



TÀI LIỆU GIẢI PHÁP DÀNH CHO DOANH NGHIỆP VỪA VÀ NHỎ

CROWDSTRIKE FALCON BẢO VỆ MÁY TÍNH VÀ MÁY CHỦ

Triển khai gọn nhẹ • Quản lý tập trung • Giảm gánh nặng cho đội IT

THÔNG điệp CHÍNH

CrowdStrike Falcon giúp doanh nghiệp bảo vệ máy tính và máy chủ mà không phải dựng thêm hệ thống quản lý tại văn phòng. Đội IT theo dõi tập trung, xử lý sự cố nhanh hơn và có thể mở rộng chức năng theo nhu cầu.

KHUYẾN NGHỊ KHỞI ĐẦU Falcon Pro hoặc Falcon Enterprise

ĐỐI TƯỢNG Doanh nghiệp vừa và nhỏ, nhiều chi nhánh, đội IT tinh gọn

PHIÊN BẢN v1.4 - cập nhật 11/09/2026

ĐƠN VỊ BIÊN SOẠN Arbolume

MỤC LỤC • TRA CỨU NHANH

Chọn nội dung cần đọc

Mỗi dòng trong bảng dưới đây có liên kết để chuyển thẳng đến nội dung tương ứng. Người đọc không cần đọc từ đầu đến cuối.

Mục	Nội dung	Đi tới
01	Giá trị dành cho doanh nghiệp	Mở mục
02	Rủi ro doanh nghiệp cần quan tâm	Mở mục
03	Vì sao phần mềm diệt virus chưa đủ	Mở mục
04	Cách CrowdStrike hoạt động	Mở mục
05	Ngăn mã độc và ransomware	Mở mục
06	Phát hiện và xử lý sự cố	Mở mục
07	Quy trình dành cho đội IT	Mở mục
08	Bảo vệ tài khoản người dùng	Mở mục
09	Kiểm tra điểm yếu của tài khoản	Mở mục
10	Tự động hóa có kiểm soát	Mở mục
11	Khi nào cần giám sát 24 giờ	Mở mục
12	Bắt đầu nhỏ và mở rộng khi cần	Mở mục
13	Chọn gói giải pháp	Mở mục
14	Kế hoạch triển khai	Mở mục
A	Thuật ngữ dễ hiểu	Mở mục
B	Nguồn CrowdStrike chính thức	Mở mục

Tra cứu nhanh: [Thuật ngữ dễ hiểu](#) • [Nguồn CrowdStrike chính thức](#)

01 • GIÁ TRỊ DÀNH CHO DOANH NGHIỆP

CrowdStrike Falcon giúp doanh nghiệp giải quyết việc gì

CrowdStrike Falcon bảo vệ máy tính và máy chủ của doanh nghiệp từ một trang quản trị trực tuyến. Doanh nghiệp không phải dựng thêm máy chủ quản lý tại văn phòng. Một chương trình gọn nhẹ được cài trên thiết bị để ngăn mã độc, ghi nhận hành vi đáng ngờ và hỗ trợ đội IT xử lý khi có sự cố. Doanh nghiệp có thể bắt đầu với bảo vệ cơ bản rồi mở rộng khi nhu cầu tăng.

Bài toán	CrowdStrike hỗ trợ như thế nào	Lợi ích đối với doanh nghiệp
Phần mềm diệt virus chỉ tập trung vào file	Xem cả file và hành vi của chương trình	Nhận ra thêm các cuộc tấn công không dùng file mã độc
Cảnh báo thiếu thông tin	Ghi lại chuỗi hoạt động trên thiết bị	Biết sự việc bắt đầu từ đâu và ảnh hưởng tới đâu
Đội IT ít người	Quản lý trên cloud, chính sách tập trung	Giảm máy chủ quản lý và công việc lặp lại
Tài khoản bị lộ	Liên kết rủi ro tài khoản với thiết bị	Hạn chế kẻ tấn công dùng tài khoản thật để di chuyển trong hệ thống

02 • RỦI RO DOANH NGHIỆP CẦN QUAN TÂM

Tấn công hiện nay không chỉ đến từ file chứa mã độc

Kẻ tấn công ngày càng dùng tài khoản bị lộ, công cụ có sẵn trong Windows và các đoạn lệnh nhỏ để tránh bị phần mềm diệt virus phát hiện. Theo Global Threat Report 2026 của CrowdStrike, các số liệu dưới đây phản ánh hoạt động mà hãng quan sát trong năm 2025.

Dấu hiệu CrowdStrike ghi nhận	Số liệu	Điều doanh nghiệp cần lưu ý
Tấn công không dùng file mã độc	82%	Chỉ quét file sẽ bỏ sót nhiều hành vi nguy hiểm.
Thời gian trung bình để kẻ tấn công lan sang hệ thống khác	29 phút	Quy trình báo cáo và cô lập máy phải đủ nhanh.
Trường hợp lan nhanh nhất	27 giây	Các cảnh báo nghiêm trọng cần được ưu tiên tự động.
Hoạt động của đối tượng tấn công có dùng AI	Tăng 89%	Email lừa đảo và kịch bản tấn công có thể được tạo nhanh hơn.
Khai thác lỗ hổng chưa được công bố rộng rãi	Tăng 42%	Cần phát hiện hành vi, không chỉ dựa vào danh sách mối đe dọa đã biết.

KẾT LUẬN	Doanh nghiệp cần một công cụ vừa ngăn chặn tại máy, vừa giúp đội IT thấy toàn bộ diễn biến để xử lý nhanh khi sự cố xảy ra.
----------	---

Ba thay đổi dễ nhận thấy

- Kẻ tấn công có thể dùng công cụ hợp pháp và tài khoản thật, nên việc chỉ quét file là chưa đủ.
- Một sự cố có thể bắt đầu từ máy tính, lan sang tài khoản rồi tiếp cận dữ liệu hoặc hệ thống trên cloud.
- Đội IT cần biết cảnh báo nào phải xử lý trước và cần cô lập thiết bị nhanh khi có nguy cơ lan rộng.

03 • VÌ SAO PHẦN MỀM DIỆT VIRUS CHƯA ĐỦ

Doanh nghiệp cần nhìn thấy cả hành vi đáng ngờ

Hạn chế	Biểu hiện thường gặp	Rủi ro
Chỉ nhận diện mã độc đã biết	Quét file và cập nhật mẫu nhận diện	Có thể bỏ sót hành vi mới hoặc không dùng file
Không có lịch sử hoạt động	Cảnh báo chỉ nói file nào bị chặn	Khó biết nguyên nhân và phạm vi ảnh hưởng
Nhiều phần mềm quản lý riêng	Chống virus, USB và tường lửa dùng các công cụ khác nhau	Tổn công vận hành và dễ đặt chính sách không đồng nhất
Xử lý chậm	Phải kiểm tra qua nhiều màn hình rồi mới cô lập máy	Sự cố có thêm thời gian lan rộng
Không xem rủi ro tài khoản	Máy tính có vẻ an toàn nhưng tài khoản đã bị chiếm	Đăng nhập bằng tài khoản thật có thể qua mặt kiểm soát

Cách tiếp cận phù hợp với doanh nghiệp vừa và nhỏ

- Thiết bị vẫn được bảo vệ khi tạm thời mất kết nối Internet.
- Dữ liệu cần thiết được phân tích tập trung để nhận ra các hành vi liên quan.
- Đội IT có một quy trình rõ ràng từ nhận cảnh báo, kiểm tra, cô lập đến khắc phục.
- Chỉ mua thêm chức năng bảo vệ tài khoản, kiểm soát thiết bị hoặc dịch vụ 24/7 khi thực sự cần.

04 • CÁCH CROWDSTRIKE HOẠT ĐỘNG

Một chương trình gọn nhẹ và một trang quản trị tập trung

Falcon cài một chương trình bảo vệ nhỏ trên máy tính và máy chủ. Chương trình này thực thi chính sách bảo vệ tại thiết bị và gửi các tín hiệu cần thiết lên nền tảng CrowdStrike trên cloud để phân tích. Với mô hình triển khai thông thường, doanh nghiệp không cần máy chủ quản lý antivirus hoặc EDR tại chỗ.

1 CHƯƠNG TRÌNH TRÊN THIẾT BỊ	2 NỀN TẢNG CROWDSTRIKE TRÊN CLOUD	3 TRANG QUẢN TRỊ
Ngăn mã độc Theo dõi hành vi Thực thi chính sách	Phân tích tín hiệu Đánh giá mức độ rủi ro Tạo cảnh báo có ngữ cảnh	Kiểm tra sự cố Cô lập máy Thực hiện quy trình xử lý
Windows • macOS • Linux	CrowdStrike Security Cloud	Đội IT • Đối tác vận hành • Dịch vụ 24/7

Hình 1. Mô hình hoạt động rút gọn của CrowdStrike Falcon.

Thông tin đi đâu và đội IT làm gì

- Chương trình trên thiết bị theo dõi file, ứng dụng, kết nối và hành vi có dấu hiệu bất thường.
- Nền tảng trên cloud phân tích các tín hiệu liên quan và tạo cảnh báo có mức độ ưu tiên.
- Đội IT xem nguyên nhân, thiết bị và người dùng liên quan; khi cần có thể cô lập máy khỏi mạng.
- Nếu mua thêm chức năng bảo vệ tài khoản, Falcon có thể liên kết rủi ro của thiết bị với tài khoản đăng nhập.

05 • NGĂN MÃ ĐỘC VÀ RANSOMWARE

Falcon Prevent bảo vệ nhiều lớp

Falcon Prevent là chức năng chống mã độc thế hệ mới của CrowdStrike. Hệ thống không chỉ so sánh file với danh sách mã độc đã biết mà còn xem cách file và chương trình hoạt động. CrowdStrike công bố hỗ trợ Windows, macOS và Linux; phạm vi cụ thể cần đối chiếu theo phiên bản hệ điều hành đang dùng.

Lớp bảo vệ	Cách hoạt động dễ hiểu	Ví dụ
Nhận diện file đáng ngờ	Đánh giá file trước hoặc khi file chạy	Chặn hoặc cách ly file theo chính sách
Chặn hành vi khai thác	Nhận ra cách chương trình lợi dụng lỗ hổng	Ngăn chuỗi lệnh tạo và chạy mã nguy hiểm
Nhận diện hành vi tấn công	Xem chuỗi hành động thay vì một file riêng lẻ	Phát hiện lệnh bất thường, tạo điểm bám hoặc đánh cắp thông tin đăng nhập
Phân tích trên cloud	So sánh tín hiệu từ nhiều thiết bị	Liên kết các dấu hiệu mới và đánh giá mức độ nghiêm trọng
Thông tin về mối đe dọa	Bổ sung dữ liệu về dấu vết và cách tấn công đã biết	Giúp đội IT ưu tiên việc cần xử lý trước

Khi có dấu hiệu ransomware

- Chặn file nguy hiểm trước hoặc ngay khi file chạy, nếu hệ thống đủ cơ sở xác định.
- Nhận ra các hành vi như mã hóa nhiều file, xóa bản sao phục hồi hoặc tìm cách tắt phần mềm bảo mật.
- Cho đội IT thấy chương trình nào khởi đầu sự việc và những thiết bị nào có thể liên quan.
- Cô lập máy tính khỏi mạng khi nguy cơ lây lan hoặc điều khiển từ xa ở mức cao.

06 • PHÁT HIỆN VÀ XỬ LÝ SỰ CỐ

Falcon Insight XDR giúp hiểu chuyện gì đã xảy ra

Falcon Insight XDR ghi nhận hoạt động trên thiết bị và xâu chuỗi các dấu hiệu liên quan. Thay vì chỉ báo rằng một file đã bị chặn, hệ thống giúp đội IT thấy sự việc bắt đầu từ đâu, đã ảnh hưởng tới máy nào và nên xử lý bước nào trước. Các chức năng nâng cao và khả năng kết nối nguồn dữ liệu khác phụ thuộc gói bản quyền.

Chức năng	Câu hỏi được trả lời	Đội IT có thể làm gì
Chuỗi chương trình	Chương trình nào khởi đầu và chạy tiếp những gì?	Xác định điểm bắt đầu của sự cố
Nhóm cảnh báo liên quan	Các dấu hiệu có thuộc cùng một sự cố không?	Ưu tiên sự cố quan trọng thay vì xem từng cảnh báo rời
Tìm kiếm chủ động	Dấu hiệu tương tự có xuất hiện trên máy khác không?	Mở rộng phạm vi kiểm tra
Cô lập thiết bị	Máy có cần ngắt khỏi mạng nội bộ không?	Chặn lan truyền nhưng vẫn giữ kênh quản trị Falcon
Xử lý từ xa có kiểm soát	Cần kiểm tra hoặc loại bỏ thành phần nào?	Chạy lệnh theo quyền được cấp và có ghi nhận
Quy trình tự động	Bước lặp lại nào có thể giao cho hệ thống?	Gửi thông báo, bổ sung thông tin hoặc cô lập theo điều kiện

KHI NÀO CẦN XDR

XDR mở rộng việc phân tích từ máy tính sang các nguồn dữ liệu khác. Khả năng kết nối, dung lượng dữ liệu và chi phí phụ thuộc gói bản quyền; doanh nghiệp chỉ nên dùng khi có tình huống cụ thể cần liên kết.

Mục tiêu là giúp đội IT hiểu nhanh mức độ nguy hiểm và phạm vi ảnh hưởng, thay vì phải ghép thông tin từ nhiều công cụ. Giao diện thực tế có thể thay đổi theo phiên bản, gói bản quyền và quyền của người dùng.



1. Xem mức độ nghiêm trọng, máy tính, tài khoản và thời điểm xảy ra cảnh báo.
2. Kiểm tra chương trình nào khởi đầu và các chương trình nào chạy tiếp theo.
3. Tìm xem dấu hiệu tương tự có xuất hiện trên máy tính khác hay không.
4. Cô lập máy hoặc hạn chế tài khoản nếu sự cố có nguy cơ lan rộng.
5. Khắc phục, phục hồi và cập nhật chính sách để tránh lặp lại sự cố.

Quyền cô lập máy, xử lý từ xa và thay đổi chính sách phải được cấp cho đúng người, có ghi nhận và có bước phê duyệt phù hợp.

08 • BẢO VỆ TÀI KHOẢN NGƯỜI DÙNG

Giảm rủi ro khi mật khẩu hoặc tài khoản bị lộ

Một tài khoản hợp lệ vẫn có thể bị kẻ tấn công sử dụng. Falcon Identity Threat Protection là chức năng mua thêm, giúp phát hiện cách đăng nhập bất thường, nhận biết tài khoản có quyền cao và áp dụng biện pháp kiểm soát theo mức độ rủi ro. CrowdStrike nêu phạm vi hỗ trợ cho Active Directory và Microsoft Entra ID; cần khảo sát hệ thống thực tế trước khi triển khai.

Nhóm chức năng	Mô tả dễ hiểu	Giá trị sử dụng
Nhận diện tài khoản	Phân biệt tài khoản người dùng, dịch vụ, dùng chung và quản trị	Biết tài khoản nào cần ưu tiên bảo vệ
Kiểm tra cấu hình	Tìm quyền và cấu hình thư mục có thể bị lợi dụng	Giảm điểm yếu trước khi xảy ra sự cố
Theo dõi đăng nhập	Liên kết đăng nhập với rủi ro của thiết bị	Tăng độ tin cậy của cảnh báo
Kiểm soát truy cập	Cho phép, chặn hoặc yêu cầu xác thực thêm theo mức rủi ro	Hạn chế kẻ tấn công dùng tài khoản bị lộ
Điều tra thống nhất	Nối tài khoản, thiết bị và chương trình trong cùng sự cố	Xác định nhanh người dùng và máy bị ảnh hưởng

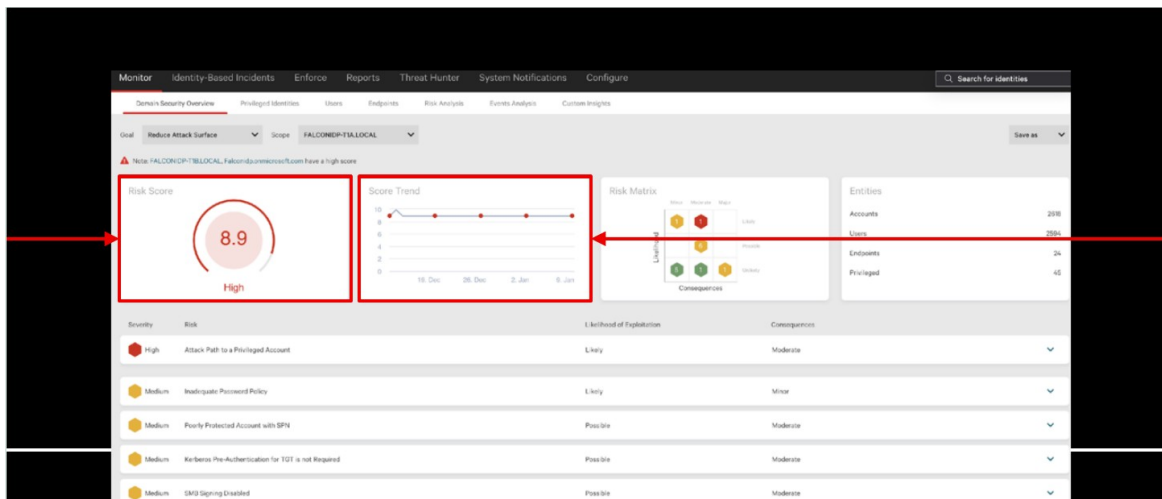
LƯU Ý

Khả năng bảo vệ các hệ thống cũ, máy chưa được quản lý và yêu cầu xác thực bổ sung phụ thuộc hạ tầng tài khoản, phiên bản sản phẩm và gói bản quyền.

09 • KIỂM TRA ĐIỂM YẾU CỦA TÀI KHOẢN

Ưu tiên những tài khoản có thể gây thiệt hại lớn

Bảng tổng hợp rủi ro giúp đội IT biết tài khoản nào có quyền cao, cấu hình nào còn yếu và đường truy cập nào có thể dẫn tới hệ thống quan trọng. Falcon cung cấp thông tin để ưu tiên; doanh nghiệp vẫn cần người chịu trách nhiệm và quy trình phê duyệt trước khi thay đổi tài khoản hoặc quyền truy cập.



Hình 3. Ví dụ bảng tổng hợp rủi ro tài khoản trong Falcon Identity Protection.

Nội dung nên kiểm tra trong giai đoạn thử nghiệm

- Tài khoản quản trị, tài khoản dùng cho dịch vụ và tài khoản không còn người phụ trách.
- Mật khẩu yếu, dùng lại hoặc đã xuất hiện trong nguồn dữ liệu rò rỉ mà hệ thống quan sát được.
- Các đường truy cập có thể dẫn đến tài khoản quản trị cao nhất hoặc hệ thống quan trọng.
- Đăng nhập bất thường và hoạt động đáng ngờ bắt đầu từ một thiết bị có rủi ro.
- Khả năng yêu cầu xác thực bổ sung hoặc chặn có điều kiện mà không làm gián đoạn công việc.

10 • TỰ ĐỘNG HÓA CÓ KIỂM SOÁT

Tự động làm việc lặp lại nhưng không tự ý gây gián đoạn

Không phải cảnh báo nào cũng nên tự động cô lập máy hoặc khóa tài khoản. Doanh nghiệp nên tự động các bước ít rủi ro như bổ sung thông tin, gửi thông báo và tạo phiếu xử lý. Các hành động có thể ảnh hưởng công việc cần điều kiện rõ ràng, người phê duyệt và cách khôi phục.

Mức xử lý	Ví dụ	Cách kiểm soát
Bổ sung thông tin	Thêm dữ liệu về máy, người dùng và mối đe dọa	Có thể tự động vì ít ảnh hưởng vận hành
Thông báo và giao việc	Gửi cảnh báo hoặc tạo phiếu xử lý	Quy định người nhận và thời gian phản hồi
Hạn chế có điều kiện	Cô lập máy, hạn chế tài khoản hoặc yêu cầu xác thực thêm	Chỉ dùng cho rủi ro cao; có người phê duyệt và cách hoàn tác
Khắc phục kỹ thuật	Dừng chương trình hoặc xóa file từ xa	Giới hạn quyền, ghi lại lệnh và thử trên nhóm nhỏ
Kết nối công cụ khác	Gửi dữ liệu sang hệ thống phiếu việc, email hoặc quản lý tài khoản	Bảo vệ khóa kết nối và tránh chạy lặp

Ví dụ xử lý cảnh báo ransomware nghiêm trọng

- Hệ thống phát hiện hành vi mã hóa dữ liệu hoặc tìm cách vô hiệu hóa bảo mật.
- Tự động bổ sung thông tin về máy và tài khoản, sau đó thông báo cho người phụ trách.
- Cô lập máy theo điều kiện đã duyệt; yêu cầu xác thực thêm nếu tài khoản cũng có rủi ro.
- Người có thẩm quyền kiểm tra và loại bỏ thành phần còn sót lại.
- Khôi phục từ nguồn sạch, đưa máy trở lại hoạt động và cập nhật chính sách.

11 • KHI NÀO CẦN GIÁM SÁT 24 GIỜ

Tự vận hành hay dùng dịch vụ CrowdStrike Falcon Complete

Công cụ chỉ tạo ra giá trị khi có người theo dõi và xử lý. Doanh nghiệp có thể tự vận hành, nhận thêm hỗ trợ sẵn tìm mối đe dọa hoặc thuê dịch vụ giám sát và phản ứng 24/7. Lựa chọn phụ thuộc số người trong đội IT, thời gian trực và mức độ quan trọng của hệ thống.

Lựa chọn	AI theo dõi	Vai trò
Thông tin mối đe dọa tích hợp	Nền tảng và đội IT của doanh nghiệp	Bổ sung bối cảnh để xếp ưu tiên cảnh báo
Falcon Adversary OverWatch	Chuyên gia CrowdStrike 24/7	Chủ động tìm dấu hiệu tấn công tinh vi và chuyển thông tin cho khách hàng
Falcon Complete	Đội ngũ CrowdStrike và công nghệ tự động	Theo dõi, điều tra và khắc phục trong phạm vi dịch vụ đã thỏa thuận
Đội IT của doanh nghiệp	Khách hàng	Nắm hệ thống kinh doanh, phê duyệt thay đổi và phục hồi dịch vụ

Ba cách vận hành phổ biến

- Tự vận hành: phù hợp khi doanh nghiệp có người đủ kỹ năng và quy trình xử lý sự cố rõ ràng.
- Dùng Falcon Enterprise kèm OverWatch: CrowdStrike hỗ trợ sẵn tìm dấu hiệu tinh vi, còn đội IT của doanh nghiệp xử lý cảnh báo.
- Dùng Falcon Complete: phù hợp khi thiếu người trực 24/7; cần thống nhất rõ phạm vi hành động, người liên hệ và trách nhiệm phục hồi.

PHÂN BIỆT

OverWatch hỗ trợ sẵn tìm dấu hiệu tấn công. Falcon Complete là dịch vụ giám sát và phản ứng có phạm vi vận hành rộng hơn. Hai dịch vụ không thay thế cho nhau.

12 • BẮT ĐẦU NHỎ VÀ MỞ RỘNG KHI CẦN

Chỉ bổ sung chức năng khi có nhu cầu rõ ràng

Nhu cầu	Chức năng CrowdStrike	Khi nào nên xem xét
Chống mã độc	Falcon Prevent	Thay phần mềm diệt virus và tăng khả năng ngăn ransomware
Điều tra sự cố	Falcon Insight XDR	Cần biết nguyên nhân, phạm vi và cô lập thiết bị
Kiểm soát USB	Falcon Device Control	Cần giới hạn thiết bị lưu trữ gắn ngoài
Quản lý tường lửa trên máy	Falcon Firewall Management	Muốn đặt chính sách tường lửa tập trung
Kiểm kê thiết bị	Falcon Discover	Cần biết máy, phần mềm và tài khoản đang được sử dụng
Ưu tiên lỗ hổng	Falcon Exposure Management	Cần tập trung xử lý các lỗ hổng có rủi ro cao
Bảo vệ tài khoản	Falcon Identity Threat Protection	Có Active Directory hoặc Entra ID và nhiều tài khoản quản trị
Bảo vệ dữ liệu	Falcon Data Protection	Cần theo dõi và hạn chế dữ liệu nhạy cảm bị đưa ra ngoài
Giám sát 24/7	Falcon Complete	Không có đủ nhân sự trực và xử lý sự cố liên tục

LƯU Ý KHI BÁO GIÁ

Một chương trình cài trên máy không có nghĩa là mọi chức năng đều được sử dụng. Báo giá phải ghi rõ gói bản quyền, số thiết bị, thời hạn, mức hỗ trợ và dịch vụ đi kèm.

13 • CHỌN GÓI GIẢI PHÁP

Falcon Pro, Enterprise và Complete phù hợp với nhu cầu khác nhau

Phương án	Mục tiêu	Thành phần chính	Phù hợp khi
Falcon Pro	Thay phần mềm diệt virus	Bảo vệ chống mã độc và các chức năng trong gói Pro hiện hành	Đội IT nhỏ cần triển khai đơn giản và quản lý tập trung
Falcon Enterprise	Bảo vệ và điều tra sự cố	Falcon Prevent, Falcon Insight XDR, OverWatch và các chức năng theo gói hiện hành	Doanh nghiệp cần xem nguyên nhân, phạm vi và tự thực hiện phản ứng
Falcon Complete	Thuê dịch vụ giám sát và phản ứng	Công nghệ Falcon cùng chuyên gia 24/7 trong phạm vi dịch vụ	Thiếu nhân sự trực liên tục hoặc muốn giảm gánh nặng xử lý cảnh báo

Thông tin cần có trước khi báo giá

- Số máy tính, máy chủ, hệ điều hành và những hệ thống quan trọng nhất.
- Có cần điều tra sự cố chuyên sâu, kiểm soát USB, quản lý tường lửa trên máy hoặc bảo vệ tài khoản hay không.
- Doanh nghiệp tự theo dõi cảnh báo hay cần dịch vụ giám sát 24/7.
- Yêu cầu về nơi lưu dữ liệu, proxy, đường truyền và kết nối với hệ thống nhận phiếu hỗ trợ hoặc lưu log.
- Phạm vi hỗ trợ, hướng dẫn ban đầu, đào tạo và thời gian phản hồi đã nằm trong gói hay phải mua riêng.

14 • KẾ HOẠCH TRIỂN KHAI CHO DOANH NGHIỆP VỪA VÀ NHỎ

Thử trên một nhóm nhỏ trước khi triển khai toàn bộ

Hạng mục	Thiết kế ban đầu	Quyết định cần chốt
Tài khoản quản trị	Phân quyền cho IT, bảo mật và người chỉ xem	Khu vực dịch vụ, đăng nhập một lần, xác thực nhiều lớp và tài khoản dự phòng
Chương trình trên thiết bị	Cài thử trên nhóm nhỏ; tách chính sách theo hệ điều hành và vai trò	Phiên bản hệ điều hành, phần mềm xung đột, proxy và thời gian cài đặt
Chính sách bảo vệ	Tăng mức bảo vệ theo từng giai đoạn	Ai phê duyệt ngoại lệ, lý do và ngày hết hạn
Xử lý sự cố	Giới hạn quyền cô lập máy và xử lý từ xa	Ai được phép làm, ai phê duyệt và cách hoàn tác
Bảo vệ tài khoản nếu mua thêm	Thử với nhóm tài khoản quản trị	Phạm vi thư mục, xác thực nhiều lớp và tài khoản dịch vụ
Kết nối hệ thống khác	Chỉ kết nối khi có nhu cầu cụ thể	Công cụ nhận dữ liệu, quyền truy cập và thời gian phản hồi

Chuẩn bị trước khi chạy thử

- Lập danh sách thiết bị và chọn một nhóm đại diện cho các hệ điều hành, phòng ban và ứng dụng quan trọng.
- Kiểm tra khả năng chạy cùng phần mềm bảo mật hiện tại và chuẩn bị kế hoạch gỡ bỏ công cụ cũ.
- Cho phép các địa chỉ và cổng kết nối theo tài liệu CrowdStrike; kiểm tra proxy nếu doanh nghiệp đang sử dụng.
- Ghi nhận mức dùng CPU, bộ nhớ và đường truyền trước khi cài để so sánh sau thử nghiệm.
- Chỉ định người nhận cảnh báo và người có quyền phê duyệt việc cô lập máy hoặc xử lý từ xa.

PHỤ LỤC A • THUẬT NGỮ DỄ HIỂU

Tra cứu thuật ngữ khi gặp trong tài liệu

Các tên tiếng Anh dưới đây là thuật ngữ sản phẩm thường gặp. Phần giải thích tập trung vào ý nghĩa thực tế đối với người quản lý và đội IT.

Thuật ngữ	Hiểu đơn giản
Endpoint	Máy tính để bàn, laptop hoặc máy chủ cần được bảo vệ.
Sensor	Chương trình CrowdStrike được cài trên thiết bị. Có thể hiểu tương tự phần mềm bảo vệ đầu cuối.
NGAV	Phần mềm chống mã độc thế hệ mới; xem cả file và hành vi, không chỉ so sánh mẫu virus.
EDR	Chức năng ghi nhận hoạt động trên thiết bị để phát hiện, điều tra và xử lý sự cố.
XDR	Mở rộng việc phân tích bằng cách liên kết dữ liệu endpoint với các nguồn bảo mật khác khi có bản quyền phù hợp.
Detection	Cảnh báo bảo mật đã có thông tin về thiết bị, người dùng và hành vi liên quan.
Incident	Một nhóm cảnh báo được hệ thống xem là có liên quan tới cùng một sự cố.
IOC	Dấu vết đã biết của mối đe dọa, chẳng hạn file, địa chỉ mạng hoặc tên miền nguy hiểm.
IOA	Chuỗi hành vi cho thấy một cuộc tấn công có thể đang diễn ra, dù chưa thấy file mã độc đã biết.
Process tree	Sơ đồ cho biết chương trình nào khởi đầu và những chương trình nào chạy tiếp theo.
Containment	Cô lập thiết bị khỏi mạng nội bộ để hạn chế lây lan nhưng vẫn giữ kết nối quản trị với Falcon.
RTR	Công cụ xử lý từ xa dành cho người được cấp quyền để kiểm tra và khắc phục trên thiết bị.
Threat hunting	Chủ động tìm dấu hiệu tấn công chưa tạo thành cảnh báo rõ ràng.
MDR	Dịch vụ có chuyên gia theo dõi, điều tra và phản ứng 24/7 trong phạm vi đã thỏa thuận.
Entitlement	Quyền sử dụng chức năng được bao gồm trong gói bản quyền đã mua.

[Quay lại Mục lục tra cứu nhanh](#)

PHỤ LỤC B • NGUỒN CROWDSTRIKE CHÍNH THỨC

Liên kết dùng để kiểm tra thông tin sản phẩm

Các liên kết dưới đây dẫn tới tài liệu do CrowdStrike công bố. Tên gói, chức năng và điều kiện cấp phép có thể thay đổi; cần kiểm tra lại trước khi chốt thiết kế và báo giá.

Chủ đề	Tài liệu	Tra cứu
Gói Endpoint	Falcon Endpoint Protection Pro Data Sheet	Mở tài liệu
Gói Endpoint	Falcon Enterprise Data Sheet	Mở tài liệu
NGAV	Falcon Prevent Data Sheet	Mở tài liệu
EDR và XDR	Falcon Insight XDR Data Sheet	Mở tài liệu
Bảo vệ danh tính	Falcon Identity Threat Protection Data Sheet	Mở tài liệu
MDR	Falcon Complete Next-Gen MDR Data Sheet	Mở tài liệu
Threat intelligence	CrowdStrike 2026 Global Threat Report	Mở tài liệu

Ngày kiểm tra liên kết: 11/09/2026. [Quay lại Mục lục tra cứu nhanh](#)