Trang bị cho doanh nghiệp đang phát triển của bạn khả năng bảo mật mở rộng hiệu quả, thân thiện với người dùng và tiết kiệm chi phí

Kaspersky Next XDR Optimum

kaspersky khai mở tương lai

Dành cho doanh nghiệp vừa và nhỏ

Kaspersky Next XDR Optimum dành cho các doanh nghiệp vừa và nhỏ có cơ sở hạ tầng CNTT có sẵn và ngân sách bảo mật mạng hợp lý. Cho dù là bảo mật do nhóm CNTT lớn quản lý hay do một nhóm nhỏ chuyên trách quản lý, giải pháp này cung cấp các công cụ dễ quản lý, mang đến khả năng bảo vệ mạnh mẽ, toàn diện mà không làm quá tải tài nguyên hiện có.

Tận dụng tối đa các nguồn lực và tăng hiệu quả ứng phó sự cố của bạn

Những mối đe dọa mạng nhắm vào doanh nghiệp vừa và nhỏ đang phát triển ngày càng tinh vi và dữ dội. Kẻ tấn công ngày càng khai thác công cụ hệ thống hợp pháp và các kỹ thuật tiên tiến để tránh bị phát hiện. Trong khi đó, nhân viên không nhận thức được rủi ro bảo mật mạng dễ bị tấn công lừa đảo và tấn công phi kỹ thuật, gây thiệt hại về tài chính và danh tiếng.

Đồng thời, nguồn lực hạn chế, bao gồm ngân sách eo hẹp và thiếu nhân viên có kỹ năng khiến việc bảo vệ trước những mối đe dọa này trở nên khó khăn hơn. Đó là lý do điều cần thiết là phải có các công cụ tiên tiến nhưng dễ sử dụng để cung cấp mức độ bảo vệ phù hợp cho doanh nghiệp của bạn.

Mở rộng khả năng bảo mật của bạn bằng Kaspersky Next XDR Optimum

Được thiết kế cho các nhóm bảo mật quy mô nhỏ, giải pháp này tăng cường ứng phó sự cố và xây dựng chuyên môn mà không phải phải đảm nhận thêm gánh nặng từ các tác vụ tốn thời gian. Với nhiều quy trình được tự động hóa, đội ngũ của bạn có thể tập trung nhiệm vụ quan trọng nhất.

Kaspersky Next XDR Optimum tích hợp dễ dàng vào cơ sở hạ tầng hiện có của bạn mà không cần thêm các thành phần hệ thống mới.

Phát hiện, phân tích và phản hồi

- Phát hiện hành vi
- Tổng hợp cảnh báo
- Cloud Sandbox
- Phát hiện bằng chứng mối đe dọa (IoC) và IoC tùy chỉnh
- Phân tích nguyên nhân gốc rễ
- Một loạt hành động ứng phó

Tính năng bảo vệ điểm cuối

- Chống phần mềm độc hại nâng cao
- Tăng cường mở rộng
- Đánh giá lỗ hổng bảo mật
- Kiểm soát người dùng cuối
- Bảo vệ dữ liệu
- Quản lý bản vá

Từ khả năng bảo vệ điểm cuối và bảo mật đám mây có một không hai cho đến tự động hóa tác vụ CNTT và các tính năng XDR thiết yếu:

Giải phóng khả năng **bảo vệ điểm cuối vượt trội**

Tránh gián đoạn kinh doanh nhờ khả năng bảo vệ tự động, được hỗ trợ bởi bộ công cụ chống phần mềm tống tiền và phần mềm độc hại dựa trên ML đã được kiểm chứng trong ngành, nhằm ngăn lây nhiễm từ các mối đe dọa đã biết và chưa biết.

Khắc phục các lỗ hổng bảo mật thông qua việc tăng cường hệ thống và đào tạo

Giảm bề mặt tấn công bằng cách tăng cường hệ thống dựa trên hành vi của người dùng và tiết kiệm thời gian nhờ quản lý lỗ hổng bảo mật, bản vá và mã hóa tập trung. Ngoài ra, chúng tôi còn cung cấp mọi nội dung đào tạo mà nhóm của bạn cần để tận dụng tối đa các khả năng bảo mật mới của mình.

Mở rộng **khả năng phát hiện và phản hồi** của bạn

Có thông tin chuyên sâu về các mối đe dọa và cách chúng di chuyển bên trong và bên ngoài điểm cuối. Sử dụng tự động hóa và phản hồi có hướng dẫn để đối phó với các cuộc tấn công và sử dụng bộ công cụ điều tra thiết yếu để theo dõi hoạt động của chúng.

Đào tạo toàn bộ đội ngũ của bạn để đóng vai trò tích cực trong bảo mật

Trang bị cho đội ngũ CNTT và nhân viên không chuyên về kỹ thuật những kiến thức và kỹ năng để duy trì bảo mật. Tăng cường cho đội ngũ bảo mật CNTT, đồng thời xây dựng văn hóa cao, có ý thức về bảo mật trong lực lượng lao động.

Tận dụng hệ thống dựa trên đám mây của chúng tôi để **xử lý tập tin**

Dễ dàng điều tra tập tin độc hại và thu thập thêm ngữ cảnh và thông tin chi tiết với tích hợp Cloud Sandbox của chúng tôi — tải lên mẫu độc hại tiềm ẩn để kiểm tra danh tiếng của qua vài giây ngay từ giao diện sản phẩm và sử dụng dữ liệu được tạo cho các tác vụ quét IoC sau này.

Kiểm soát CNTT ngầm nhờ bảo mật đám mây mà bạn có thể tin tưởng

Giảm lỗ hổng bảo mật, bảo vệ dữ liệu và nhân viên của bạn bằng cách kiểm soát CNTT ngầm. Xem những dịch vụ đám mây nào đang được sử dụng, chặn truy cập trái phép và xác định những dữ liệu nhạy cảm nào được lưu trữ trong bộ ứng dụng Microsoft 365.

Hưởng lợi từ các **tùy chọn cung cấpkhác nhau**

Giảm tổng chi phí sở hữu nhờ các công cụ tự động hóa và triển khai dựa trên đám mây hoặc cài đặt tại chỗ để kiểm soát toàn diện[1].

[1] Bảng điều khiển quản lý tại chỗ dựa trên Linux. Kaspersky Next XDR Optimum hỗ trợ tất cả các hệ điều hành trên tác nhân điểm cuối và bảng điều khiển đám mây của giải pháp. Tùy chọn triển khai dựa trên đám mây sẽ khả dụng vào quý 4 năm 2025

Kaspersky Next XDR Optimum — thuộc dòng sản phẩm Kaspersky Next của chúng tôi

Kaspersky Next là dòng sản phẩm được phân cấp, dành cho các doanh nghiệp thuộc mọi quy mô. Kaspersky Next Optimum dành cho doanh nghiệp vừa và nhỏ, đội ngũ bảo mật mạng tinh gọn, muốn mở rộng quy mô bảo vệ mà không làm tăng thêm mức độ phức tạp. Giải pháp này có khả năng bảo vệ điểm cuối mạnh mẽ, được tăng cường bởi các tính năng phát hiện và phản hồi điểm cuối, cho phép nâng cấp tiện lợi lên XDR hoặc MXDR thiết yếu để đạt mức độ bảo mật mạng phức tạp.

Vì sao chọnKaspersky Next Optimum?

Được dựa trên giải pháp điểm cuối tốt nhất của chúng tôi

Trong hơn một thập kỷ, các sản phẩm của Kaspersky đã liên tục được xếp hạng hàng đầu trong các bài kiểm tra và đánh giá độc lập. Giải pháp bảo vệ điểm cuối tự động đã được kiểm chứng của chúng tôi giúp giảm số lượng cảnh báo mà các đội ngũ bảo mật cần phân tích, nâng cao hiệu quả của họ.

Dựa trên kiến thức, kỹ năng và chuyên môn sâu

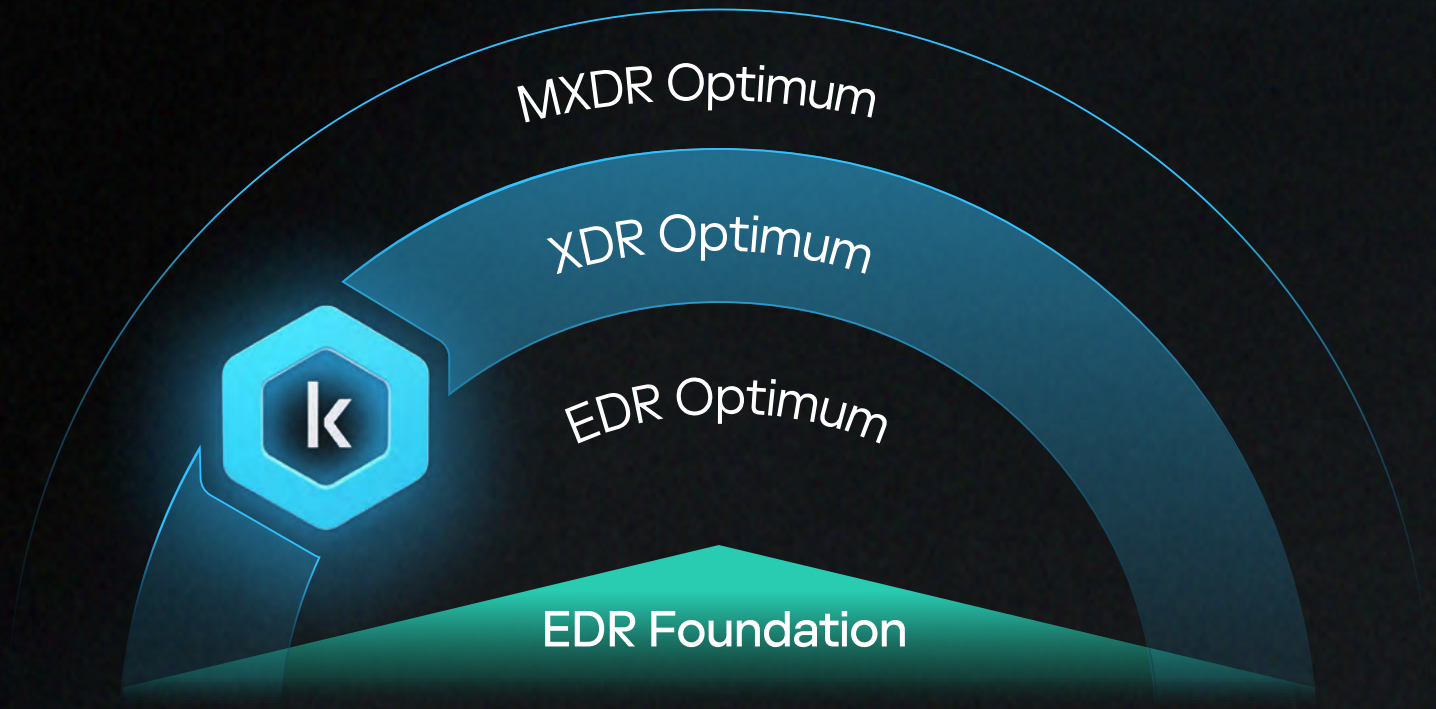
Kaspersky Next được xây dựng dựa trên hàng chục năm tích lũy kinh nghiệm và chuyên môn sâu của các đội ngũ bảo mật toàn cầu của chúng tôi. Đội ngũ chuyên gia của chúng tôi hợp tác để giải quyết các mối đe dọa mạng phức tạp, liên tục tinh chỉnh công nghệ nền tảng cho bộ sản phẩm của chúng tôi. Cách tiếp cận dựa vào chuyên gia này đảm bảo các giải pháp của chúng tôi đáng tin cậy, sáng tạo và phù hợp với nhu cầu bảo mật ngoài đời thực.

Tuyến bảo vệ đa lớp dựa trên công nghệ AI

Kaspersky sử dụng thuật toán dự đoán, phân cụm, mạng nơ-ron, mô hình thống kê và thuật toán cấp độ chuyên gia để tăng tốc độ phát hiện và nâng cao độ chính xác.

Bảo mật mạng phát triển cùng bạn

Kaspersky Next bảo vệ doanh nghiệp thuộc mọi quy mô. Khi nhu cầu tăng lên, bạn có thể dễ dàng mở rộng quy mô từ bảo vệ điểm cuối thiết yếu sang các giải pháp nâng cao, cấp độ chuyên gia có sẵn ở các bậc cao hơn.



www.kaspersky.com.vn/

Tìm hiểu thêm

#kaspersky
#bringonthefuture