- 사칭을 차단하고 유사 도메인이 고객에게 도달하기 전에 폐쇄
- 플랫폼 통합을 통해 총 소유 비용 40% 절감

이 솔루션 세트는 Proofpoint의 통합 Human-Centric Security 플랫폼의 일부이며 에이전트형 업무 공간에서 사람과 데이터를 보호합니다.

개요

AI는 모든 사람을 위한 환경을 변화시켰습니다. 공격자들은 이를 사용하여 더 새롭고 개인화된 공격을 더 정교하고 대규모로 수행하고 있습니다. BEC(비즈니스 이메일 사기 공격)와 같은 캠페인은 27% 증가했으며, AI가 생성한 피싱은 기존 피싱보다 4.5배 더 높은 클릭률을 기록하고 있습니다. 사용자는 AI가 생성한 콘텐츠에 더 취약해졌고, 방어자는 경고 분류와 파편화된 도구로 인해 압도당하고 있습니다.

조직은 에이전트 시대를 위해 구축된 근본적으로 다른 접근 방식이 필요합니다. 이 시대에는 AI 기반 도구와 어시스턴트가 이메일, 메시징, 클라우드 앱 전반에서 확장된 인력에 합류하여 공격자가 이미 악용하고 있는 공격 표면을 확장하고 있습니다.

불행히도, 많은 조직은 보안에 대해 분산된 단일 제품 중심의 접근 방식을 취할 수밖에 없습니다. 하지만 이는 방어 체계에 추가적인 허점을 만들고, 팀 간의 장벽을 높이며, 운영 복잡성을 증가시킵니다.

오늘날 다양한 채널과 단계에 걸쳐 발생하는 AI 기반 확장 공격으로부터 조직을 방어하고, 사람 간, 인간과 AI 도우미 간, 인간과 클라우드 응용 프로그램 간의 신뢰할 수 있는 상호 작용을 보호하기 위해서는 종합적인 접근 방식이 필요합니다. Proofpoint Collaboration Security Prime이 도움을 드릴 수 있습니다. Proofpoint Prime은 에이전트형 업무 공간에서 위협 감지와 대응을 통합합니다.

다음과 같이 지원합니다.

- 공격 표면 전반에 걸친 더 뛰어난 가시성으로 AI가 생성한 새로운 위협을 더 빠르게 탐지합니다.
- 업계 최고의 정확도와 낮은 오탐률로 확실하게 차단합니다.
- 배송 전, 배송 후, 브라우저 및 에이전트 커버리지 전반에 걸쳐 지속적인 보호를 제공합니다.
- 채팅, 앱, 에이전트 등 비즈니스 커뮤니케이션이 이루어지는 모든 곳을 보호합니다.
- 계정 침해를 며칠이 아닌 몇 분 만에 차단합니다.

더 뛰어난 가시성으로 새로운 위협을 더 빠르게 탐지

AI가 생성한 새로운 공격은 기존 방어 체계가 따라잡을 수 없을 정도로 빠르게 움직이고 있습니다. 그 결과, 기존 필터를 우회하여 이메일, 협업 플랫폼, 클라우드 애플리케이션 전반에서 사용자에게 도달하고 있습니다.

Proofpoint Collaboration Security Prime은 이메일 배송 전부터 배송 후 아키텍처까지, 그리고 클릭 시점부터 로그인까지, 사람들이 일하는 모든 채널에서 전체 위협 수명 주기에 걸친 지속적인 보호를 통해 이러한 격차를 해소합니다.

Prime은 다음을 포함하여 가장 광범위한 위협으로부터 보호합니다.

- 자격 증명 피싱 및 콜백 피싱을 포함한 고급 피싱
- BEC 및 CEO 사칭
- 멀웨어 전달
- QR 코드 공격
- 전화 지향적 공격 전송(TOAD)
- 이메일 폭탄 공격
- 랜섬웨어
- 계정 탈취
- 정상적인 서비스 악용
- AI 생성 공격 및 AI 악용 기술(예: 프롬프트 인젝션)

이 보호의 핵심은 업계에서 가장 진보된 탐지 엔진인 Proofpoint Nexus® AI입니다. 업계 최대 규모의 데이터 세트 중 하나로 학습된 Nexus AI는 메시지당 1,000개 이상의 속성을 평가합니다. 언어 모델, 관계 그래프, 머신 러닝, 위협 인텔리전스, 컴퓨터 비전 등 5가지 모델 유형을 결합하여 함께 작동하며 모든 판정 결과로부터 지속적으로 학습합니다.

그 결과 99.999%의 탐지 효율성과 업계 최저 수준의 오탐률을 기록하여, 보안 팀이 불필요한 정보에 파묻히지 않고 실제 위협을 차단할 수 있습니다.

계정 침해로부터 방어

계정 침해는 피싱 이메일에만 국한되지 않습니다. AI는 위협 행위자가 받은 편지함을 넘어 자격 증명 공격을 쉽게 확장하도록 돕고 있으며, 설득력 있고 정교한 가짜 로그인 페이지 생성부터 자동화된 프롬프트 폭탄을 통한 다중 인증 무력화까지 가능하게 합니다.

협업 중심의 에이전트 지원 업무 환경에서는 침해 전, 침해 중, 침해 후 등 모든 단계에서 이러한 위협을 차단하는 것이 중요합니다.

Proofpoint Collaboration Security Prime은 침해가 발생하기 전에 예방하도록 돕습니다. Prime의 SSO Password Guard는 직원이 기업용 비밀번호를 비기업용 사이트에서 재사용할 때 이를 감지하여 자격 증명 기반 공격의 가장 흔한 진입점 중 하나를 차단하고, 이메일을 넘어 브라우저 자체까지 보호 범위를 확장합니다.

예방만으로 충분하지 않을 때, Prime은 침해가 발생하는 즉시 이를 감지합니다.

Microsoft 365, Google Workspace 및 Okta 전반의 ID 및 액세스 후 신호를 상호 연관시켜 침해 징후가 있는 계정을 식별합니다.

침해가 식별되면 Prime은 며칠이 아닌 몇 분 만에 조사 및 봉쇄를 지원하여 공격자가 환경 내부로 더 이동하기 전에 피해 범위를 제한합니다.

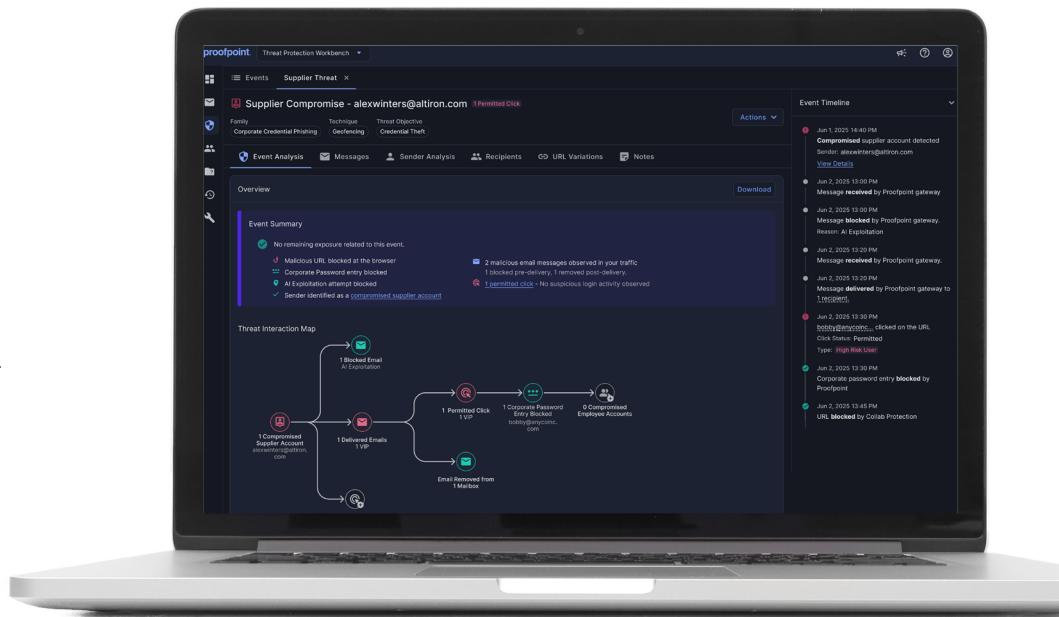


그림 1. Proofpoint Collaboration Security Prime은 이메일, 메시징 및 협업, 클라우드 및 공급업체 채널에서 위협을 차단하고 연계 분석합니다.

Nexus® AI 모델은 사이버 보안 분야에서 가장 크고 다양한 데이터 세트 중 하나를 바탕으로 학습되었습니다.

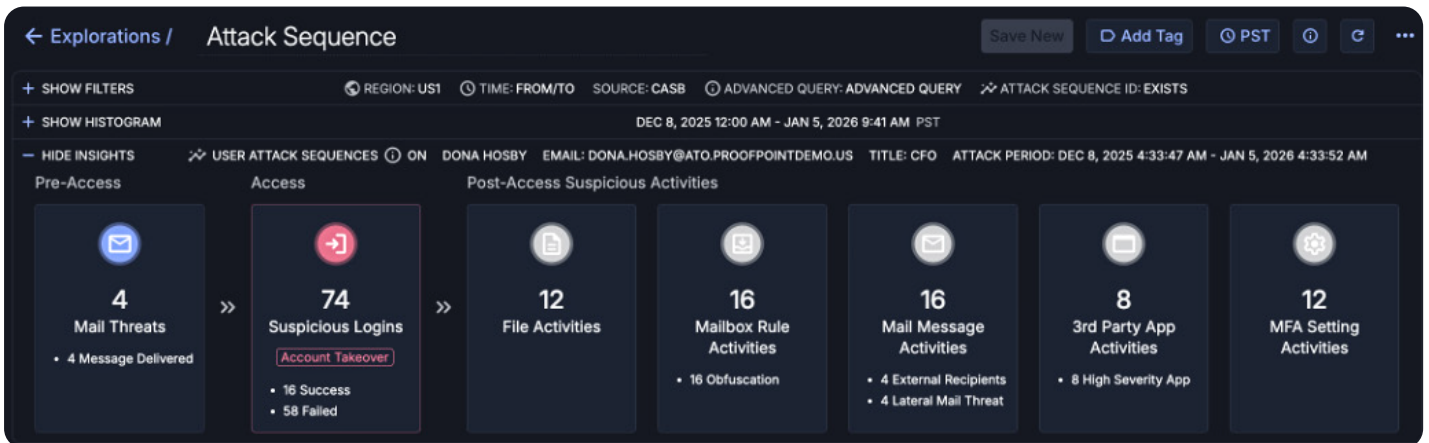


그림 2. Proofpoint Collaboration Security Prime은 공격 시퀀스에 대한 가시성을 제공하고 진압을 자동화합니다.

신뢰할 수 있는 비즈니스 커뮤니케이션 보호

공격자는 직접적인 도메인 스푸핑, 유사 도메인 또는 침해된 공급업체 계정을 통해 신뢰할 수 있는 비즈니스 커뮤니케이션에 개입하기 위해 사칭 전술을 자주 사용합니다. 귀하의 조직이나 파트너가 사칭당하거나 침해당하면 직원과 고객이 위험에 처하게 되며, 브랜드에 심각한 피해를 줄 수 있습니다.

Proofpoint Collaboration Security Prime이 이러한 사칭 위험을 사전에 완화할 수 있도록 도와드리겠습니다. 이 솔루션은 제3자가 보낸 이메일을 포함하여 신뢰할 수 있는 도메인을 통해 전송되는 모든 이메일에 대한 완전한 가시성을 제공합니다. 강력한 도구에 액세스하고, 모든 이메일 인증률 아웃 단계를 안내해 줄 전문 컨설턴트의 도움도 받을 수 있습니다. 이를 통해 DMARC 규정을 완벽하게 준수하고 공격자의 도메인 스푸핑을 차단할 수 있습니다.

Proofpoint의 보호는 사용자 생성 이메일 및 그 외 영역으로 확장하여 응용 프로그램 생성 메시지와 제3자 SaaS 공급업체가 고객을 대신하여 보내는 이메일을 모두 전달하는 안전한 전용 환경을 포함합니다.

공급업체 위험과 관련하여 Proofpoint Prime은 침해된 제3자 계정을 이용하는 공격자로부터 직원을 보호합니다. 공급업체 계정에서 발생하는 의심스러운 활동을 식별하고 경고 표시 및 URL 격리와 같은 적응형 보호 기능을 적용하여 정상적인 비즈니스 커뮤니케이션을 방해하지 않으면서 위험을 줄입니다.

또한 Proofpoint Prime은 고급 유사 도메인 검색 기능을 제공합니다. Proofpoint Prime은 인터넷에서 고객의 도메인과 매우 유사한 도메인을 동적으로 모니터링합니다. Proofpoint Prime은 등록 세부 정보 및 잠재적 오용에 대한 자세한 인사이트를 제공합니다.

당사는 단순히 탐지에만 그치지 않습니다. 당사는 등록 기관, 호스팅 공급업체 및 최상위 도메인(TLD) 인증 기관과의 긴밀한 관계를 활용하여 고객을 대신하여 악의적인 도메인 및 URL을 차단하는 노력을 할 수 있습니다. 저희 전문가가 전체 프로세스를 관리하므로, 귀사의 팀은 핵심 비즈니스 운영에 집중하실 수 있습니다.

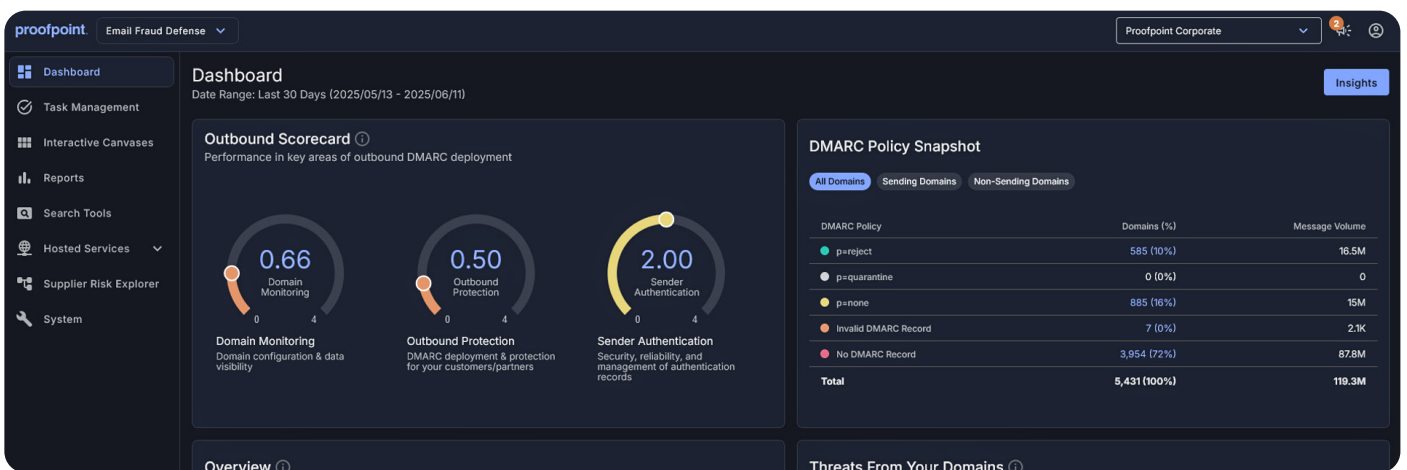


그림 3. Proofpoint Collaboration Security Prime은 도메인 스푸핑, 악성 유사 도메인과 같은 사칭 위협에 대한 가시성을 제공합니다.

위험 기반 지침으로 인적 탄력성 강화

업무가 더욱 협업적이고 동적으로 변화하면서 사람들은 사이버 공격에 대한 회복 탄력성을 강화해야 합니다. 이를 위해 규정 준수 중심의 교육에서 벗어나 인적 위험 관리로 나아가야 합니다. 실시간 교육은 사용자의 업무 방식과 직면하는 실제 위험을 반영합니다.

Proofpoint Collaboration Security Prime은 일회성 교육이 아닌 실제 위험과 연계된 지속적인 주기를 통해 체계적으로 인간의 회복탄력성을 구축합니다.

이는 타겟팅에서 시작됩니다. Human Resilience Workbench는 플랫폼 전반에서 행동 및 위험 신호를 수집하여 고위험 사용자, 신규 입사자, 반복 클릭 사용자를 자동으로 식별하므로, 보안 팀이 가장 중요한 곳에 집중할 수 있도록 합니다.

그 다음, Prime은 위험이 가장 높은 순간에 더 안전한 행동을 강화합니다. AI 기반 ThreatFlip을 활용하여 실제 활성 위험을 즉시 원클릭 시뮬레이션으로 전환함으로써, 직원들이 일반적인 교육 모듈에서 몇 주 뒤에 배우는 것이 아니라 공격을 경험한 직후에 공격이 어떤 모습인지 정확히 확인할 수 있도록 합니다.

마지막으로, Prime은 그 효과를 입증합니다. 위험 점수와 벤치마킹을 통해 관리자는 행동이 개선되는 부분과 여전히 격차가 존재하는 부분을 명확하게 파악할 수 있습니다. 이 접근 방식을 사용하는 조직은 6개월 이내에 실제 악성 링크 클릭이 40% 감소하는 것을 경험하며, 이는 단순한 인식이 아닌 회복탄력성이 지속적인 변화를 이끌어낸다는 증거입니다.

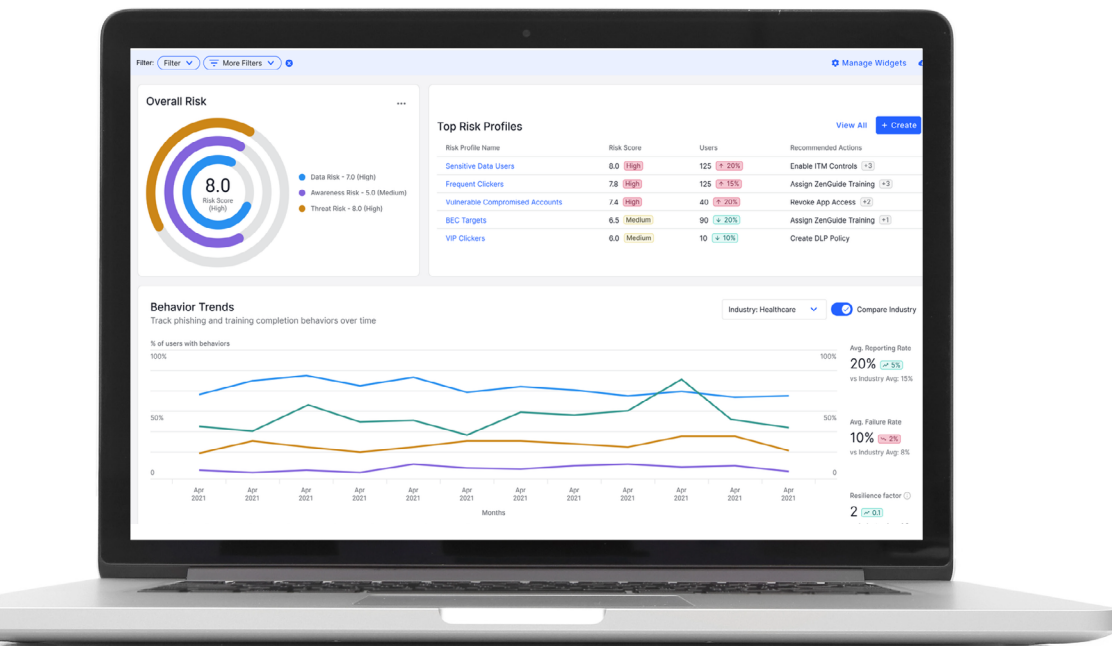


그림 4. Proofpoint Collaboration Security Prime은 실제 사용자 행동에 대한 가시성을 제공하여 맞춤형 위험 기반 학습을 가능하게 합니다.

보안 운영 간소화

위협이 이메일을 넘어 협업 도구, 클라우드 플랫폼, 공급업체 에코시스템으로 확대되면서 보안 팀은 적은 자원으로 더 많은 성과를 달성해야 한다는 압박을 받고 있습니다. 이러한 환경에서는 단편적인 솔루션으로는 상황이 나아지지 않습니다. 복잡성을 증가시킬 뿐만 아니라, 응답 시간을 늦추고 운영 비용을 상승시킵니다. 이러한 모든 요소는 위협을 대폭적으로 줄이는 것을 어렵게 만듭니다.

Proofpoint Collaboration Security Prime은 위협 탐지와 조사를 통합하고 워크플로 및 대응을 자동화하여 보안 운영을 간소화합니다. Threat Protection Workbench는 기본 통합을 활용하여 이메일, 메시징, 협업 플랫폼, 클라우드 계정 및 공급업체 에코시스템에서 탐지 인사이트와 공격 포렌식을 결합합니다. 팀은 단일의 통합된 업무 공간에서 사고를 조사하고 결정적인 조치를 취하여 효율성을 극대화할 수 있습니다.

또한 Proofpoint Prime은 팀이 효과적으로 우선순위를 지정할 수 있도록 지원합니다. Threat Interaction Map은 제어 지점에서 위협 및 보안 이벤트를 연계 분석하여 공격 경로를 시각적 맵으로 보여줍니다. 이를 통해 분석가는 가장 중요한 사고를 신속하게 파악할 수 있습니다. 동시에 사용자 보고 메시지를 자동으로 검사하고 악성 콘텐츠를 수습하며 사용자에게 피드백을 제공합니다. 그 결과, 수작업이 감소하면서 안전한 사용자 행동이 강화됩니다.

그 결과 응답 속도가 빨라지고 운영 복잡성이 줄어듭니다. 그리고 귀하의 보안팀은 보호를 희생하지 않으면서 더 적은 자원으로 더 많은 일을 할 수 있습니다.

적절한 보호 수준 선택

Proofpoint Collaboration Security Prime은 여러 계층으로 제공됩니다. 이를 통해 귀하는 조직의 위협 프로필 및 운영 요구 사항에 맞춰 보호를 조정할 수 있습니다. 각 계층은 이전 계층을 기반으로 구축됩니다.

핵심 이메일 위협에서 협업 채널, 계정 침해, 인적 위협 감소 및 고급 브랜드 보호까지 적용 범위가 확대됩니다.

사용 가능한 기능은 다음
페이지를 참조하십시오.



자세히 알아보기: proofpoint.com/kr

Proofpoint, Inc. 소개 Proofpoint, Inc.는 사람 중심 및 에이전트 중심의 사이버 보안 분야의 글로벌 리더로서 이메일, 클라우드 및 협업 도구 전반에 걸쳐 사람, 데이터 및 AI 에이전트가 연결되는 방식을 보호합니다. Proofpoint는 Fortune 100대 기업 중 80개 이상, 10,000개 이상의 대기업, 그리고 수백만 개의 소규모 조직이 위협 차단, 데이터 손실 방지, 그리고 사람 및 AI 워크플로우 전반에 걸친 회복력 구축을 위해 선택한 신뢰받는 파트너입니다. Proofpoint의 협업 및 데이터 보안 플랫폼은 모든 규모의 조직이 AI를 안전하고 자신감 있게 채택하면서 직원을 보호하고 역량을 강화할 수 있도록 도와줍니다. 자세히 알아보기: www.proofpoint.com/kr

Proofpoint에 문의하기: [LinkedIn](#)

Proofpoint는 미국 및/또는 기타 국가에서 Proofpoint, Inc.의 등록 상표 또는 상표입니다. 여기에 포함된 모든 다른 상표는 해당 소유주의 재산입니다.

모든 Proofpoint Collaboration Security 솔루션 등급은 SEG 및 API 배포 환경 모두에서 사용할 수 있습니다. 기능의 이용 가능 여부는 배포 모델에 따라 다를 수 있습니다.

	사용 가능한 기능	Proofpoint Core Email Protection	Proofpoint Collaboration Security 계층 2	Proofpoint Collaboration Security 계층 3	Proofpoint Collaboration Security Prime
이메일 보안	BEC, 피싱, 콜백 피싱 및 멀웨어 방지	✓	✓	✓	✓
	Nexus AI 기반 다중 계층 탐지 스택	✓	✓	✓	✓
	280만 명 이상의 고객으로부터 수집한 비교할 수 없는 위협 데이터	✓	✓	✓	✓
	첨부 파일 및 URL 샌드박스	✓	✓	✓	✓
	URL 다시 작성 및 클릭 시간 샌드박스	SEG	SEG	SEG	SEG
	다시 작성된 URL에 대한 의심스러운 클릭 격리	VAPS*	모든 사용자*	모든 사용자*	모든 사용자*
	스팸 방지 및 협박 메일 탐지	✓	✓	✓	✓
	상황별 이메일 경고 태그	✓	✓	✓	✓
	적응형 이메일 건전성은 사용자 행동을 기반으로 자체 학습함	✓	✓	✓	✓
	구성 가능한 메일 라우팅 정책	SEG	SEG	SEG	SEG
	자동화된 메시지 수습	✓	✓	✓	✓
	악용 메일함 자동화	✓	✓	✓	✓
	VAP(Very Attacked People)™, 위협 행위자 및 글로벌 인텔리전스	✓	✓	✓	✓
	침해된 클라우드 계정 탐지 및 수정		✓	✓	✓
다중 채널, 다단계 위협 방지	메시징 및 협업 응용 프로그램을 통해 전송되는 악성 URL 차단		✓	✓	✓
	위험하거나 승인되지 않은 웹사이트에서 발생하는 기업 암호의 오용 탐지		✓	✓	✓
	침해된 공급업체 계정 보호		✓	✓	✓
	자동화된 위협 기반 교육으로 사용자 안내			✓	✓
인적 탄력성 및 보안 인식	실제 위협 기반 시뮬레이션으로 직원 인식 제고			✓	✓
	활성 위협을 안전한 시뮬레이션으로 변환			✓	✓
	행동, 위협 원격 측정 및 역할을 기반으로 위협에 처한 사용자 탐지 및 우선순위 지정			✓	✓
	이메일 인증을 통해 브랜드 악용 방지				✓
사칭 방지	악성 유사 도메인 탐지 및 수정				✓
	보안 응용 프로그램 이메일 릴레이(250GB)				✓

SEG = 보안 이메일 게이트웨이 배포 전용

* = SEG 배포에서만 사용 가능.