Mi2
PARTNERING SUCCESS

BỘ GIẢI PHÁP
BẢO VỆ DỮ LIỆU TOÀN DIỆN

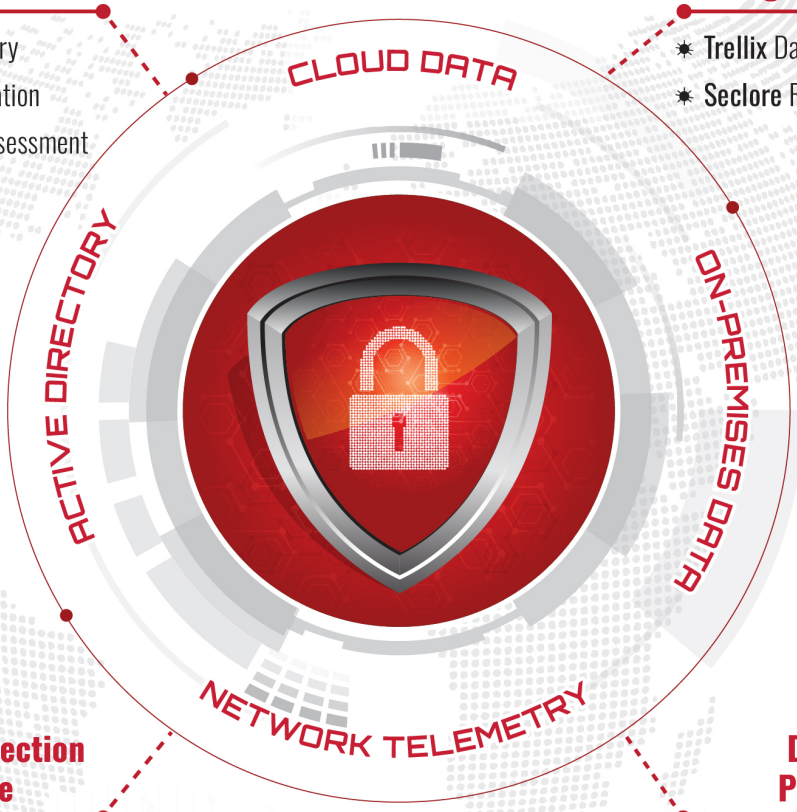
Complete Data Protection Solution

Data Discovery & Classification

- **Varonis** Data Discovery
- **Fortra** Data Classification
- **Varonis** Data Risk Assessment

Data Encryption & Right Management

- **Trellix** Data Encryption
- **Seclore** Right Management



Data Threat Detection & Response

- **Varonis** Data Usage Insight (UEBA)
- **Varonis** Threat Detection & Response

Data Loss Prevention

- **Trellix** Data Loss Prevention

www.mi2.com.vn

RÀ QUÉT, KHÁM PHÁ KIỂM KÊ DỮ LIỆU HỆ THỐNG

Giải pháp cung cấp sẵn 01 engine thực thi rà quét, kiểm kê và khám phá dữ liệu đã và đang lưu trữ trên toàn bộ các hệ thống data repo (File Server, NAS, Sharepoint, Database,...) của tổ chức.

Engine rà quét, kiểm kê dữ liệu cho phép thiết lập tối ưu hóa cho tổ chức bao gồm:

* Built-in sẵn bộ thư viện Data Discovery lớn (**khoảng hơn 400+ rule nhận diện**), giúp dễ dàng phát hiện và định danh dữ liệu theo các chuẩn tuân thủ tương ứng.
* Dễ dàng **xây dựng bộ pattern** cho các dữ liệu quan trọng riêng của tổ chức.
* Engine cũng có khả năng **nhận diện các thông tin nhạy cảm** trong hệ thống như **Passwords, Database credentials, Connection strings, Private keys, Encryption certificates, API keys, Authentication tokens, Encryption keys,...**
* Khả năng **thiết lập quét theo lịch**, đảm bảo **khả năng kiểm kê/khám phá liên tục** và mềm dẻo theo nhu cầu.
* Khả năng thực thi **quét dạng Incremental Scan, giúp tối ưu hóa** kiểm kê dữ liệu hệ thống.

Với kết quả kiểm kê, khám phá dữ liệu, tổ chức sẽ có cái nhìn toàn cảnh về dữ liệu và việc lưu trữ trong tổ chức:

* Hệ thống data repo đang lưu trữ **như thế nào.**
* Dữ liệu quan trọng của tổ chức đang lưu trữ **ở đâu, vị trí nào.**
* Dữ liệu quan trọng đã và đang được **thiết lập kiểm soát bảo mật, truy cập ra sao.**
* Có hay không dữ liệu quan trọng đã và đang **tiềm ẩn nguy cơ, rủi ro bảo mật (có khả năng truy cập bất hợp pháp).**

Từ đó giúp định hình và chuẩn bị phương án về bảo mật cho dữ liệu trong các bước tiếp theo.

PHÂN LOẠI VÀ GÁN NHÃN DỮ LIỆU HỆ THỐNG

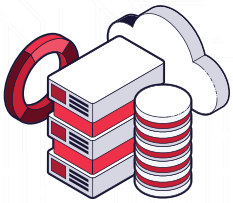
Để bảo vệ dữ liệu một cách hiệu quả nhất, dữ liệu trong hệ thống cần được phân loại theo các mức độ quan trọng khác nhau và được gán nhãn rõ ràng, giúp người dùng và hệ thống có thể nhận diện và thực thi theo chính sách bảo mật đã thiết lập.

Giải pháp phân loại và gán nhãn dữ liệu theo nhiều tiêu chí khác nhau:

- Mức độ phân loại
- Phòng ban sở hữu
- Phạm vi sử dụng

Hoặc kết hợp các tiêu chí liên quan.

Dữ liệu được phân loại và gán nhãn xong thì nhãn sẽ được bổ sung vào header, footer, watermark, metadata của tài liệu.



1 PHÂN LOẠI GÁN NHÃN DỮ LIỆU TRÊN DATA REPO

Lập lịch để tự động hóa tác vụ rà quét dữ liệu trên hệ thống lưu trữ dữ liệu. Với các dữ liệu matching theo các tiêu chí đặt ra (như đường dẫn lưu trữ, kiểu file, data owner, tên file, nội dung của file,...), công cụ sẽ tự động phân loại và gán nhãn theo chính sách phân loại dữ liệu.

2 PHÂN LOẠI GÁN NHÃN DỮ LIỆU TRÊN MÁY TRẠM

Khi người dùng của khách hàng sử dụng các chương trình trong bộ Microsoft Office để tạo ra dữ liệu (tạo và lưu - save), thành phần phân loại dữ liệu trên máy trạm sẽ yêu cầu người dùng phân loại và gán nhãn cho dữ liệu này.

Khi dữ liệu được tạo ra, người dùng bắt buộc phải phân loại dữ liệu (Lựa chọn phòng ban, mức độ quan trọng) thì mới có thể lưu dữ liệu. Tính năng đảm bảo mọi dữ liệu đều được phân loại và chuẩn hóa.

Người quản trị có thể thiết lập các chính sách cho phép/không cho phép/cảnh báo,... khi người dùng thay đổi nhãn phân loại dữ liệu, đồng thời lưu thông tin người dùng đã thay đổi nhãn để phục vụ quá trình điều tra, quy trách nhiệm khi cần.

MÃ HOÁ DỮ LIỆU

Giải pháp đảm bảo chỉ những người liên quan mới được truy cập vào dữ liệu theo mức độ quan trọng khác nhau, đảm bảo tính an toàn, bí mật cho dữ liệu quan trọng.

Mã hóa toàn bộ ổ cứng

Mã hóa toàn bộ ổ cứng dữ liệu

Sử dụng thuật toán mã hóa mạnh chuẩn quốc tế AES-256, đảm bảo dữ liệu trên ổ cứng luôn được bảo mật ngay cả khi máy tính/laptop/ổ cứng bị mất. Cho phép tùy chọn các vùng được mã hóa tùy mục đích khác nhau.

Kiểm soát truy cập dữ liệu mạnh mẽ

Sử dụng công nghệ kiểm soát truy cập mạnh Preboot Authentication để xác thực người dùng được phép truy cập vào ổ cứng dữ liệu đã được mã hóa. Hỗ trợ tích hợp xác thực với các phương thức: Password, Token, Certificate,...

Hỗ trợ Single Sign On

Giải pháp mã hóa máy tính/laptop kết hợp nền tảng Multi factor authentication giúp đơn giản hoá việc thiết lập chế độ đăng nhập một lần Single Sign On khi tích hợp với tài khoản Active Directory và vẫn đảm bảo an toàn, bí mật.

Mã hóa/giải mã trong suốt với người dùng

Dữ liệu trên ổ cứng chỉ được giải mã khi người dùng xác thực thành công với hệ thống mã hóa. Quá trình mã hóa và giải mã diễn ra nhanh chóng, không ảnh hưởng đến hiệu suất hoạt động hay thao tác sử dụng của người dùng.

Tăng tốc mã hóa với công nghệ AES-NI

Giải pháp mã hóa dữ liệu máy tính/laptop có khả năng tích hợp với thế hệ CPU mới (Core I3, I5) tăng tốc quá trình mã hóa, giải mã cũng như xử lý dữ liệu.

Mã hóa File/Folder File Server và USB

Mã hóa dữ liệu

Sử dụng thuật toán, engine mã hóa mạnh bao gồm AES 256 Bits FIPS 140-2 để ngăn chặn hành vi truy cập bất hợp pháp các thông tin quan trọng được mã hóa.

Duy trì tính bí mật toàn diện

Tính năng đảm bảo dữ liệu luôn được mã hóa bất kể dữ liệu đó được copy, move hay được truyền/gửi đến bất kỳ vị trí nào thông qua bất kỳ phương thức/giao thức nào.

Thiết lập chính sách mã hóa tự động

Cho phép người quản trị định nghĩa chính sách mã hóa tự động. Với chính sách này, khi dữ liệu được tạo ra sẽ tự động được mã hóa dựa trên ứng dụng hoặc vị trí.

Hỗ trợ chính sách dựa trên người dùng

Mỗi vai trò khác nhau sẽ có khóa và chính sách mã hóa riêng. Khi người dùng xác thực và truy cập vào hệ thống Active Directory thành công, khóa và chính sách mã hóa sẽ được tải về và thiết lập cho người dùng này.

Hỗ trợ cơ chế chia sẻ khóa dùng chung

Giải pháp đảm bảo người dùng trong nhóm/phòng có thể chia sẻ được tài liệu cho nhau, trong khi vẫn đảm bảo tính bí mật của tài liệu đối với các người dùng khác.

GIẢI PHÁP PHÒNG CHỐNG THẤT THOÁT DỮ LIỆU

Các module phòng chống thất thoát dữ liệu giúp tổ chức giám sát, phát hiện, và ngăn chặn việc truyền gửi dữ liệu quan trọng ngoài chính sách bảo mật.

» Chúng được triển khai từ máy trạm đến mạng/gateway và Cloud.

DLP - MONITOR

- Giám sát -
- Cảnh báo -
- Capture thông tin truyền gửi -

» Định danh các hành vi truyền gửi vi phạm chính sách

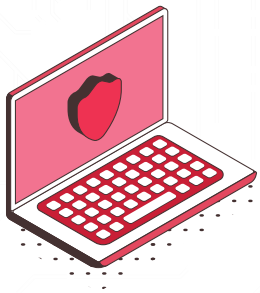
DLP Monitor sử dụng cổng Span trên Core Switch để định danh hành vi vi phạm chính sách. Nó ghi lại toàn bộ luồng dữ liệu, phân tích thời gian thực, và lưu bằng chứng cho các vi phạm. Báo cáo chi tiết giúp ngăn chặn mất mát dữ liệu và bảo vệ thông tin tổ chức.

» Khả năng capture, điều tra trong quá khứ và tinh chỉnh Policy

Trellix DLP nổi bật với khả năng capture và lưu trữ dữ liệu truyền gửi, tạo điểm mạnh cho triển khai DLP hiệu quả. Sử dụng công nghệ Capture, Trellix DLP cho phép tạo và kiểm thử chính sách trực tiếp trên dữ liệu đã được capture, giúp quản trị viên đánh giá hiệu quả chính sách nhanh chóng và linh hoạt. Điều này được Gartner đánh giá cao cho việc xây dựng chính sách DLP hiệu quả.

DLP - PREVENT

Chống thất thoát dữ liệu qua kênh Web/Mail



DLP Prevent tích hợp với Web Proxy để bảo vệ dữ liệu trên luồng Web

Khi người dùng truy cập internet, Web Proxy gửi yêu cầu tới DLP qua ICAP. DLP xác định hành động và thông tin qua X-Header. Web Proxy dựa vào X-Header để thực hiện biện pháp bảo vệ, như ngăn chặn hoặc cho phép truy cập.

Khả năng capture, tối ưu chính sách và điều tra an ninh

NDLP Monitor và **NDLP Prevent** ghi lại toàn bộ traffic, hỗ trợ xây dựng và kiểm tra chính sách nhanh chóng. Cả hai cũng cho phép điều tra hành vi truyền gửi dữ liệu trong quá khứ.

DLP Prevent tích hợp với Email Gateway để bảo vệ dữ liệu trên luồng email

DLP xác định hành động, sau đó thông qua gắn thẻ X-header, Email Gateway thực hiện các biện pháp bảo vệ tương ứng.

Các module phòng chống thất thoát dữ liệu giúp tổ chức giám sát, phát hiện, và ngăn chặn việc truyền gửi dữ liệu quan trọng ngoài chính sách bảo mật.

» Chúng được triển khai từ máy trạm đến mạng/gateway và Cloud.

GIẢI PHÁP PHÒNG CHỐNG THẤT THOÁT DỮ LIỆU

DLP - CLOUD

Chống thất thoát dữ liệu mức Cloud

Phòng chống thất thoát dữ liệu trên môi trường Cloud.

Trellix/Skyhigh là thành phần DLP Cloud, tích hợp với Gsuite, O365, Box, Dropbox để giám sát và ngăn chặn việc chia sẻ dữ liệu từ môi trường cloud qua email.

Giám sát, kiểm soát việc lưu trữ dữ liệu trên Cloud.

Trellix/Skyhigh giám sát và phát hiện việc người dùng tải lên dữ liệu quan trọng của tổ chức lên các nền tảng lưu trữ cloud như OneDrive, Google Drive và thực thi xử lý đối với các trường hợp vi phạm chính sách.

Giám sát, kiểm soát việc chia sẻ và tương tác dữ liệu qua môi trường Cloud.

Trellix/Skyhigh giám sát liên tục và kiểm soát việc người dùng chia sẻ dữ liệu quan trọng ra bên ngoài một cách bất hợp pháp qua kênh lưu trữ chia sẻ.

Giám sát hành vi người dùng, phát hiện các trường hợp thỏa hiệp.

Trellix/Skyhigh giám sát liên tục hành vi người dùng trên hạ tầng Cloud bằng công nghệ machine learning. Nó định danh và phát hiện insider threats, compromised account, và hành vi bất thường của người dùng đặc quyền trên cloud.

DLP - ENDPOINT

Chống thất thoát dữ liệu tại máy trạm

Dò quét định danh tài nguyên quan trọng trên máy trạm «

Trellix DLP Endpoint dò quét và bảo vệ dữ liệu trực tiếp trên máy trạm người dùng, làm cho quá trình này nhanh chóng và hiệu quả hơn so với các đối thủ.

Chống thất thoát dữ liệu toàn diện cho máy trạm «

Trellix DLP Endpoint bảo vệ toàn diện trên nhiều kênh truyền gửi từ máy trạm, ngăn chặn việc truyền gửi dữ liệu qua web, email, P2P, IM và các hành vi lẩn tránh, thậm chí ở chế độ Safemode.

GIÁM SÁT PHÂN TÍCH PHÁT HIỆN XỬ LÝ ĐE DỌA

01 Phát hiện định danh các bất thường liên quan đến truy cập vào dữ liệu.

02 Phát hiện định danh các đe dọa bên trong hệ thống và ransomware.

03 Phát hiện định danh các trường hợp data exfiltration.

04 Tự động hóa xử lý/sửa chữa khi phát hiện các đe dọa an ninh dữ liệu.

» Giám sát, phân tích chuyên sâu các hành vi tương tác, sử dụng đối với dữ liệu/tài liệu bên trong hệ thống - Áp dụng machine learning để định danh các hành vi bất thường và xử lý dữ liệu.

TỰ ĐỘNG VÀ LIÊN TỤC ĐỊNH DANH RỦI RO DỮ LIỆU

Giải pháp thiết lập tự động và liên tục khám phá thêm dữ liệu, các thiết lập mới (phân quyền, cập nhật quyền), từ đó đánh giá và xác định các rủi ro mới đối với dữ liệu và có thể thực thi hành vi phản ứng (tự động theo playbook hoặc thủ công).

TỰ ĐỘNG GIÁM SÁT VÀ PHÂN TÍCH HÀNH VI NGƯỜI DÙNG, PHÁT HIỆN BẤT THƯỜNG VÀ XỬ LÝ

Giải pháp tự động thu thập thông tin từ nhiều nguồn khác nhau và không giới hạn. Thực thi dựa trên bộ luật định danh bất thường, kết hợp học máy và dịch vụ chuyên gia chính hãng, giúp định danh và cảnh báo các mối đe dọa có rủi ro cao đối với dữ liệu của tổ chức.

THỰC THI XỬ LÝ VỚI PLAYBOOK TỐI ƯU TỪ CHÍNH HÃNG

Với mối đe dọa đã được định danh, giải pháp cung cấp best practice để xử lý. Cung cấp khả năng thiết lập tự động hóa và đảm bảo an toàn khi thực thi bao gồm:

» Khả năng thiết lập yêu cầu và phê duyệt để áp dụng hành vi xử lý tự động hóa.

» Review, đánh giá mức độ ảnh hưởng trước khi áp dụng hành vi xử lý tự động hóa.

GIẢI PHÁP QUẢN TRỊ VÀ VẬN HÀNH TẬP TRUNG

» Giám sát, phân tích chuyên sâu các hành vi tương tác, sử dụng đối với dữ liệu/tài liệu bên trong hệ thống - Áp dụng machine learning để định danh các hành vi bất thường và xử lý dữ liệu.

» TRELLIX EPO:

Quản lý tập trung toàn bộ các module về phân loại dữ liệu, mã hóa dữ liệu, phòng chống thất thoát dữ liệu cũng như quản lý các incident gây thất thoát dữ liệu.

» VARONIS:

Quản lý toàn bộ tập trung các module về kiểm kê, khám phá dữ liệu, giám sát và phân tích toàn bộ hành vi tương tác với dữ liệu, phân tích, định danh các rủi ro/đe dọa (trong nội bộ: Insiders, compromised account) liên quan đến dữ liệu và thực thi hành động phản ứng/xử lý tương ứng.

Hệ thống quản trị có khả năng tích hợp với các hệ thống vận hành an ninh tập trung (SIEM, SOAR) giúp đảm bảo khả năng giám sát tập trung, điều tra và xử lý sự cố an ninh tập trung cho toàn hệ thống.