

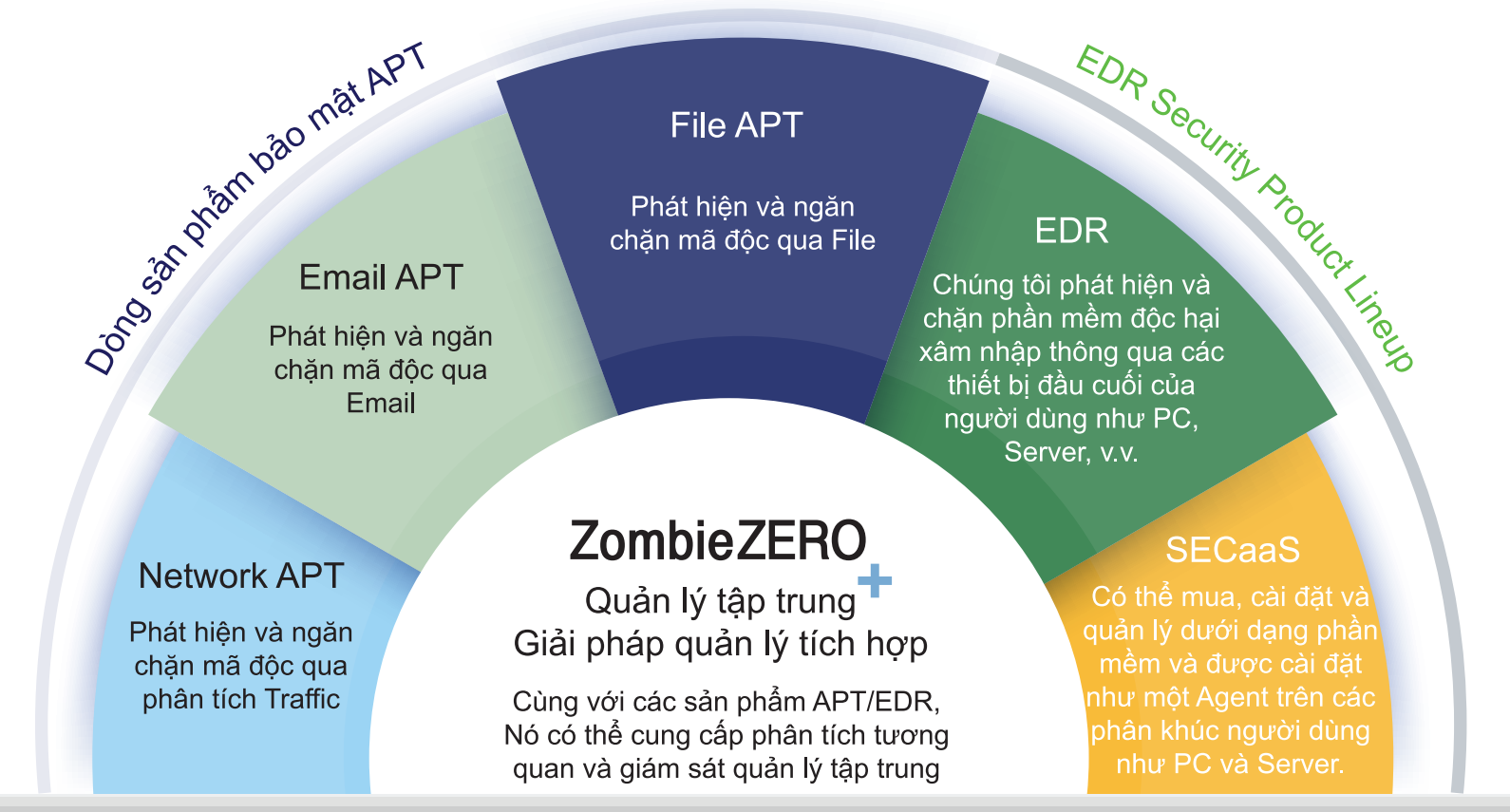
Zombie ZERO

Giải pháp dựa vào nền tảng AI để phát hiện và ngăn chặn mã độc mới, các biến thể và Ransomware.



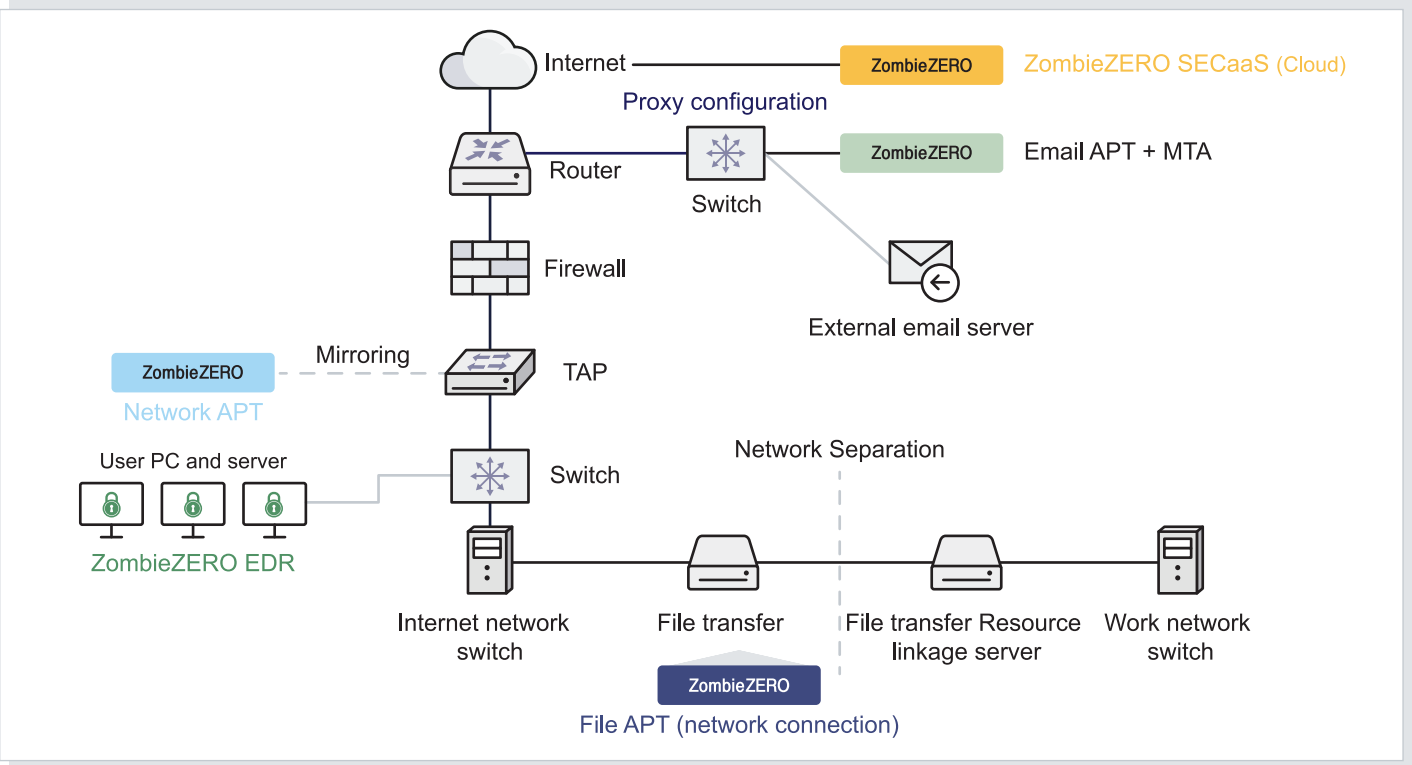
Chúng tôi tạo ra một môi trường bảo mật an toàn từ các mối đe dọa tấn công mạng.

Giải pháp bảo mật phân tích hành động dựa trên AI giúp phát hiện và chặn phần mềm độc hại mới và biến thể như ransomware và APT



ZombieZERO Hệ thống

- Giải pháp được xây dựng trên nhiều cách khác nhau mà qua đó phần mềm độc hại có thể xâm nhập vào hệ thống



| ZombieZERO APT

Giải pháp bảo mật tích hợp dựa trên thiết bị (HW+SW)

Network, Email và File (được xây dựng trong phần điều phối mạng)



Network APT

Phân tích hành vi bổ sung cho phân tích dựa trên signature-based
Khả năng lấp lỗ hổng zero-day mà hệ thống không phát hiện được

- Theo dõi lưu lượng mạng hai chiều đối với luồng vào và luồng ra của tệp
- Thu thập và phân tích các giao thức dịch vụ Internet chính
- Phát hiện và chặn quyền truy cập vào các trang web có hại và kết nối C&C



Email APT

Giải quyết các hạn chế của các giải pháp thư rác dựa trên signature-based để bị phần mềm độc hại tấn công

- Tích hợp APT với Message Transfer Agents (MTA)
- Chỉ chặn thông tin độc hại từ thư rác, lừa đảo trực tuyến và phần mềm độc hại
- Phân tích tệp đính kèm email và URL và chỉ gửi thư hợp pháp đến mail server



File APT

Khắc phục những hạn chế của các giải pháp thư rác chữ ký truyền thống để bị tấn công bởi các biến thể và mã độc mới

- Phân tích và chặn các tệp đang chuyển tiếp cùng với các giải pháp kết nối mạng
- Phân loại các tệp được phân tích và chỉ gửi những tệp được coi là bình thường tới mạng doanh nghiệp
- Cung cấp kết quả phân tích bằng các thư mục được chia sẻ (SMB, NFS, API Web, v.v.)

Kỳ vọng

- Khi các sản phẩm APT và EDR được triển khai đồng thời



Ứng phó với phần mềm độc hại và ransomware

Phát hiện và phản hồi đối với phần mềm độc hại biến thể mới chưa biết mà AV không thể phát hiện



Đảm bảo khả năng hiển thị điểm cuối

Khả năng hiển thị về tình huống cụ thể do tấn công mạng gây ra ở điểm cuối



Ngăn chặn sự xâm nhập của phần mềm độc hại có thể

Xác định đường dẫn nhập phần mềm độc hại và kết nối giữa các hệ thống để cải thiện bảo mật bằng cách và các lỗ hổng từ bên trong



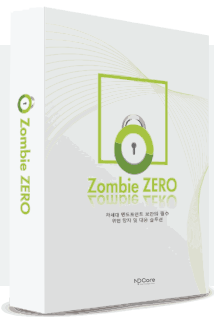
Giảm chi phí

Phát hiện Ransomware, Backup và tính năng chống virus không cần phải mua một sản phẩm riêng biệt

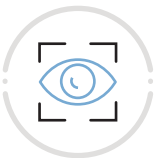


| ZombieZERO EDR

Triển khai tại chỗ / đám mây để phát hiện và chặn phần mềm độc hại xâm nhập qua các phân khúc người dùng như PC và máy chủ



Tính năng chính



Phát hiện và phản ứng theo thời gian thực đối với ransomware

- Chống mã hóa tập tin và giả mạo/giả mạo bởi ransomware
- Tích hợp API với 'Bitdefender'



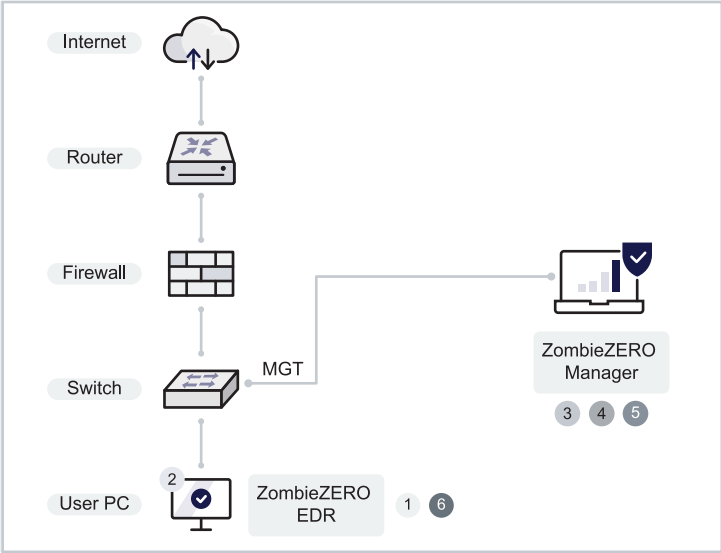
Zero Trust (Execution pending)

- Tải thông tin lên máy chủ phân tích bằng cách tạm dừng thực thi tệp khi tệp mới được giới thiệu hoặc tệp đe dọa được thực thi



Phát hiện mối đe dọa theo thời gian thực dựa trên IOC

- Phát hiện các chỉ số thỏa hiệp (IOC) đối với hành vi của thiết bị người dùng (network, file, process, registry, etc.)

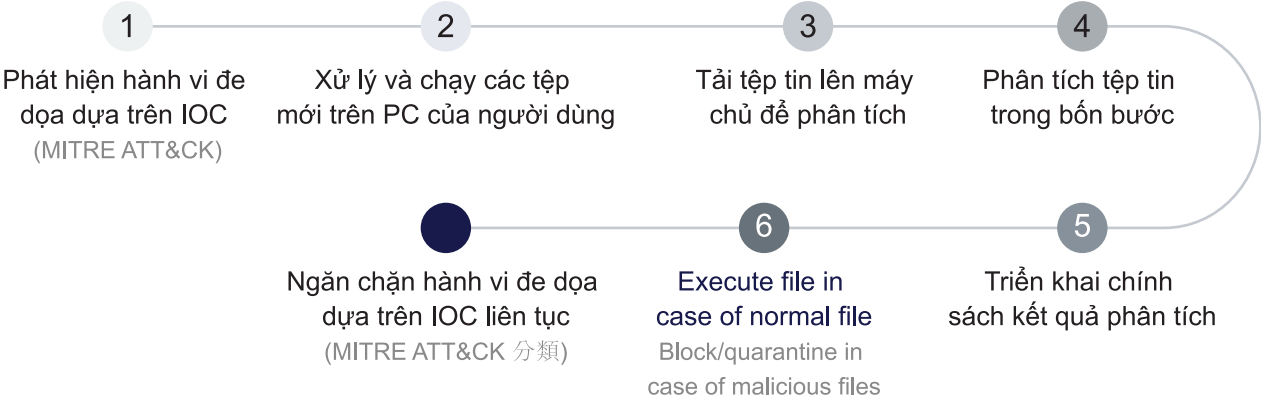


ZombieZERO SECaaS

ZombieZERO EDR Cloud Service

- Phát hiện các chỉ số thỏa hiệp (IOC) đối với hành vi của thiết bị người dùng
- Đầy đủ chức năng bao gồm mua, cài đặt và quản lý tập trung trên web
- Khả năng quản lý người dùng cao và tiện lợi, không tốn chi phí H/W
- Thích hợp cho các doanh nghiệp vừa và nhỏ và môi trường làm việc từ xa

Lưu đồ khả năng phát hiện và phân tích của EDR




ZombieZERO UI

- Sắp xếp bố cục với thiết kế trực quan để quản trị viên có thể dễ dàng tìm thấy thông tin họ đang tìm kiếm
- Áp dụng thiết kế trực quan giúp người quản trị nhận biết tình huống nhanh và chính xác
- Tăng cường bảo mật với xác thực và kiểm soát quyền để đảm bảo chỉ những người dùng được ủy quyền mới có quyền truy cập




Các tính năng phổ biến chính

phân tích đa chiều




AV- Phát hiện và phân tích đa chiều bao gồm phân tích tĩnh, động và định danh

Ngăn chặn bỏ qua máy ảo




Cung cấp các phân tích hành vi động giống như máy thật

MITRE ATT&CK




Phát hiện phần mềm độc hại theo tiêu chí MITRE ATT&CK

Biểu đồ Malware




Chức năng chi tiết và giám sát các loại tấn công dựa trên các chỉ số thỏa hiệp (IOC)

Công thức ECSC



Tích hợp với Trung tâm an toàn mạng của Bộ Giáo dục Quy tắc Yara

Phát hiện mã độc dựa trên AI



Công nghệ phát hiện mã độc nhanh và chính xác dựa trên AI

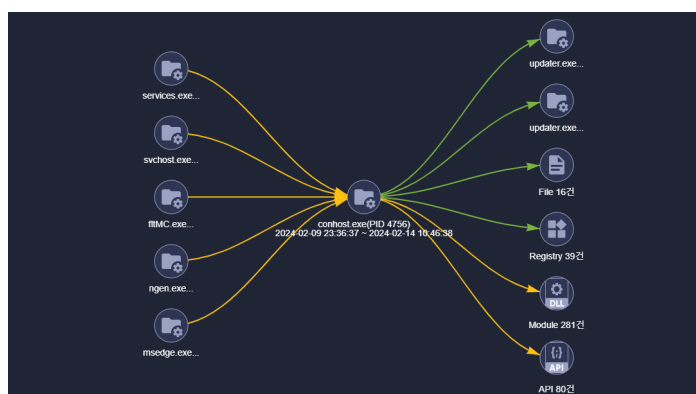
Phân tích đa chiều

- Phát hiện và chặn mã độc bằng phân tích đa chiều lưu lượng truy cập qua mạng của bạn từ bên ngoài vào bên trong.



MITRE ATT&CK · Sơ đồ hành vi mã độc

- Theo dõi hình thức của các kỹ thuật và phương pháp đối với các cuộc tấn công đang diễn ra, không phải kết quả của các cuộc tấn công



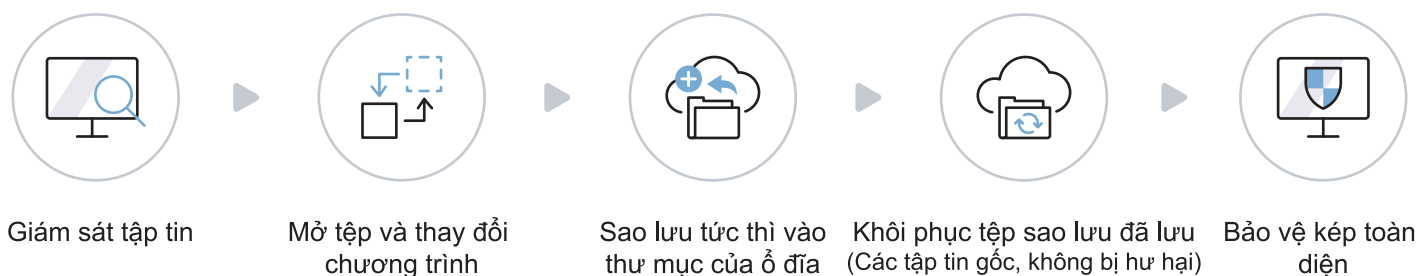
Thông tin phân tích quy trình
(sơ đồ hành vi mã độc)



Điều hướng MITRE ATT&CK

Sao lưu thời gian thực

- Sao lưu tệp vào thư mục bảo mật không thể truy cập được bằng quy trình thông thường vào phút cuối trước khi mã hóa tệp
- Sao lưu và thực thi ở cấp trình điều khiển Kernel, loại bỏ xung đột giữa các ứng dụng và suy giảm hiệu suất



References

Số 1 về APT tại Hàn Quốc với hơn 150 khách hàng tại Hàn Quốc và nước ngoài



Giấy chứng nhận và bằng sáng chế

NPCore có chứng nhận GS, chứng nhận chức năng bảo mật, ISO9001 và chứng nhận sản phẩm đổi mới, đồng thời đã đăng ký 15 bằng sáng chế, trong đó có 2 bằng sáng chế ở Mỹ và 1 ở Nhật Bản.



Security Functionality Certificate

ISO 9001 : 2015

GS Certificate 1st Grade

Patent in US

Certificate of The Innovative Product

