CROWDSTRIKE

CrowdStrike Endpoint Security

Global Adversaries

Thông tin về các nhóm tội phạm mạng toàn cầu

26 Kẻ thù mới

257 Kẻ thù được theo dõi

140+ Nhóm có hành vi độc hại

CROWDSTRIKE

CROWDSTRIKE

GLOBAL THREAT REPORT 2025

Bối cảnh mối đe dọa qua những Con Số

XÂM NHẬP BAN ĐẦU

442%

Tỷ lệ gia tăng của số vụ lừa đảo qua giọng nói (vishing) giữa nửa đầu và nửa cuối năm 2024

50%

Tỷ lệ gia tăng hoạt động quảng cáo của các "nhà môi giới truy cập"

52%

Số lỗ hổng bảo mật được CrowdStrike ghi nhận trong năm 2024 có liên quan đến giai đoạn Xâm nhập Ban đầu (Initial Access)

PHÁT TÁN

51s

Là thời gian phát tán nhanh nhất trong năm 2024

ẨN NẤP

79%

Các phát hiện trong năm 2024 là malware-free

HỒ SƠ KẺ TẤN CÔNG:

PUNK SPIDER

Mục tiêu	Động cơ	Loại hình
Trục lợi Tài chính	**Criminal**	**eCrime**

Lạm Dụng Công Cụ Hợp Lệ

Sử dụng phần mềm hợp lệ và các công cụ mã nguồn mở

Leo Thang Đặc Quyền

Sao chép/gán quyền hạn cho các tài khoản mới hoặc đã bị xâm nhập

Phát Tán

Lợi dụng việc di chuyển qua các hệ thống để tránh bị phát hiện

Rò Rỉ Dữ Liệu

Đánh cắp dữ liệu user và group để sử dụng sau này

Ransomware

Triển khai ransomware để tống tiền nạn nhân

CROWDSTRIKE

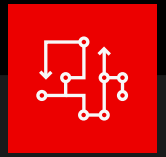
Kẻ thù đang nhanh hơn và ẩn nấp tinh vi hơn.

Các endpoint của bạn chính là con đường tấn công chủ yếu.

Các Biện Pháp Phòng Thủ Lỗi Thời Không Thể Ngăn Chặn Các Mối Đe Dọa Hiện Đại

Cách Tiếp Cận Bảo Mật Lỗi Thời

Khả Năng Quan Sát Và Mức Độ Bao Phủ Các Lỗ Hổng Bị Giới Hạn



Phức tạp, Nặng, Khó để vận hành

Cách Tiếp Cận Hiện Đại của CrowdStrike Đối Với Endpoint

Bảo vệ vượt trội.
An ninh hàng đầu.
Hiệu quả đã được kiểm chứng.

Một Agent. Một Platform.
Bảo vệ các endpoint, danh tính và workload.

Bao phủ ngay lập tức. Đem lại giá trị tức thì.
Bảo vệ nhanh chóng, liền mạch ngay sau khi triển khai.

Phát hiện thông minh hơn. Bảo vệ hiện đại.
Sức mạnh AI giúp phát hiện các mối đe dọa đang ẩn nấp.

Sức mạnh từ Tình báo. Cập nhật liên tục.
Tình báo dựa trên hành vi của kẻ tấn công, cung cấp bối cảnh mối đe dọa quan trọng.

CrowdStrike® Charlotte AI™. Trả lời tức thì.
Đẩy nhanh hoạt động bảo mật với chuyên gia phân tích bảo mật AI.

Triển khai dễ dàng, Bảo vệ tự tin

Qua một agent duy nhất

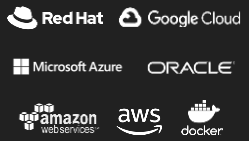
Falcon Platform

- Dễ dàng cài đặt và quản lý
- Mở rộng từ on premise, hybrid và cloud
- Nền tảng tích hợp AI
- Giao diện Cloud-native
- Quản lý đơn giản và hợp nhất

Clouds

Data Centers

Workloads



Containers

Servers

Endpoints

Workstations

Mobile Devices

Servers

IoT Devices

ChromeOS

Identities

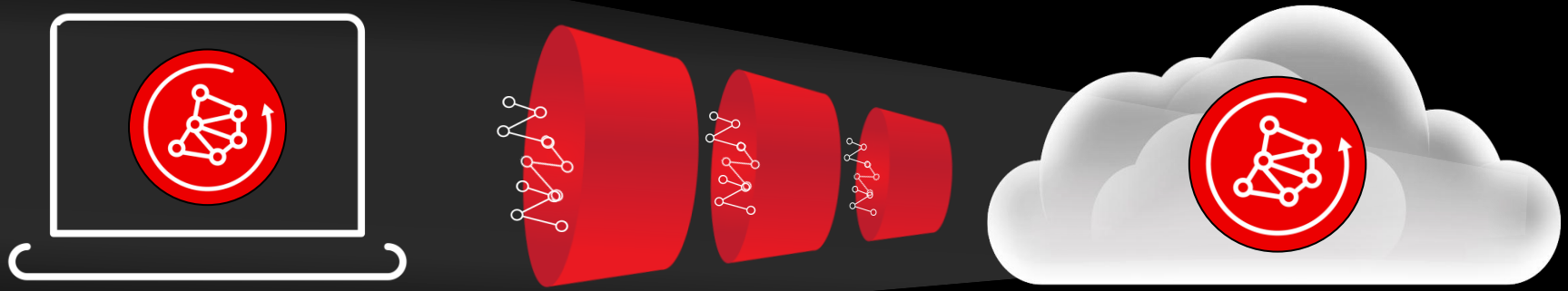
Active Directory
Entra ID
Okta

Human and Service Accounts

Third Parties

Sử Dụng Ai-native Trong Phát Hiện Và Ngăn Chặn

Từ sensor đến cloud



Trên Sensor

Sensor ML

Là các model cốt lõi để ngăn chặn malware trực tiếp

Trên Cloud

Indicators of Attack (IOA) với sức mạnh AI

Các IOA hành vi nâng cao kết hợp với ML trên cloud để phát hiện mối đe dọa với độ chính xác cao

Cloud ML

Nhiều loại model đa dạng chạy ở quy mô cloud

Tích Hợp Threat Intelligence.
Bảo Vệ Endpoint Vượt Trội.

Thu thập	Hàng nghìn tỷ sự kiện mỗi tuần
Làm phong phú	257 kẻ thù toàn cầu bị theo dõi
Phát triển	Hơn 800K dấu hiệu xâm nhập (IOCs) được công bố mỗi tuần
Bảo vệ	Hơn 180 triệu quyết định IOA mỗi giây

FORRESTER® **#1 trong Thu Thập Tình Báo**
The Forrester Wave™: External Threat Intelligence Service Providers, Q3 2023

Figures from the Falcon platform, CrowdStrike 2024 Threat Hunting Report and CrowdStrike 2025 Global Threat Report.

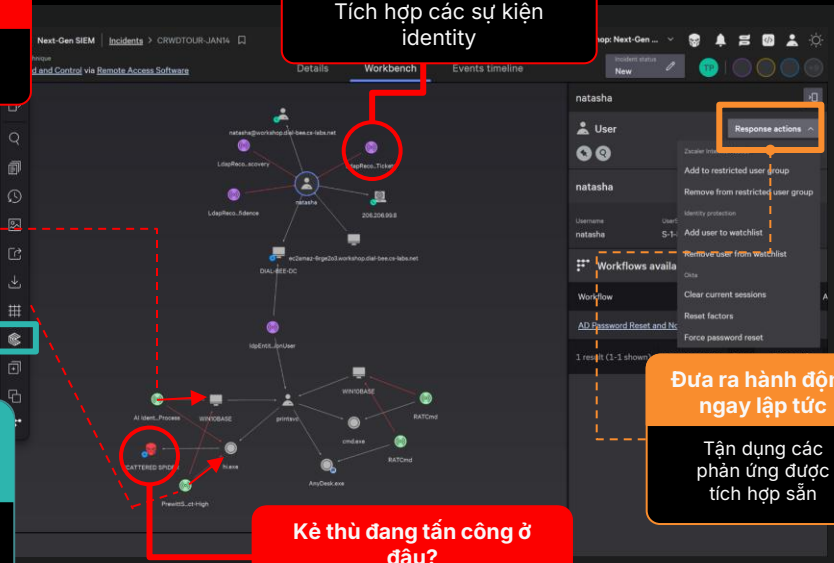
Phát Hiện và Bảo Vệ Đa Miền Hợp Nhất

Các phát hiện endpoint liên quan như thế nào?

Liên kết các phát hiện endpoint với nhau

Có danh tính nào bị xâm phạm không?

Tích hợp các sự kiện identity



Tìm các câu trả lời nhanh hơn với generative AI

Điều tra sự cố với Charlotte AI

Đưa ra hành động ngay lập tức

Tận dụng các phản ứng được tích hợp sẵn

Kẻ thù đang tấn công ở đâu?

Biết rõ về kẻ thù của bạn

Tăng tốc vận hành bảo mật trên toàn bộ nền tảng Falcon

Điều tra nhanh chóng

Chuyển hướng điều tra tức thì từ các phát hiện sang tìm kiếm, thông qua các workflow đơn giản được hỗ trợ bởi AI.

Thấu hiểu toàn diện

Trực quan hóa toàn bộ attack path và điều tra các host khác có nguy cơ bị ảnh hưởng

Ngữ cảnh đầy đủ

Cung cấp một góc nhìn tích hợp với đầy đủ threat intelligence, ngữ cảnh liên quan và mối liên kết giữa các đối tượng

10GB dữ liệu miễn phí mỗi ngày với dữ liệu tích hợp từ third-party

Mang Đến Sức Mạnh Cho SOC Thế Hệ Mới

Vượt xa các trợ lý ảo “hỏi - đáp“ với khả năng suy luận và hành động tự động trên toàn bộ hoạt động của SOC

ĐỘ CHÍNH XÁC CỦA CHUYÊN GIA

Hơn 98%

tỷ lệ chính xác trong phân loại cảnh báo tự động

TIẾT KIỆM THỜI GIAN

Lấy lại hơn 40 giờ

thời gian làm việc mỗi tuần cho đội ngũ phân tích

HÀNH ĐỘNG TỰ ĐỘNG

Liên tục 24/7

Mang lại kết quả thực tiễn

CHARLOTTE AI

PHÂN LOẠI PHÁT HIỆN

Tự động, phân loại đa miền

→ Phân loại liên tục với độ chính xác ngang tầm chuyên gia

→ Giảm tải công việc phân loại thủ công và chỉ làm nổi bật những gì thực sự quan trọng

CHARLOTTE AI

PHẢN HỒI AGENTIC

Các cuộc điều tra được hướng dẫn bởi AI

→ Áp dụng kiến thức chuyên môn thực chiến vào mọi cuộc điều tra

→ Tăng tốc việc ra quyết định của chuyên viên phân tích bằng cách cung cấp ngữ cảnh nhanh và đầy đủ hơn

CHARLOTTE AI

AGENTIC WORKFLOWS

Giải pháp SOAR tích hợp LLM

→ Thích ứng một cách liền mạch với các trường hợp ngoại lệ và chưa xác định

→ Tùy chỉnh kết quả đầu ra để phù hợp với mọi đội nhóm, đối tượng, hoặc nhiệm vụ

Accuracy rating is a measure of Charlotte AI triage decisions that match the expert decisions from the CrowdStrike Falcon Complete Next-Gen MDR team.
Time savings represents the amount of time an analyst would have spent triaging detections but can now use that time for other skilled work while Charlotte triages the detections. Individual results may vary based on factors such as total alert volume.

CrowdStrike Được Xướng Là Một Leader

2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

> **Được định vị Xa nhất về bên phải cho Mức độ Toàn diện về Tầm nhìn và Cao nhất về Khả năng Thực thi**

Gartner

Figure 1: Magic Quadrant for Endpoint Protection Platforms

CROWDSTRIKE

Đổi Mới Vượt Trội. Bảo Vệ Toàn Diện.
Vị Thế Dẫn Đầu Đã Được Kiểm Chứng.

Kiểm Tra

Độ chính xác tổng thể đạt 100%
2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

Bảo vệ 100% trước ransomware
2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

Tin Cậy

Bởi hơn 74,000 khách hàng cuối trực tiếp và khách hàng của MSSP trên toàn thế giới

Chứng Thực

Leader trong:
Forrester Wave cho XDR
Forrester Wave cho Endpoint
GigaOm Radar cho XDR
GigaOm Radar cho Ransomware

Named a Leader in The Forrester Wave: Extended Detection And Response Platforms, Q2 2024
Named a Leader in The Forrester Wave: Endpoint Security, Q4 2023
Named a Leader in the 2025 GigaOm Radar for Extended Detection and Response
Named a Leader in the 2024 GigaOm Radar for Ransomware Prevention

CROWDSTRIKE

Bạn Không Cần Phải Tự Mình Giải Quyết

Tăng cường sức mạnh cho đội ngũ của bạn với các chuyên gia hàng đầu thế giới.

Quản lý phát hiện và phản ứng

Dịch vụ quản lý toàn diện 24/7/365 hoặc bổ sung nhân sự chuyên gia

Quản lý săn tìm mối đe dọa

Chủ động phát hiện các cuộc tấn công tinh vi và ẩn mình bằng sự kết hợp giữa AI và chuyên môn của con người

Ứng cứu và Tư vấn sự cố

Gia cố hệ thống trước sự cố và phản ứng sau sự cố với các chuyên gia hàng đầu thế giới

2024 MITRE Engenuity ATT&CK® Evaluations: Managed Services, Round 2

4 phút **Thời gian trung bình để phát hiện (MTTD)**

Phạm vi phát hiện toàn diện và khả năng phát hiện mối đe dọa nhanh chóng

Thank You

Phụ lục

CROWDSTRIKE'S AI-NATIVE PLATFORM STOPS BREACHES

V07.24.25

Kẻ thù Endpoint

HỒ SƠ KẺ TẤN CÔNG:

PUNK SPIDER

Mục tiêu	Động cơ	Loại hình
Trục lợi Tài chính	**Criminal**	**eCrime**

Lạm Dụng Công Cụ Hợp Lệ

Sử dụng phần mềm hợp lệ và các công cụ mã nguồn mở

Leo Thang Đặc Quyền

Sao chép/gán quyền hạn cho các tài khoản mới hoặc đã bị xâm nhập

Phát Tán

Lợi dụng việc di chuyển qua các hệ thống để tránh bị phát hiện

Rò Rỉ Dữ Liệu

Đánh cắp dữ liệu user và group để sử dụng sau này

Ransomware

Triển khai ransomware để tống tiền nạn nhân

CROWDSTRIKE

PUNK SPIDER: Thực Hiện Đánh Cắp Dữ Liệu Và Triển Khai Ransomware

Mục tiêu: Các công ty công nghệ Bắc Mỹ

Chuỗi Tấn Công

Xâm Nhập Ban Đầu

Khai thác lỗ hổng CVE-2024-3400 trên một thiết bị VPN Palo Alto GlobalProtect không được quản lý để giành quyền truy cập bằng cách sử dụng các thông tin đăng nhập đã bị rò rỉ

Phát Tán

Sử dụng Giao thức Remote Desktop (RDP) với một tài khoản dịch vụ để di chuyển sang một hệ thống nội bộ khác

Truy Cập Thông tin Xác thực

Trích xuất thông tin xác thực và leo thang đặc quyền bằng cách thêm người dùng vào các nhóm quản trị viên cục bộ (local Admins) và nhóm ESX Admins

Duy trì Truy Cập và Ẩn Nấp

Triển khai các công cụ tạo đường hầm proxy (proxy-tunneling) và công cụ truy cập từ xa

Trinh Sát

Sử dụng SharpShares và Invoke-ShareFinder.ps1 để liệt kê các tài nguyên được chia sẻ trong mạng (network shares).

Thu thập Dữ liệu và Tác Động

Sử dụng WinRAR để nén dữ liệu và cố gắng tuồn dữ liệu ra ngoài qua FileZilla. Bước cuối cùng: Triển khai ransomware Akira

Đánh cắp dữ liệu
Ransomware

CROWDSTRIKE

PUNK SPIDER: Thực Hiện Đánh Cắp Dữ Liệu Và Triển Khai Ransomware

Mục tiêu: Các công ty công nghệ Bắc Mỹ

Kết quả: Bị chặn hoàn toàn bởi Falcon Sensor và bởi sự phát hiện của đội Falcon Adversary OverWatch.

Chuỗi Tấn Công

Xâm Nhập Ban Đầu

Khai thác lỗ hổng CVE-2024-3400 trên một thiết bị VPN Palo Alto GlobalProtect không được quản lý để giành quyền truy cập bằng cách sử dụng các thông tin đăng nhập đã bị rò rỉ

Thiết bị VPN không được quản lý (tức là không có Falcon sensor nào được cài đặt)

Phát Tán

Sử dụng Giao thức Remote Desktop (RDP) với một tài khoản dịch vụ để di chuyển sang một hệ thống nội bộ khác

Phát hiện bởi Falcon. Hành vi này cũng được phát hiện bởi đội Falcon Adversary OverWatch.

Truy Cập Thông tin Xác thực

Trích xuất thông tin xác thực và leo thang đặc quyền bằng cách thêm người dùng vào các nhóm quản trị viên cục bộ (local Admins) và nhóm ESX Admins

Falcon sensor ngăn chặn hành vi leo thang đặc quyền

Duy trì Truy Cập và Ẩn Nấp

Triển khai các công cụ tạo đường hầm proxy (proxy-tunneling) và công cụ truy cập từ xa

Falcon sensor đã chặn việc thực thi của các công cụ này, qua đó ngăn chặn các cơ chế duy trì truy cập (persistence) được thiết lập.

Trinh Sát

Sử dụng SharpShares và Invoke-ShareFinder.ps1 để liệt kê các tài nguyên được chia sẻ trong mạng (network shares).

Falcon sensor đã ngăn chặn việc thực thi của cả hai công cụ trinh sát. Hoạt động này cũng được phát hiện bởi đội Falcon Adversary OverWatch.

Thu thập Dữ liệu và Tác Động

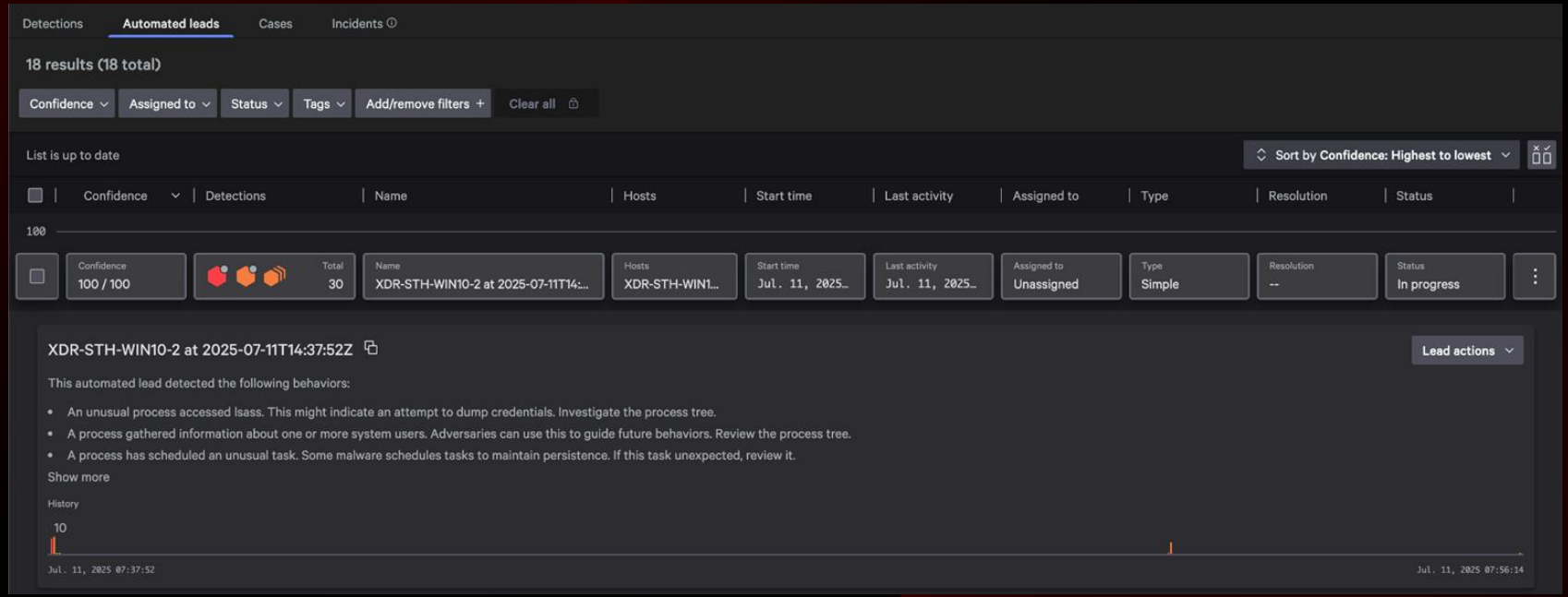
Sử dụng WinRAR để nén dữ liệu và cố gắng tuồn dữ liệu ra ngoài qua FileZilla. Bước cuối cùng: Triển khai ransomware Akira

Đội Falcon Adversary OverWatch đã phát hiện FileZilla đang được sử dụng để tuồn dữ liệu và thông báo cho khách hàng, sau đó họ sẽ ngay lập tức cách ly host. Ransomware Akira cũng bị nền tảng Falcon chặn lại trước khi bất kỳ hành động mã hóa nào có thể xảy ra.

CROWDSTRIKE

Năng Lực Chính

Các Đầu Mối Điều Tra Tự Động
Với sức mạnh từ CrowdStrike® Signal



- Dùng AI để phát hiện những mối đe dọa ẩn mình mà các công cụ khác thường bỏ lỡ.
- Phát hiện sớm các mối đe dọa, nhận diện vấn đề trước khi sự việc leo thang
- Tự động thích ứng với môi trường của bạn, giúp các manh mối điều tra trở nên đặc biệt phù hợp và giá trị

Các Đầu Mối Điều Tra Tự Động

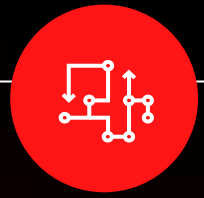
Với sức mạnh từ CrowdStrike® Signal

Phát Hiện Dễ Dàng Hơn

- Điểm khởi đầu cho các cuộc điều tra được **kết hợp với AI.**
- **Ưu tiên** các đầu mối tự động để tăng tốc quá trình phân loại

Phát Hiện Sớm Hơn

- **Làm nổi bật** các dấu hiệu ban đầu và tinh vi của một cuộc tấn công
- **Phát hiện** mối đe dọa ở giai đoạn đầu trước khi chúng gây ra thiệt hại đáng kể



Phát Hiện Thích Ứng

- **Tự động** thích ứng với môi trường của bạn
- **Đảm bảo** các manh mối tự động đều liên quan tới sự cố và có thể hành động

CROWDSTRIKE

Theo Dõi Và Ngăn Chặn Kẻ Thù Với Khả Năng Quan Sát Toàn Diện

THẤY nhiều hơn

Cung cấp khả năng quan sát sâu về endpoint trên toàn bộ doanh nghiệp để làm rõ toàn bộ phạm vi của các cuộc tấn công.

BIẾT nhiều hơn

Threat Intelligence trọng yếu dựa trên phân tích kẻ tấn công và sự cộng tác theo thời gian thực của các chuyên viên phân tích

LÀM nhiều hơn

Ứng phó tức thì với các SOAR workflow tự động hóa từ một command console hợp nhất

Dữ liệu đo lường chính cho khả năng quan sát đa miền

Endpoint

Identity

Cloud

Mobile

Data

Workbench Tương Tác

Rút ngắn thời gian ngăn chặn và thời gian khắc phục sự cố.

Điều Tra Tập Trung

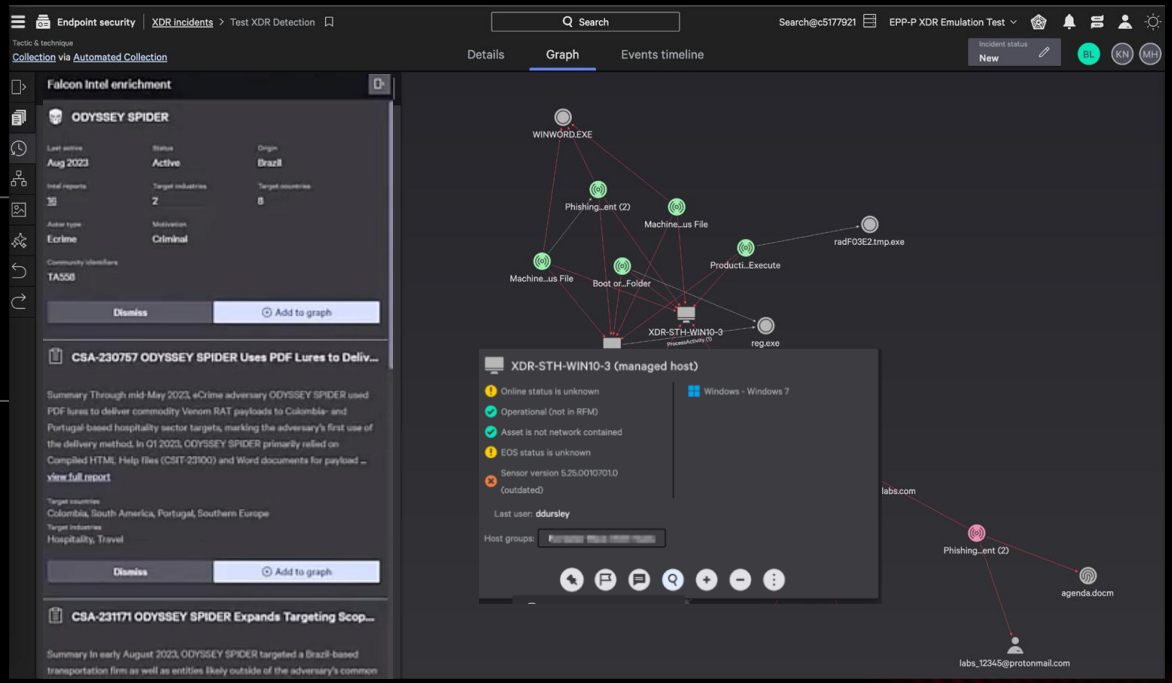
Chế độ xem đồ thị tương tác hỗ trợ các workflow săn tìm và điều tra mà không cần phải rời khỏi console

Trung Tâm Điều Hành Cộng Tác

Hỗ trợ cộng tác theo thời gian thực, nhiều người dùng; gắn tag các chuyên viên phân tích và thêm ghi chú, bổ sung thêm đối tượng hoặc case

Làm Phong Phú và Khắc Phục

Các tùy chọn làm phong phú dữ liệu và khắc phục tự động được tích hợp sẵn để chạy các workflows và playbooks



Tất cả khách hàng có Falcon Insight XDR:
Thu thập 10GB dữ liệu bên thứ ba miễn phí mỗi ngày

Hơn 100

Connector tích hợp sẵn, đi kèm với các bộ phân tích cú pháp

Hệ sinh thái đối tác mạnh mẽ

ExtraHop · mimecast · zscaler · PingIdentity · CLOUDFLARE · VECTRA · MENLO SECURITY · okta · FORGEROCK · Skyhigh Security · proofpoint · CISCO · corelight · FORTINET · THREAT WARRIOR · servicenow · CLAROTY · Google Cloud · ARMIS · Abnormal · netskope · Cribl · zeek

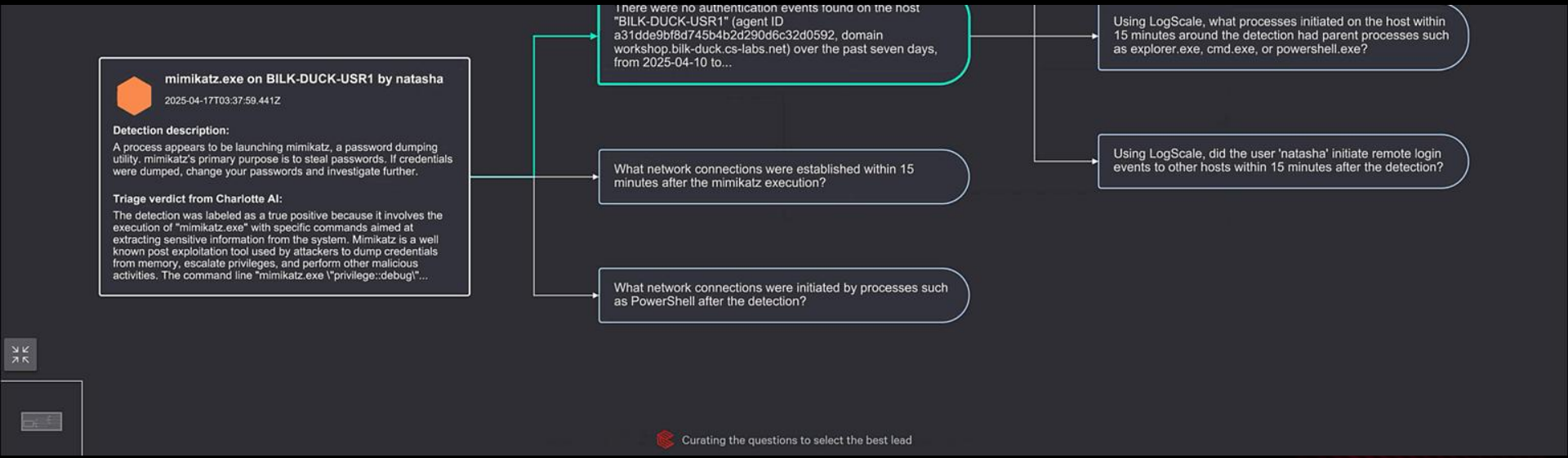
Charlotte AI

Từ vai trò trợ lý GenAI đến các hoạt động tự chủ

Tối ưu hóa các cuộc điều tra thực tế
VỚI GENAI ĐƯỢC TÍCH HỢP

Nhận câu trả lời nhanh chóng cho các câu hỏi
VỚI AI HỘI THOẠI

Tự động hóa các tác vụ phức tạp
VỚI AGENTIC AI



CROWDSTRIKE

Charlotte AI Agentic Workflow cho Endpoint Security

Tự động hóa việc phân tích các tập dữ liệu để tiến hành đánh giá, gửi báo cáo, dịch kết quả đầu ra, v.v.

Phân Loại Các Lệnh Powershell

"Phân loại tất cả các lệnh PowerShell được mã hóa đã thực thi trong 24 giờ qua và gửi một báo cáo về mọi hoạt động đáng ngờ"

Phát Hiện "Di Chuyển" Bất Thường Qua RDP

"Kiểm tra hoạt động RDP trong tuần qua và gửi một báo cáo chỉ ra bất kỳ trường hợp "di chuyển" bất thường nào"

Báo Cáo An Ninh Cấp Cao

"Tạo một bản tóm tắt về các phát hiện an ninh trong tuần qua so với tuần trước đó, và xuất bản tóm tắt dưới dạng PDF lên một kênh Slack"

Tóm Tắt Cảnh Báo Đa Ngôn Ngữ

"Tóm tắt mọi cảnh báo có mức độ nghiêm trọng 'Critical' từ các nhóm host A, B và C, sau đó gửi bản tóm tắt bằng tiếng Bồ Đào Nha"

Case Studies

Case Study

Coventry University

Đại học Coventry đạt được kết quả hàng đầu với Chiến lược An ninh Endpoint nâng cao

- Cải thiện thời gian phản ứng trước sự cố
- Không còn phải cài lại toàn bộ endpoint sau khi bị tấn công
- Giải phóng tài nguyên cho đội IT

Thách thức

- Gặp khó khan trong cách tiếp cận bị động và không hiệu quả với endpoint security, vốn không thể theo kịp bối cảnh mối đe dọa thay đổi nhanh chóng
- Đối mặt với khó khăn trong việc bảo vệ môi trường IT đa dạng và phân tán toàn cầu, bao gồm cả các mô hình làm việc từ xa và hybrid
- Quy trình phản ứng sự cố tốn nhiều thời gian

Giải pháp

- Triển khai các mô-đun của nền tảng Falcon, bao gồm Falcon Prevent (NGAV), Falcon Insight XDR và Falcon Complete Next-Gen MDR
- Hợp nhất các hoạt động an ninh vào một nền tảng cloud-native, sử dụng một agent
- Giảm thiểu đáng kể thời gian ứng phó và phục hồi

Kết Quả Nổi Bật

Giảm 94%

thời gian cho việc giải quyết các mối đe dọa.

Từ 2-3 ngày xuống còn dưới 1 tiếng

là thời gian trung bình để giải quyết sự cố bảo mật.

"Khả năng quan sát mà chúng tôi có được hiện nay là một tài sản mạnh mẽ trong việc giữ an ninh cho trường.

Chúng tôi có thể sử dụng các báo cáo chi tiết để trình bày cho đội quản lý cấp cao về các cấp độ mối đe dọa và rủi ro trên toàn bộ môi trường hệ thống."

— Steve Rogers, Enterprise Cloud, Infrastructure, Security Architect

Case Study

Pegasystems Hợp Nhất Endpoint, Identity và Cloud Security với CrowdStrike

- Khả năng quan sát hợp nhất với một nền tảng duy nhất
- Đơn giản hóa hoạt động vận hành
- Dịch vụ quản lý phát hiện và phản ứng được 24/7 (MDR)

Thách thức

- Cần phải hợp nhất các công cụ bảo mật rời rạc, thiếu sự tích hợp
- Yêu cầu một giải pháp để bảo vệ danh tính, các workload trên cloud, và endpoint dưới một chiến lược thống nhất
- Gặp phải những thiếu sót trong việc phát hiện các thông tin đăng nhập bị đánh cắp và hành vi phát tán.

Giải pháp

- Triển khai nền tảng Falcon để tích hợp endpoint, identity và cloud security trong một giải pháp duy nhất
- Có được khả năng quan sát theo thời gian thực về các tài khoản dịch vụ, hành vi lạm dụng của quản trị viên và các thông tin xác thực bị xâm nhập
- Tối ưu hóa hoạt động bảo mật với kiến trúc cloud-native và một agent duy nhất

Kết Quả Nổi Bật

Tỷ lệ phát hiện 100%
Trong suốt quá trình POC

Triển khai nhanh chóng
Cho 5,000 endpoint và 6,000 servers

"[Triển khai] CrowdStrike EDR và identity protection từ cùng một nền tảng và sensor giúp chúng tôi tiết kiệm thời gian, đồng thời lấp đầy các lỗ hổng bảo mật."

— Steve Tieland,
Giám đốc Vận hành An ninh Doanh nghiệp

Case Study

CoreWeave

Từ Endpoint đến Cloud, CoreWeave Hợp nhất Toàn bộ "Ngăn xếp Bảo mật" (Security Stack) với CrowdStrike.

- Không gây ảnh hưởng đến hiệu năng
- Bảo mật hợp nhất và có khả năng mở rộng
- Cải thiện khả năng quan sát attack surface

Thách thức

- Cần bảo vệ một hạ tầng cloud đang mở rộng nhanh chóng, hỗ trợ các workload tính toán hiệu năng cao
- Đối mặt với các mối đe dọa ngày càng phức tạp và nhiều hơn trong khi đang mở rộng các dịch vụ cung cấp ra thị trường
- Đòi hỏi phải có khả năng quan sát và kiểm soát chặt chẽ trên các endpoint và workload mà không làm suy giảm hiệu năng.

Giải pháp

- Triển khai nền tảng Falcon để hợp nhất việc bảo vệ endpoint và workload trên cloud bằng một agent duy nhất
- Đạt được khả năng mở rộng bảo mật một cách liền mạch song song với sự tăng trưởng kinh doanh mà không làm ảnh hưởng đến kỳ vọng về hiệu năng của khách hàng
- Có được khả năng quan sát toàn diện về attack surface, giúp nâng cao hình thái bảo mật trong khi vẫn hỗ trợ các môi trường phức tạp và throughput cao.

Kết Quả Nổi Bật

Giảm 100 lần
Số lượng cảnh báo false positive

Hàng trăm
Giờ làm việc được tiết kiệm mỗi năm

"CrowdStrike là tâm điểm chính trong hệ thống SOC của chúng tôi. Detection dashboard hiển thị cho chúng tôi bất cứ điều gì CrowdStrike xem là nguy hiểm... đem lại cho chúng tôi khả năng quan sát và bảo vệ end-to-end."

— Matt Bellingeri, CISO

Case Study

Anywhere®

Anywhere Real Estate Thay đổi Hoàn toàn Hình thái Bảo mật với CrowdStrike

- Phản ứng nhanh hơn và hợp nhất
- Tăng cường bảo vệ endpoint và Identity
- Khả năng quan sát mạnh mẽ trên toàn doanh nghiệp

Thách thức

- Vận hành một môi trường IT phi tập trung với nhiều vendor và nền tảng, gây phức tạp cho việc quan sát và ứng phó với mối đe dọa
- Đối mặt với rủi ro ransomware ngày càng tăng và cần một giải pháp bảo vệ danh tính và endpoint mạnh mẽ hơn
- Yêu cầu một giải pháp an ninh cloud-native có khả năng mở rộng để hỗ trợ quá trình chuyển đổi số trên toàn doanh nghiệp

Giải pháp

- Triển khai nền tảng Falcon để hợp nhất việc phát hiện, ứng phó tại endpoint và bảo vệ khỏi các mối đe dọa identity
- Tận dụng giải pháp Falcon Identity Protection để ngăn chặn các cuộc tấn công dựa trên thông tin xác thực và các hành vi phát tán
- Có được khả năng quan sát và ứng phó với mối đe dọa theo thời gian thực trên toàn bộ một tổ chức có cấu trúc phân tán cao

Kết Quả Nổi Bật

Giảm 500 lần
Số lượng cảnh báo

98% các cảnh báo
Là true positive

"Với CrowdStrike, chúng tôi đang có được giải pháp tốt nhất của tốt nhất. Đối với chúng tôi, việc sử dụng nền tảng Falcon cùng với dịch vụ OverWatch đã đưa chúng tôi vào nhóm 1% dẫn đầu về bảo mật."

— Brett Fernicola, Giám đốc Cấp cao Vận hành An ninh

Chứng Thực

Endpoint Security Leader

Nhận được điểm số cao nhất về Current Offering và điểm số hàng đầu trong 15 tiêu chí, vượt qua tất cả các vendor khác

> CrowdStrike được công nhận với giải pháp **"endpoint vượt trội"** với **"khả năng quan sát ưu việt"**

FORRESTER®

The Forrester Wave: Endpoint Security, Q4 2023

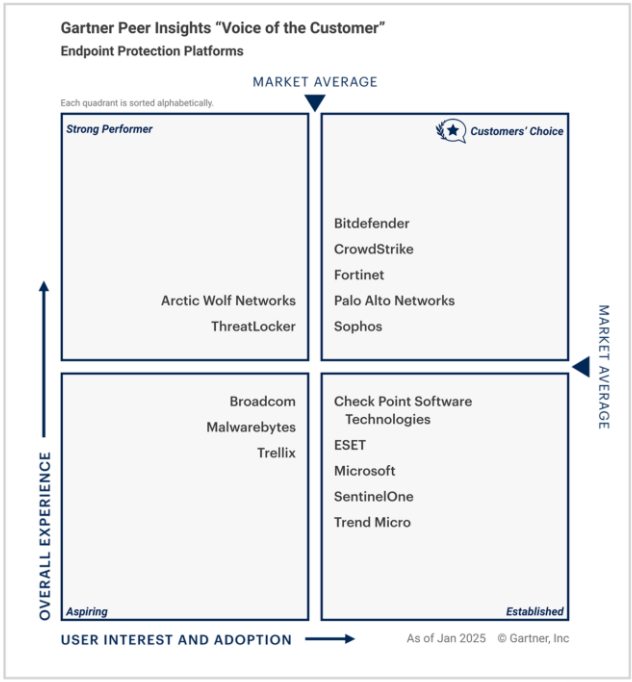
CrowdStrike được vinh danh là Lựa chọn của Khách hàng năm 2025 cho EPP [1]

Được vinh danh trong báo cáo Gartner Peer Insights™ Voice of the Customer năm 2025 cho hạng mục Nền tảng Bảo vệ Endpoint (EPP)

97% khách hàng sẵn lòng giới thiệu.[2]
601 lượt đánh giá.
Một nền tảng hợp nhất.

Gartner®

Figure 1. Voice of the Customer for Endpoint Protection Platforms



Source: Gartner (May 2025)

[1]As of January 2025. Gartner, Voice of the Customer For Endpoint Protection Platforms, Peer Editors, May 23, 2025

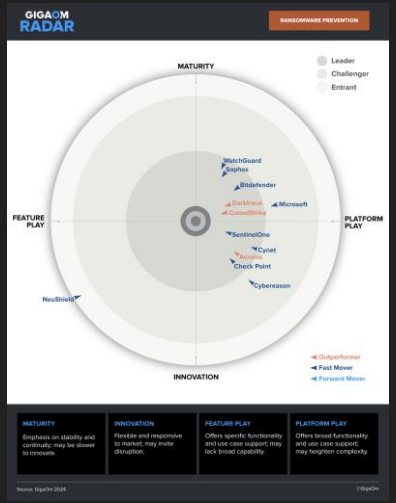
[2]Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CrowdStrike.

Chứng Thực Qua Các Bài Kiểm Tra Ngăn Chặn Ransomware

SE LABS
AAA
DECEMBER 2024
Advanced Security
EDR Protection

2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

Nền tảng CrowdStrike Falcon Đạt tỷ lệ Phát hiện, Ngăn chặn và Chính xác 100%



2024 GigaOm Radar for Ransomware Prevention

CrowdStrike Được vinh danh là một Leader và là vendor có Hiệu suất Vượt trội trong lĩnh vực Ngăn chặn Ransomware

SE LABS
AAA
JUL-SEPT 2024
ENTERPRISE ADVANCED SECURITY

SE Labs Q3 2024 Enterprise Advanced Security Test

CrowdStrike đạt Giải thưởng AAA, trở thành người chiến thắng duy nhất với điểm Chính xác Toàn diện 100%.

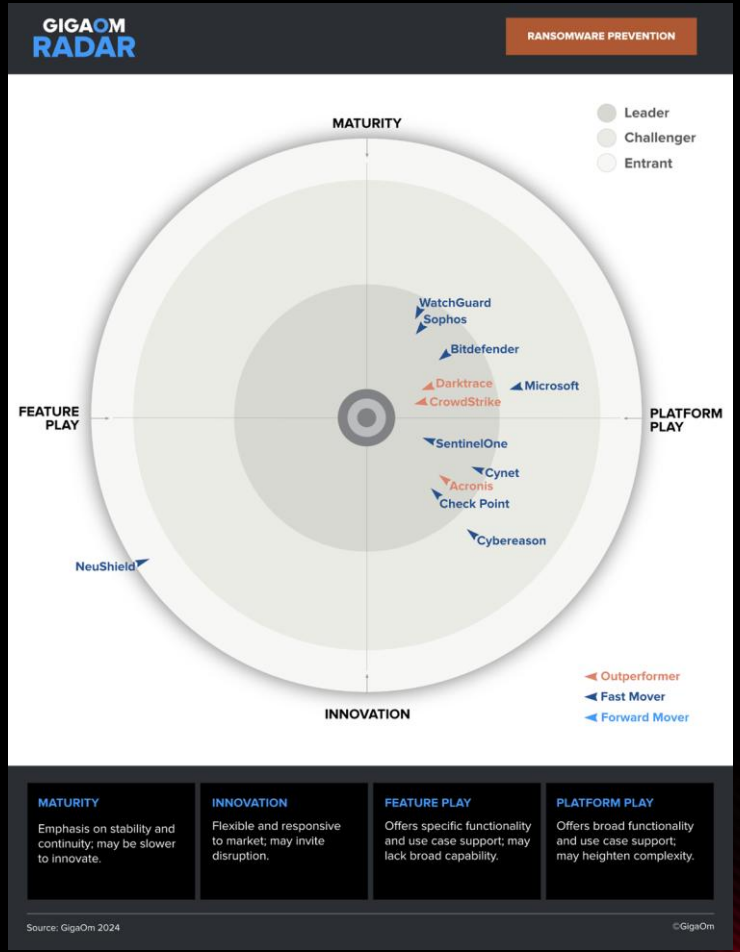
CrowdStrike Được vinh danh là một Leader và là vendor có Hiệu suất Vượt trội trong lĩnh vực Ngăn chặn Ransomware

2024 GigaOm Radar for Ransomware Prevention

Giành được 10 điểm tuyệt đối và điểm số trung bình cao nhất trong số tất cả các vendor được đánh giá

> Nền tảng Falcon cho phép phát hiện, ngăn chặn và bảo vệ toàn diện khỏi ransomware.

GIGAOM



CrowdStrike đạt Giải thưởng AAA, trở thành người chiến thắng duy nhất với điểm Chính xác Toàn diện 100%.

SE Labs Q3 Enterprise Advanced Security Test

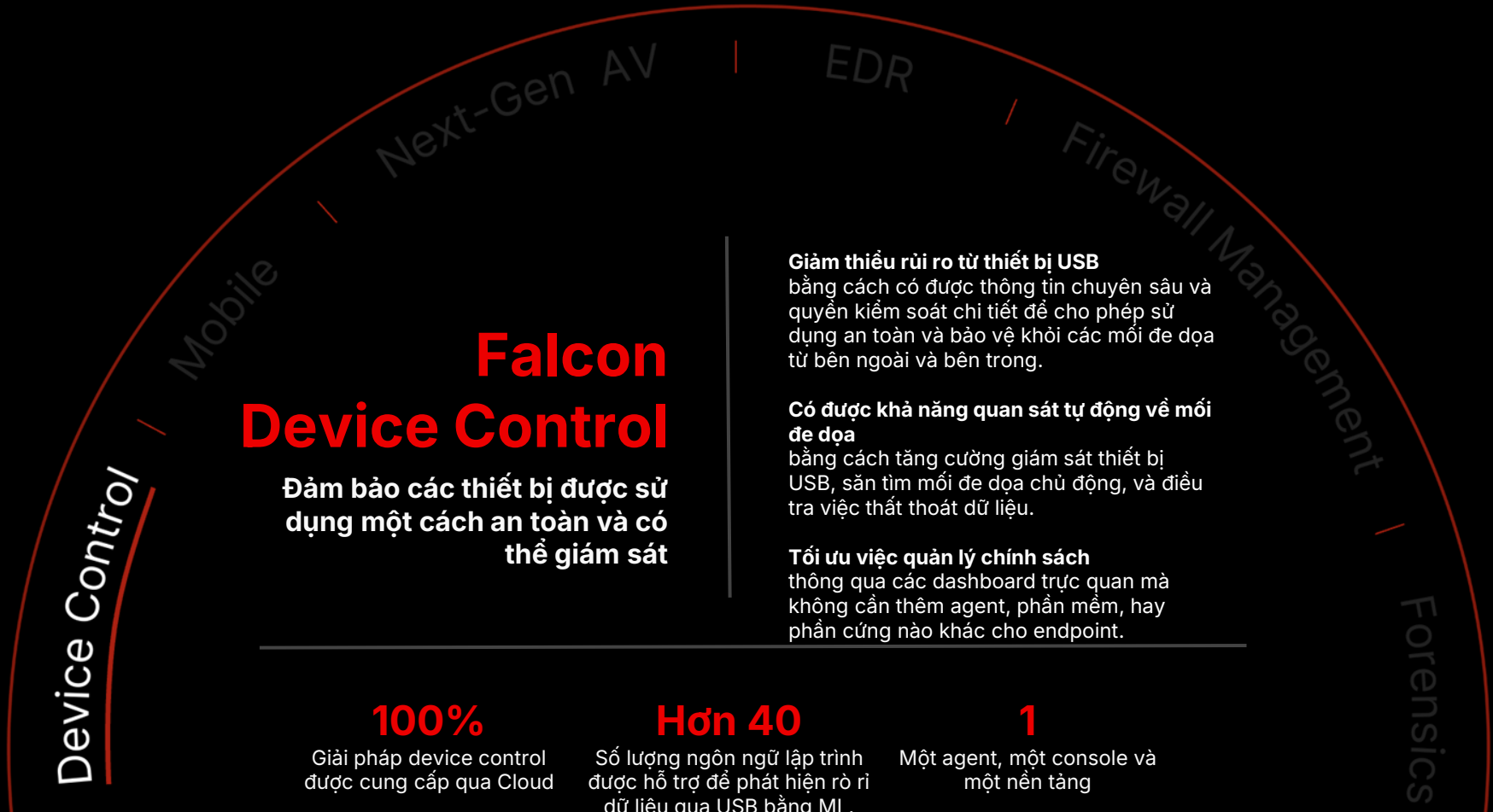
100% Độ chính xác trong Phát hiện
100% Độ chính xác đối với phần mềm Hợp lệ
100% Độ chính xác Tổng thể
0 False Positives

SE LABS

"CrowdStrike Falcon đã đạt được kết quả hoàn hảo trong bài kiểm tra này, phát hiện mọi yếu tố của từng mối đe dọa và không phạm bất kỳ sai lầm nào với các ứng dụng hợp lệ."

Endpoint Security Modules

Một Leader trong mảng Endpoint Security



Falcon Device Control

Đảm bảo các thiết bị được sử dụng một cách an toàn và có thể giám sát

Giảm thiểu rủi ro từ thiết bị USB
bằng cách có được thông tin chuyên sâu và quyền kiểm soát chi tiết để cho phép sử dụng an toàn và bảo vệ khỏi các mối đe dọa từ bên ngoài và bên trong.

Có được khả năng quan sát tự động về mối đe dọa
bằng cách tăng cường giám sát thiết bị USB, săn tìm mối đe dọa chủ động, và điều tra việc thất thoát dữ liệu.

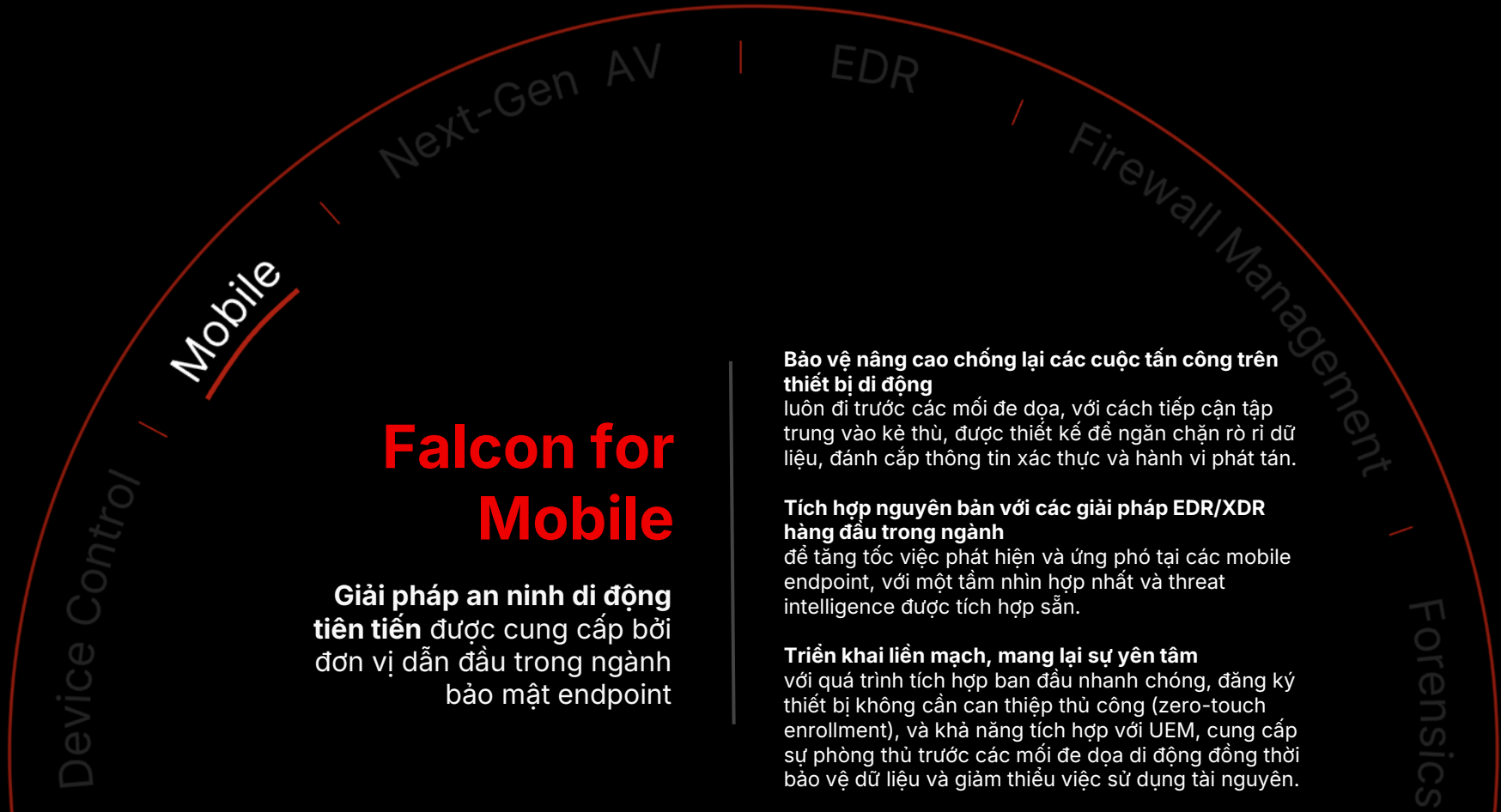
Tối ưu việc quản lý chính sách
thông qua các dashboard trực quan mà không cần thêm agent, phần mềm, hay phần cứng nào khác cho endpoint.

100%
Giải pháp device control được cung cấp qua Cloud

Hơn 40
Số lượng ngôn ngữ lập trình được hỗ trợ để phát hiện rò rỉ dữ liệu qua USB bằng ML.

1
Một agent, một console và một nền tảng

CROWDSTRIKE



Falcon for Mobile

Giải pháp an ninh di động tiên tiến được cung cấp bởi đơn vị dẫn đầu trong ngành bảo mật endpoint

Bảo vệ nâng cao chống lại các cuộc tấn công trên thiết bị di động
luôn đi trước các mối đe dọa, với cách tiếp cận tập trung vào kẻ thù, được thiết kế để ngăn chặn rò rỉ dữ liệu, đánh cắp thông tin xác thực và hành vi phát tán.

Tích hợp nguyên bản với các giải pháp EDR/XDR hàng đầu trong ngành
để tăng tốc việc phát hiện và ứng phó tại các mobile endpoint, với một tầm nhìn hợp nhất và threat intelligence được tích hợp sẵn.

Triển khai liền mạch, mang lại sự yên tâm
với quá trình tích hợp ban đầu nhanh chóng, đăng ký thiết bị không cần can thiệp thủ công (zero-touch enrollment), và khả năng tích hợp với UEM, cung cấp sự phòng thủ trước các mối đe dọa di động đồng thời bảo vệ dữ liệu và giảm thiểu việc sử dụng tài nguyên.

CROWDSTRIKE

Falcon Prevent

Khả năng ngăn chặn không đối thủ với AI đẳng cấp thế giới và thông tin tình báo về kẻ thù được tích hợp sẵn

Công nghệ ngăn chặn hiện đại nhất sử dụng AI/ML để chặn mã độc, các cuộc tấn công không cần file (fileless), và các cuộc tấn công zero-day. Threat Intelligence tinh nhuệ và khả năng quét nâng cao giúp phát hiện và chặn các hành vi độc hại từ sớm.

Bảo vệ toàn bộ hệ thống của bạn trong vài giây với sự bảo vệ tức thì từ agent siêu nhẹ của chúng tôi, cung cấp độ bao phủ cho tất cả các hệ điều hành phổ biến, dù đang online hay offline.

Tối ưu vận hành và thúc đẩy năng suất với các cảnh báo có độ chính xác cao, threat intelligence tích hợp và các workflow tự động hóa

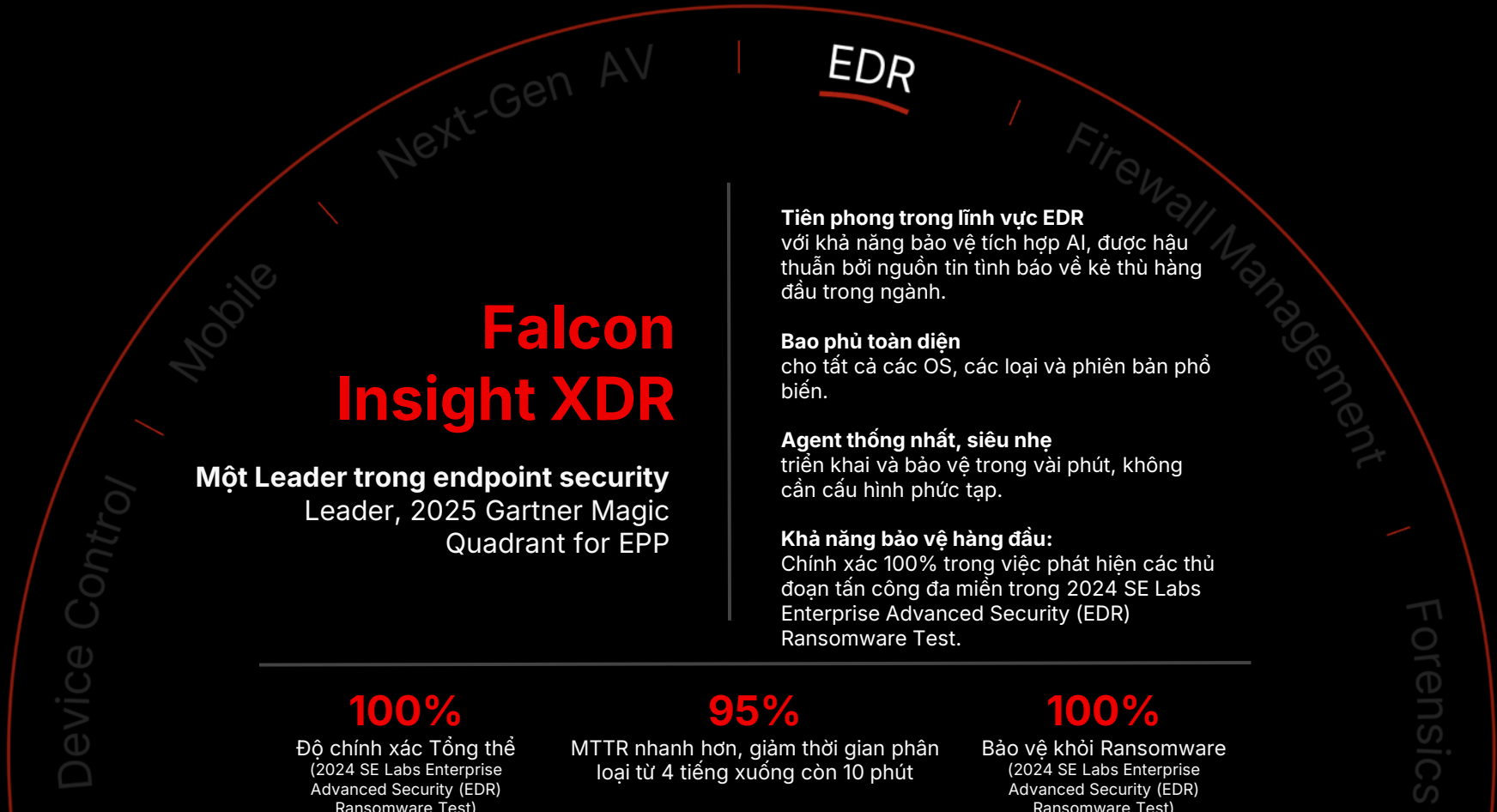
100%
Ngăn chặn Ransomware

Hơn 100K
Agent được triển khai trong một ngày

Ít hơn 1 năm
Để nhận thấy hiệu quả đầu tư (ROI)

[1] 2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test
[2] CrowdStrike Incident Response engagement with hospitality chain
[3] https://www.crowdstrike.com/wp-content/uploads/2022/08/crowdstrike-racv-case-study.pdf

CROWDSTRIKE



Falcon Insight XDR

Một Leader trong endpoint security
Leader, 2025 Gartner Magic Quadrant for EPP

Tiên phong trong lĩnh vực EDR
với khả năng bảo vệ tích hợp AI, được hậu thuẫn bởi nguồn tin tình báo về kẻ thù hàng đầu trong ngành.

Bao phủ toàn diện
cho tất cả các OS, các loại và phiên bản phổ biến.

Agent thống nhất, siêu nhẹ
triển khai và bảo vệ trong vài phút, không cần cấu hình phức tạp.

Khả năng bảo vệ hàng đầu:
Chính xác 100% trong việc phát hiện các thủ đoạn tấn công đa miền trong 2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test.

100%
Độ chính xác Tổng thể
(2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test)

95%
MTTR nhanh hơn, giảm thời gian phân loại từ 4 tiếng xuống còn 10 phút

100%
Bảo vệ khỏi Ransomware
(2024 SE Labs Enterprise Advanced Security (EDR) Ransomware Test)

CROWDSTRIKE

Falcon Firewall Management

Dễ dàng tạo và thực thi các chính sách tường lửa cho máy trạm (host firewall) với một agent duy nhất

Quản lý chính sách tường lửa đơn giản
cho Windows và macOS, với các mẫu (templates), các nhóm quy tắc có thể tái sử dụng và khả năng áp dụng thay đổi một cách nhanh chóng.

Giảm thiểu độ phức tạp
với agent Falcon siêu nhẹ và console hợp nhất, cho phép triển khai nhanh chóng và gây ảnh hưởng ở mức tối thiểu đến hiệu năng của máy.

Khả năng quan sát tức thì
với khả năng giám sát mạng tự động, nhận diện mối đe dọa và phát hiện sự bất thường, cộng thêm các chính sách tường lửa nhận biết theo ứng dụng và vị trí để tăng cường bảo mật.

CROWDSTRIKE

Falcon Forensics

Ứng phó và phục hồi
với khả năng thu thập, làm phong phú và tương quan hóa dữ liệu điều tra một cách tự động

Giảm thiểu độ phức tạp
với khả năng thu thập dữ liệu điều tra (forensic) tự động và các bảng dashboard toàn diện, giúp tăng cường chuyên môn của nhà phân tích để thực hiện phân tích sự cố một cách mạnh mẽ.

Có được một nền tảng hợp nhất
để đạt hiệu quả tối đa, với threat intelligence được tích hợp sẵn, ngữ cảnh phong phú cho các cuộc điều tra và các hành động ứng phó nhanh chóng để ngăn chặn và khắc phục.

Nhận được giá trị với các trường hợp sử dụng đa dạng
bao gồm săn tìm mối đe dọa, đánh giá tình trạng xâm nhập và phân tích rủi ro tài sản trong quá trình sáp nhập và mua lại (M&A).

1
Lightweight, dissolvable collector

6
dashboard toàn diện để tăng tốc các workflow

3
Nền tảng được hỗ trợ: Windows, macOS, và Linux

CROWDSTRIKE
CROWDSTRIKE