

보안 모듈

비즈니스에 가장
필요한 영역까지 보안을
확장하세요

Kaspersky Next Optimum용





Kaspersky Next Optimum은 중소기업에 최적화된 맞춤형 보안 솔루션입니다. 강력한 엔드포인트 보호를 기반으로 엔드포인트 탐지 및 대응 기능까지 제공하며, 더욱 고도화된 사이버 보안이 필요할 때 필수적인 XDR 또는 MXDR로 원활하게 업그레이드할 수 있습니다.

보안 모듈로 특정한 보호 영역을 집중적으로 강화하세요

비즈니스가 성장하면 공격 표면도 함께 넓어집니다. 새로운 직원과 도구, 환경, 이메일 흐름, 도메인, 디지털 서비스는 모두 공격자에게 새로운 침투 기회를 제공할 수 있습니다.

보안 모듈을 사용하면 기존 설정을 교체하거나 불필요한 복잡성을 높이지 않고도, 필요에 따라 Kaspersky Next Optimum에 원하는 보안 기능을 추가할 수 있습니다.

비즈니스가 변화하면 보안 요구 사항도 달라집니다

각 모듈은 현재 보유한 내부 전문 역량과 비즈니스 우선순위, 필요한 보호 수준에 따라 단계적으로 추가할 수 있습니다.

워크로드 보안



가장 중요한 영역에 보호 기능 추가



보안 인식

직원을 또 하나의 방어선으로 활용

- 보안 인식 교육 및 피싱 시뮬레이션
- 역할 기반 사이버 보안 교육



이메일 보안

이메일 위협이 사용자에게 도달하기 전에 차단

- 민감한 데이터 보호 및 제어
- 이메일 인프라 전반의 완전한 가시성



워크로드 보안

하이브리드 클라우드 환경 보호

- 글로벌 및 현지 규제 요건 준수
- 오탐을 최소화하는 다계층 보호



위협 조회 및 분석

위협 조사 및 분석 강화

- 의심스러운 파일과 개체를 분석하는 클라우드 샌드박스
- 위협 인텔리전스 조회 및 IoC 가시성



취약점 관리

인프라 전반의 취약점 식별 및 해결

- 자산과 취약점 가시성 확보 및 제어
- 더욱 신속한 대응과 취약점 해결 평균 시간 단축

유연한 보호 기능으로 보안 역량 강화



실제 비즈니스 여건을 고려한 설계

각 모듈은 중소기업의 우선순위와 리소스, 보안 과제에 맞춰 설계되었습니다.



손쉬운 보호 범위 확장

Kaspersky Next Optimum 신규 및 기존 고객을 위한 특별 혜택



간편한 보안 운영

불필요한 복잡성과 과도한 솔루션 배포 최소화



중요한 정보에 집중

비즈니스에 가장 중요한 영역 집중 강화



단계적 확장

새로운 위협이 등장할 때마다 보호 기능 강화

주요 보안 과제에 대한 보안 모듈의 대응 방식



보안 인식



이메일 보안



워크로드 보안



취약점 관리



위협 조회 및
분석



피싱 및 소셜
엔지니어링



민감한 데이터 노출



알 수 없거나 의심스러운
파일



하이브리드 환경 노출



취약점 및 잘못된 구성



[※] 외부 위협 가시성



자세히 보기

www.kaspersky.co.kr

© 2026 AO Kaspersky Lab.
등록 상표 및 서비스 마크는 각 소유자의 재산입니다.

#kaspersky
#truetobusiness