COMPLETED DATA PROTECTION SOLUTION

Contents

1. Nhu cầu và yêu cầu bảo mật dữ liệu toàn diện

Dữ liệu luôn là tài sản quý giá nhất của tổ chức, đặc biệt là các tổ chức hoạt động trong lĩnh vực tài chính, ngân hàng. Các thông tin quan trọng, nhạy cảm, nếu bị lộ ra bên ngoài, sẽ ảnh hưởng rất lớn đến công việc kinh doanh của tổ chức. Cùng với sự phát triển của công nghệ thông tin, phương thức truyền gửi dữ liệu, trao đổi thông tin cũng như các kênh/giao thức ngày càng đa dạng, kéo theo phát sinh càng nhiều nguy cơ mất thông tin, lộ thông tin quan trọng ra bên ngoài tổ chức. Dưới đây là các nguy cơ, đe dọa đối với dữ liệu quan trọng mà một tổ chức thường gặp phải:

- Các thiết lập yếu/ sai đối với dữ liệu và hệ thống lưu trữ dữ liệu
  - Các hệ thống lưu trữ dữ liệu tập trung (File Server, Sharepoint, …) đang thiết lập và phân quyền chưa đúng (yếu/sai) dẫn đến nhiều trường hợp dữ liệu quan trọng có thể bị truy cập bất hợp pháp, hoặc vô tình bị lộ ra.
  - Dữ liệu quan trọng trong suốt quá trình sửa dụng có thể được lưu trữ ở các vị trí không an toàn, tiềm ẩn nguy cơ bị truy cập bất hợp pháp.
- Các hành vi vô tình của người dùng:
  - Các thiết bị cá nhân như laptop, mobile bị mất hoặc được đem đi bảo hành, bảo trì tại những cửa hàng không tin cậy,… Trên ổ cứng của các thiết bị này chứa nhiều thông tin quan trọng của ngân hàng, dễ dàng bị lấy ra.
  - Các máy trạm bị nhiễm mã độc (Trojans, key loggers, malware, …) hoặc bị thỏa hiệp. Các mã độc này âm thầm thực thi các hành vi xấu như: Truy cập vào các dữ liệu quan trọng, thu thập và gửi dữ liệu trái phép ra ngoài mà bản thân người sử dụng không biết.
  - Copy một số dữ liệu quan trọng của ngân hàng ra các thiết bị ngoại vi như ổ USB để gửi cho đồng nghiệp, sau đó quên không xóa mà lại cho một người khác mượn.
- Các hành vi cố ý của người dùng:
  - Hệ thống CNTT của Doanh nghiệp khi áp dụng một số biện pháp bảo mật cũng sẽ hạn chế ít nhiều đến sự tự do của từng cá nhân. Vì vậy, một số người sẽ cố ý sử dụng một số biện pháp nhằm vượt qua các hệ thống bảo vệ. Các hành vi cố ý này sẽ trực tiếp hoặc gián tiếp tạo ra các kênh để dữ liệu nhạy cảm của Doanh nghiệp lọt ra ngoài.
  - Một số người dùng bất mãn trong công ty có thể tìm cách truy cập và đánh cắp các thông tin nhạy cảm để mang ra ngoài.

Để đảm bảo tính an toàn cho dữ liệu của tổ chức trước các nguy cơ bị khám phá cũng như bị thất thoát ra bên ngoài một cách bất hợp pháp đã đề cập ở trên, Tổ chức cần được trang bị một giải pháp bảo mật dữ liệu tổng thể, giải pháp bảo mật dữ liệu tổng thể này phải đáp ứng tối thiểu các yêu cầu:

- **Yêu cầu về việc nắm bắt và hiểu được dữ liệu:** Dữ liệu đang lưu trữ ở đâu, gồm những dữ liệu gì, ...
- **Yêu cầu về phân loại và gán nhãn cho dữ liệu:** Phân loại và gán nhãn dữ liệu theo mức độ quan trọng.
- **Yêu cầu về mã hóa đảm bảo tính bí mật cho dữ liệu:** Mã hóa và kiểm soát người dùng truy cập vào dữ liệu.
- **Yêu cầu về phòng chống thất thoát dữ liệu:** Phát hiện và ngăn chặn các hành vi gây thất thoát dữ liệu ra bên ngoài.
- **Yêu cầu về phát hiện đe dọa liên quan đến dữ liệu và xử lý:** Giám sát, phân tích liên tục, định danh và xử lý các đe dọa liên quan đến dữ liệu quan trọng của tổ chức.

2. Đề xuất giải pháp bảo mật dữ liệu tổng thể

Với những rủi ro, đe dọa đối với dữ liệu đã đề cập, các yêu cầu định hướng để bảo vệ dữ liệu hiệu quả cho tổ chức, chúng tôi đề xuất bộ giải pháp bảo mật tổng thể, đảm bảo khả năng bảo vệ toàn diện cũng như vận hành bảo mật hiệu quả, tối ưu.

Giải pháp bảo mật dữ liệu toàn diện đề xuất bao gồm:

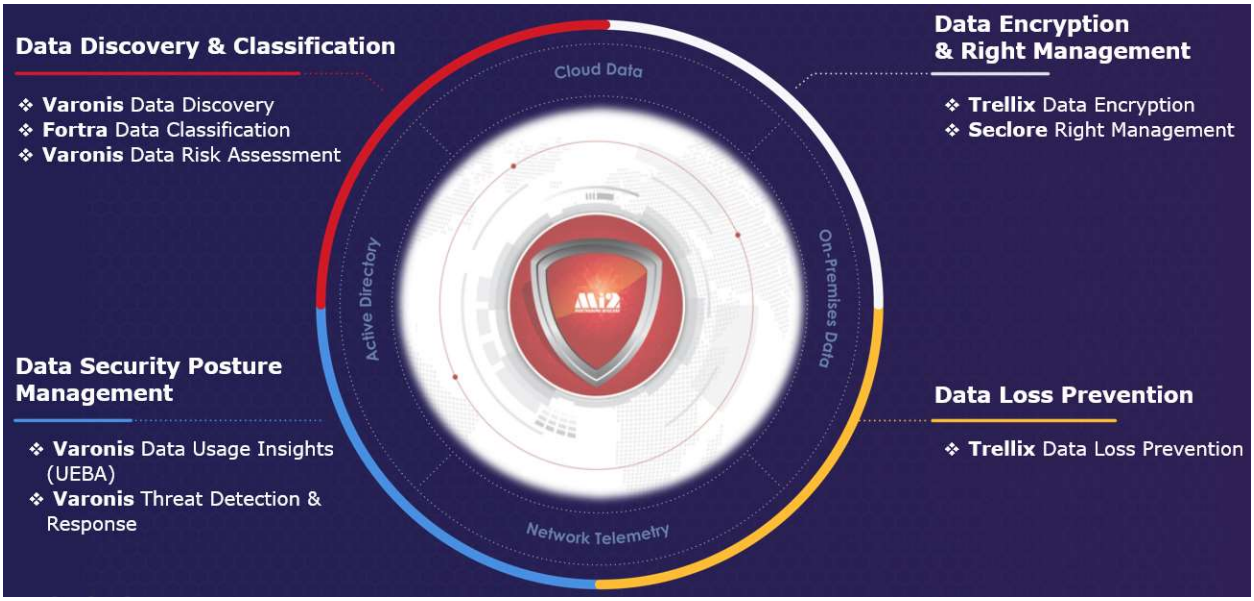


Figure 1: Completed Data Protection Platform

- **Khám phá, kiểm kê dữ liệu (Varonis – Data Discover & Inventory**): Thực thi kiểm kê và khám phá dữ liệu đã và đang lưu trữ trên các hệ thống lưu trữ tập trung bao gồm đầy đủ từ dữ liệu nào, lưu trữ ở đâu, đang được phân quyền thế nào, … giúp tổ chức dễ dàng nhận diện các dữ liệu của tổ chức đang được lưu trữ cũng như định danh các rủi ro tiềm ẩn liên quan.
- **Phân loại, đánh nhãn và chuẩn hóa dữ liệu (Fortra - Data Classification & Labeling):** Thực thi phân loại, chuẩn hóa và gán nhãn dữ liệu dựa trên mức độ quan trọng của dữ liệu, dựa theo phòng ban sở hữu dữ liệu,… đảm bảo tính dễ dàng quản lý và đưa ra các biện pháp/chính sách bảo vệ dữ liệu một cách phù hợp nhất, đồng thời hỗ trợ tổ chức đạt được các yêu cầu tuân thủ về ISO.
- **Khả năng mã hóa và kiểm soát truy cập dữ liệu (Trellix – Data Encryption):** Thực thi mã hóa dữ liệu, ngăn chặn việc truy cập/khám phá nội dung dữ liệu bất hợp pháp. Đảm bảo tính bí mật/riêng tư dữ liệu của tổ chức.

- **Khả năng giám sát, phát hiện và ngăn chặn thất thoát dữ liệu (Trellix - Data Loss Prevention):** Giám sát, phân tích các hành vi truyền gửi dữ liệu, phát hiện và ngăn chặn các hành vi truyền gửi dữ liệu vi phạm chính sách bảo mật dữ liệu của tổ chức, cảnh báo cho quản trị viên, lưu trữ bằng chứng vi phạm để điều tra và quy trách nhiệm.
- **Khả năng giám sát liên tục, phát hiện các rủi ro, đe dọa và xử lý (Varonis – Data Security Posture Management):** Giám sát liên tục các hành vi truy cập dữ liệu của người dùng, các thay đổi trong thiết lập về phân quyền, các log truy cập mức vành đai (web proxy, dns, vpn, …)… phân tích tổng hợp liên tục và phát hiện các đe dọa liên quan đến dữ liệu, từ đó đưa ra biện pháp xử lý (tự động/thủ công).

3. Chi tiết tính năng giải pháp bảo mật dữ liệu tổng thể

Bộ giải pháp bảo mật dữ liệu tổng thể, với các module tương ứng giúp tổ chức bảo mật dữ liệu toàn diện, khép kín và tối ưu hóa.

Figure 2: Data Protection Modules

3.1. 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, từ đó giúp tổ chức nhanh chóng kiểm kê và nhận diện được trạng thái dữ liệu đã và đang lưu trữ ra sao:

- Cấu trúc lưu trữ trên hệ thống data reppo thế nào
- Các loại file, kiểu file, dung lượng file và meta data của các file đã và đang lưu trữ.
- Loại dữ liệu của nội dung các file (PII, PCI, …), các loại dữ liệu trên từng file.
- Quyền đang thiết lập đối với các folder/file đang lưu trữ

- Drilldown chi tiết thông tin về file dữ liệu theo nhiều chiều khác nhau (dữ liệu, quyền, nội dung, …)

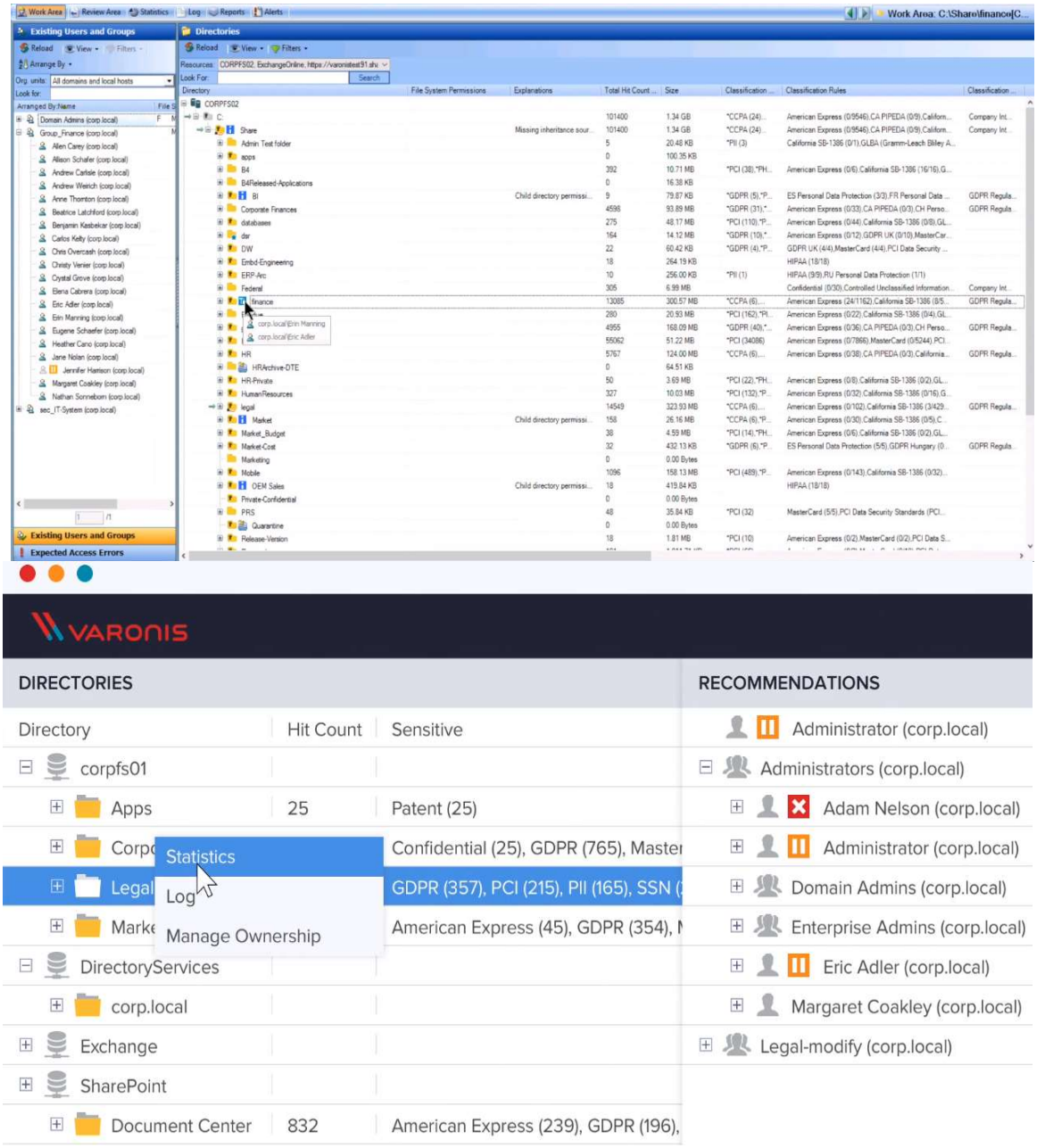


Figure 3: Data Discovery - Data, Content & Permission

Thông qua việc kiểm kê chi tiết đối với dữ liệu, tổ chức cũng có thể nhanh chóng xác định được các rủi ro tiềm ẩn đã và đang tồn tại đối với các dữ liệu quan trọng như: Các file/folder

chứa dữ liệu quan trọng nhưng lại đang được thiết lập quyền ở chế độ public (cho toàn bộ người dùng tổ chức có thể truy cập), các file quan trọng nhưng lại đang được chia sẻ với người dùng bên ngoài, … từ đó chủ động trong việc xử lý sớm các rủi ro đối với dữ liệu tiềm ẩn nguy cơ lộ lọt này.

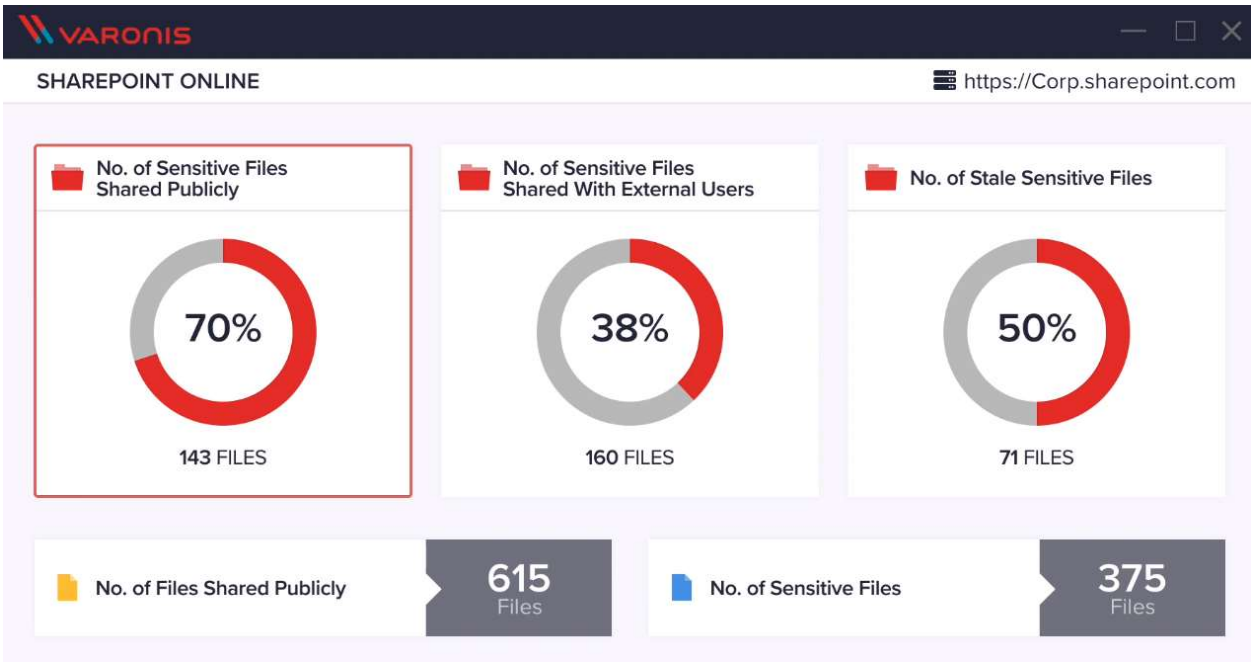


Figure 4: Data Discovery - Risk Identification & Assessment

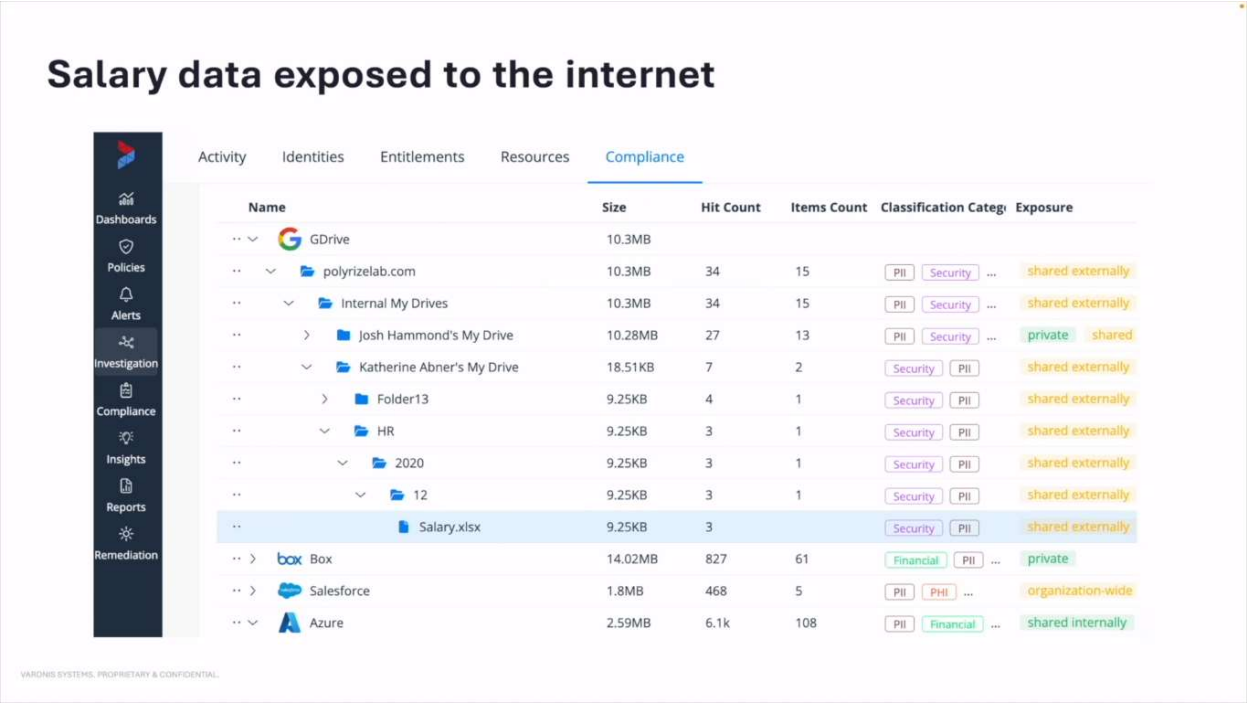


Figure 5: Data Discovery - Risk Identification & Assessment

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.
- Bên cạnh các bộ pattern nhận diện dữ liệu liên quan, engine cũng bao gồm sẵn khả năng nhận diện các thông tin secrets/tài khoản của hệ thống bao gồm không giới hạn: 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.

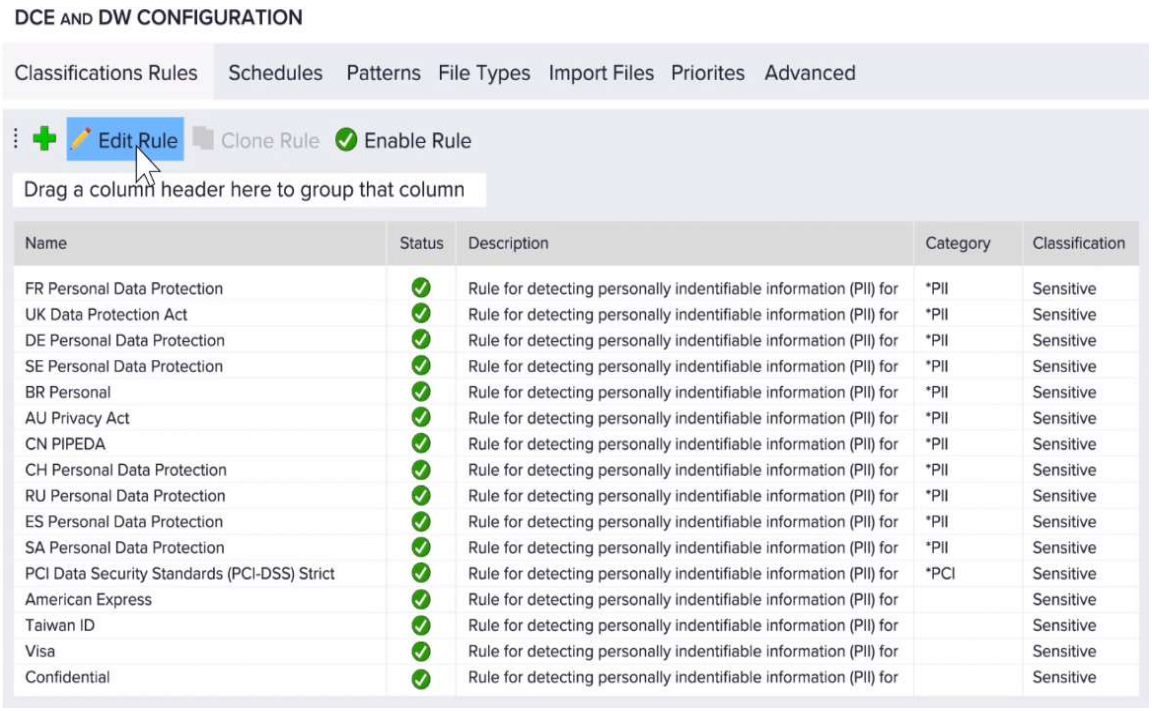


Figure 6: Data Discovery - Rules

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.

3.2. Phân loại và gán nhãn dữ liệu hệ thống

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

Với dữ liệu đã và đang được phân bố tùy biến trên: Hệ thống lưu trữ tập trung (Data Repo như File server, sharepoint, database) và trên hệ thống máy trạm của người dùng. Giải pháp phân loại dữ liệu cho phép thực thi phân loại và gán nhãn cho 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 sau khi được phân loại, gán nhãn xong thì nhãn sẽ được bổ sung vào header/footer/ watermark / metadata của tài liệu.

- **Phân loại và gán nhãn cho dữ liệu trên data repo:**

Giải pháp cho phép lập lịch để tự động hóa tác vụ rà quét dữ liệu trên các 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. Sau khi thực hiện phân loại xong, nhãn dữ liệu sẽ được bổ sung vào tài liệu giúp người dùng cũng như các giải pháp bảo mật nhận diện dữ liệu một cách dễ dàng.

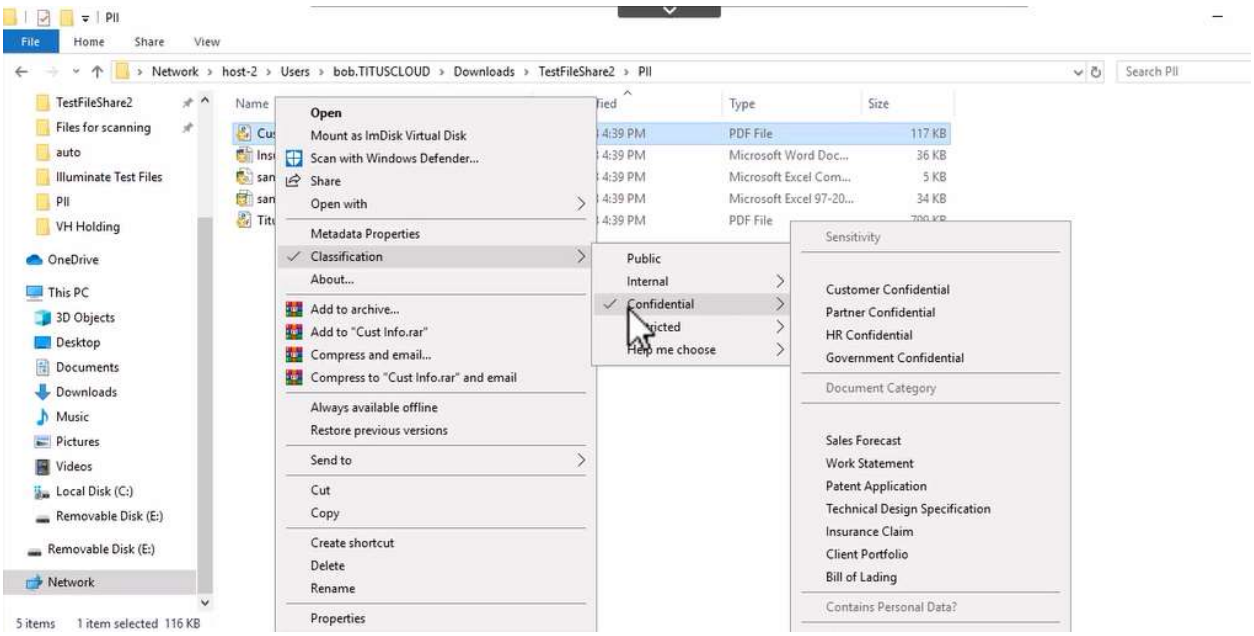


Figure 7: Data Classification & Labeling - Data in Repo

- **Phân loại và gán nhãn cho dữ liệu trên máy trạm người dùng:**

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.

Ví dụ dưới đây là kết hợp phân loại dữ liệu theo phòng ban và mức độ quan trọng của dữ liệu

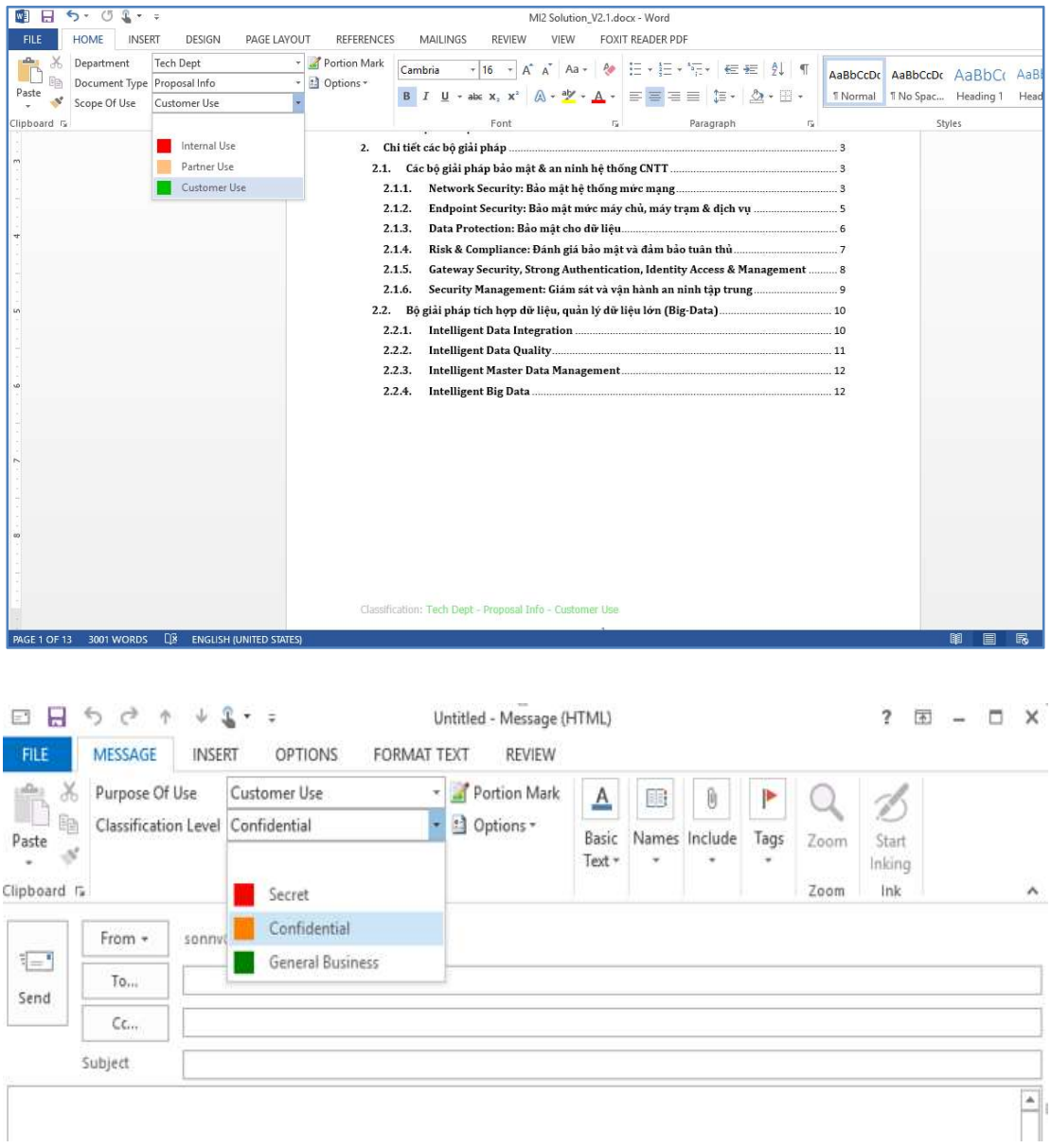


Figure 8: Data Classification - Creating & Using data

Khi tài liệu/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 (save) dữ liệu. Tính năng đảm bảo rằng mọi dữ liệu của Khách hàng mà người dùng tạo ra 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 một người dùng của Khách hàng thay đổi nhãn phân loại dữ liệu (đổi từ mức độ cao xuống thấp, từ thấp sang cao, đổi phòng ban,…), đồng thời lưu lại thông tin về người dùng đã thay đổi nhãn phân loại dữ liệu phục vụ quá trình điều tra, quy trách nhiệm khi cần thiết (trong trường hợp người dùng vô tình, cố tình phân loại dữ liệu sai mức)

3.3. Mã hóa dữ liệu

Sau khi đã nhận diện các dữ liệu quan trọng, thực thi phân loại và gán nhãn, tổ chức có thể thực thi việc mã hóa dữ liệu, kiểm soát quyền truy cập, đảm bảo chỉ những người liên quan mới có thể truy cập vào dữ liệu theo các mức độ quan trọng khác nhau, đảm bảo tính an toàn, bí mật cho dữ liệu quan trọng.

Bộ giải pháp đề xuất bao gồm sẵn tính năng mã hóa đối với các trường hợp (usecase) bảo vệ dữ liệu khác nhau bao gồm:

- Mã hóa toàn bộ ổ cứng (Full Disk Encryption): Áp dụng kết hợp chuẩn mã hóa nâng cao và pre-boot authentication để mã hóa toàn bộ ổ cứng của máy tính, phòng chống việc truy cập bất hợp pháp và đảm bảo an toàn cho dữ dữ liệu trong các trường hợp ổ cứng bị đánh cắp, laptop bị đánh cắp, hoặc các hành vi cố tình của người dùng (rút ổ cứng mang về).
- Mã hóa Folder/File Share / File Server: Tự động hóa việc mã hóa dữ liệu trên các folder / file server và phân phối khóa tập trung, đảm bảo tính tuân thủ trong truy cập vào dữ liệu quan trọng trên hệ thống lưu trữ.
- Mã hóa USB: Mã hóa USB, đảm bảo an toàn cho dữ liệu được lưu trữ và chia sẻ thông qua kênh USB.

Mã hóa toàn bộ ổ cứng

- ***Mã hóa toàn bộ ổ cứng dữ liệu***

Giải pháp sử dụng thuật toán mã hóa mạnh chuẩn quốc tế AES-256 để mã hóa toàn bộ ổ cứng dữ liệu, đảm bảo dữ liệu được lưu trữ trên ổ cứng luôn luôn được bảo mật kể cả trong các trường hợp Máy tính/Laptop hay ổ cứng bị mất, bị đánh cắp. Giải pháp cho phép

người dùng tùy chọn các ổ cứng/phân vùng sẽ được mã hóa tùy vào mục đích bảo vệ dữ liệu của mình.

- ***Kiểm soát truy cập dữ liệu mạnh mẽ***

Giải pháp 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 với nền tảng bảo mật của hệ điều hành cung cấp khả năng bảo mật nhiều lớp (Multi-factor authentication). Để đơn giản và tiện lợi cho người dùng, người dùng có thể thiết lập chế độ đăng nhập một lần – Single Sign One khi tích hợp với tài khoản Active Directory (LDAP) trong khi vẫn đảm bảo tính an toàn và bí mật.

- ***Mã hóa/giải mã trong suốt với người dùng***

Dữ liệu trên ổ cứng chỉ được giải mã (ở dạng rõ) khi người dùng xác thực thành công với hệ thống mã hóa máy tính/Laptop. Quá trình mã hóa và giải mã diễn ra nhanh chóng, không ảnh hưởng tới performance cũng như hoạt động, thao tác sử dụng của người dùng. Người dùng sử dụng máy tính/laptop như với máy tính/laptop bình thường.

- ***Tăng tốc mã hóa và hệ thống 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***

Giải pháp sử dụng các thuật toán mã hóa mạnh, các engine mã hóa mạnh để mã hóa dữ liệu, ngăn chặn các hành vi truy cập và khám phá bất hợp pháp tới các thông tin quan trọng được mã hóa. Các Engine-thuật toán mã hóa được sử dụng bao gồm: AES 256 Bits FIPS 140 -2

- ***Duy trì tính bí mật toàn diện (Persistent Encryption)***

Giải pháp có tính năng mã hóa dữ liệu và đảm bảo dữ liệu luôn được mã hóa bất kể tài liệu, dữ liệu đó được copy,move, hay được truyền/gửi tới bất kỳ vị trí nào thông qua bất kỳ phương thức/giao thức nào.

- ***Thiết lập chính sách mã hóa tự động***

Giải pháp 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:

- Mã hóa tự động dựa trên ứng dụng: Người quản trị có thể định nghĩa các dữ liệu được tạo ra bởi một ứng dụng nào đó sẽ được mã hóa tự động ngay sau khi dữ liệu được tạo ra. Ví dụ các file được tạo ra bởi ứng dụng Microsoft Word, Microsoft Powerpoint, Microsoft Excel … hoặc bất kỳ ứng dụng nào được định nghĩa.

- Mã hóa tự động dựa trên vị trí: Người quản trị có thể định nghĩa chính sách mã hóa dữ liệu dựa trên vị trí lưu trữ của dữ liệu. Theo đó, tất cả dữ liệu đang được lưu trữ hoặc được copy/move tới vị trí lưu trữ này sẽ được mã hóa một cách tự động.

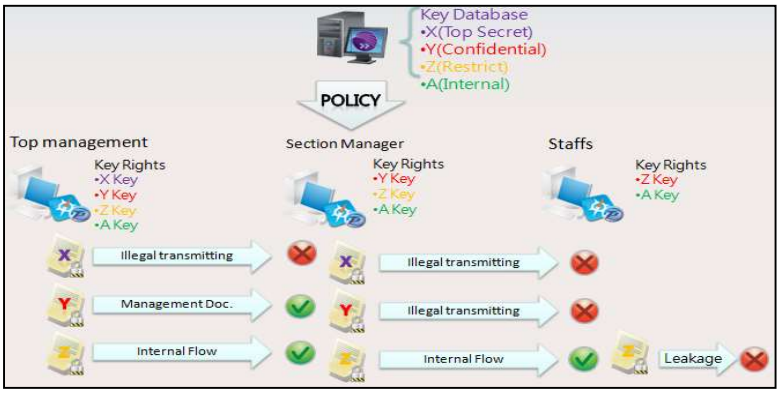
- ***Hỗ trợ chính sách dựa trên người dùng hệ thống Active Directory***

Giải pháp hỗ trợ xây dựng chính sách dựa trên tài khoản người dùng của hệ thống Active Directory. Chính vì vậy giải pháp đảm bảo tính mềm dẻo khi triển khai, các người dùng, nhóm người dùng có vai trò khác nhau sẽ có Khóa và chính sách mã hóa riêng biệt. Sau 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 hỗ trợ cơ chế chia sẻ khóa, 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.

- Mỗi người dùng sẽ có một khóa riêng để mã hóa dữ liệu của mình, đồng thời có thêm khóa chi sẻ của nhóm để mã hóa các tài liệu, dữ liệu mà nhóm. Chính vì vậy, các thành viên của nhóm luôn truy xuất được dữ liệu của nhóm mình, trong khi dữ liệu đó vẫn đảm bảo được tính bí mật đối với các thành viên không thuộc nhóm.



3.4. Phòng chống thất thoát dữ liệu

Các module phòng chống chất thoát dữ liệu giúp tổ chức thực thi việc giám sát, phát hiện và ngăn chặn các hành vi mà người dùng vô tình/ cố tình truyền gửi dữ liệu quan trọng ra bên ngoài vi phạm chính sách bảo mật của tổ chức. Các module phòng chống thất thoát dữ liệu được triển khai toàn diện từ mức máy trạm, đến mức mạng / gateway và Cloud.

3.4.1. DLP Monitor - Giám sát, cảnh báo và capture thông tin truyền gửi

- **Định danh các hành vi truyền gửi vi phạm chính sách**

Giải pháp DLP với thành phần DLP Monitor được triển khai tích hợp với cổng Span port của thiết bị Core Switch. DLP Monitor sẽ capture toàn bộ các luồng dữ liệu đi qua thiết bị Core Switch (Có thể cấu hình để DLP Monitor capture các luồng truyền gửi theo chính sách dựa trên thông tin nguồn, đích, giao thức, …) và lưu trữ vào hệ thống lưu trữ của thiết bị.

DLP Monitor đồng thời phân tích theo thời gian thực tất cả các luồng dữ liệu truyền gửi qua thiết bị Core Switch, Phát hiện các luồng dữ liệu truyền gửi có chứa các thông tin quan trọng – đã được định danh/đánh dấu là quan trọng của tổ chức.

Với những luồng dữ liệu truyền gửi vi phạm chính sách đặt ra, DLP Monitor lưu lại bằng chứng và báo cáo chi tiết:

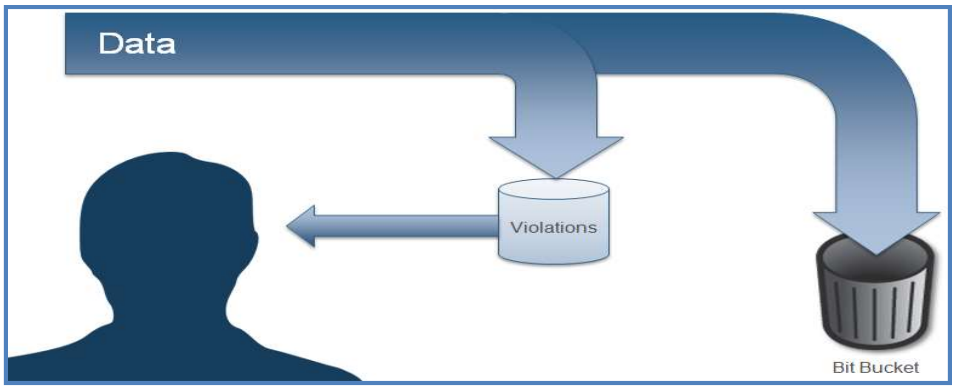
- Dữ liệu gì (Nội dung)
- Được ai gửi đi (Sender)
- Gửi đi đâu
- Gửi bằng phương thức/giao thức gì
- Thời gian truyền gửi
- …

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

Khả năng capture và lưu trữ các phiên truyền gửi dữ liệu là điểm mạnh của Trellix DLP và được coi là tầm nhìn mới để triển khai giải pháp DLP hiệu quả:

- Các giải pháp DLP monitor của các vendor khác hoạt động dựa trên cơ chế: Xây dựng Rule trên DLP monitor và giám sát, nếu traffic truyền gửi

vi phạm chính sách đặt ra thì thực hiện các Action cảnh báo cho người quản trị, lưu evidence. Tuy nhiên không thể biết được mức độ hiệu quả của chính sách đặt ra. Cũng như các trường hợp hệ thống DLP Monitor "lọt" do định nghĩa Rule chưa chính xác, việc tinh chỉnh chính sách DLP sẽ đòi hỏi phải mất một thời gian dài áp dụng vào hệ thống để biết kết quả/mức độ hiệu quả của chính sách DLP.



- Trellix DLP Monitor tiếp cận bằng cách Capture - lưu lại toàn bộ các luồng traffic truyền gửi và cung cấp khả năng:

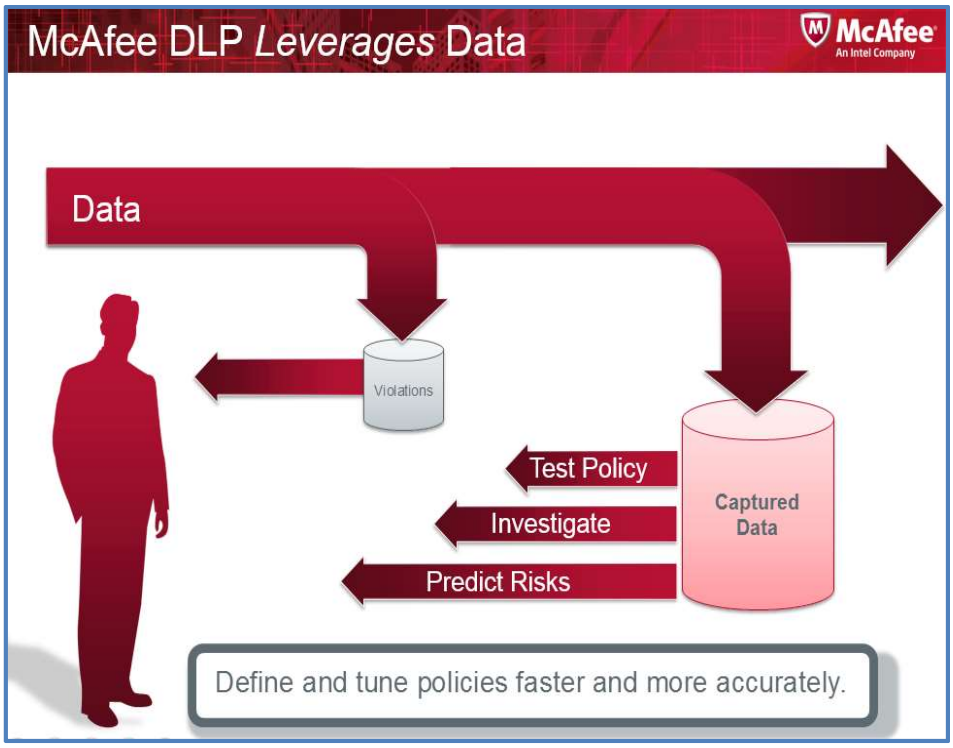


Figure 9: Trellix DLP - Data Capture for Tuning & Investigation

- Dễ dàng Tạo ra Policy mới và Test luôn Policy mới này trên luồng dữ liệu đã được Capture. Nên quản trị viên có thể biết được luôn mức độ hiệu quả của chính sách được tạo ra. Từ đó dễ dàng tinh chỉnh một chính sách DLP phù hợp trong thời gian ngắn thay vì các vendor khác muốn thử policy mới phải áp đặt policy một thời gian dài để monitor trong khi không biết được mức độ hiệu quả của chính sách đặt ra.
- Với luồng dữ liệu được captured này, quản trị viên có thể điều tra mọi hành vi truyền gửi của người dùng trong quá khứ, kể cả các hành vi truyền gửi mà hiện tại, chính sách áp dụng chưa triệt để, chưa toàn diện.

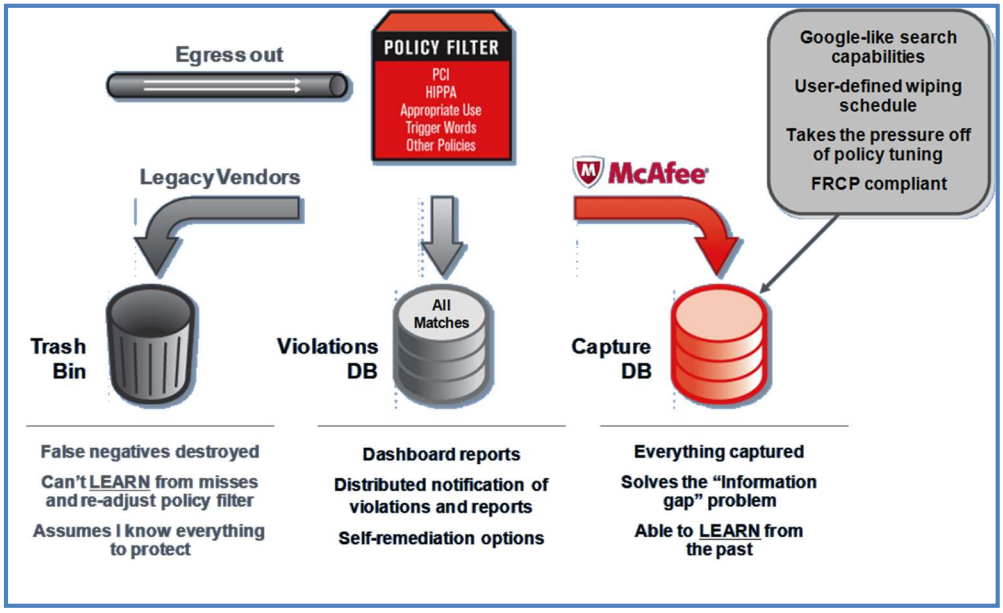


Figure 10: Data Capture - Tuning & Investigation

Việc sử dụng công nghệ Capture vào hệ thống DLP được Gartner đánh giá là phát minh về công nghệ giúp tổ chức xây dựng chính sách DLP hiệu quả/phù hợp trong thời gian ngắn nhất, điều tra hành vi trong quá khứ với đầy đủ bằng chứng.

"The capture database, which allows for previously captured data to be used for analysis and testing new rules, is an innovative and distinctive feature that has been well-received by clients and continues to be reported as a leading feature for clients adopting the McAfee/Trellix content-aware DLP solution" – **Gartner Report**

3.4.2. DLP Prevent - Chống thất thoát dữ liệu qua kênh Web/Mail

DLP Prevent có nhiệm vụ ngăn chặn người dùng truyền, gửi trái phép dữ liệu nhạy cảm, quan trọng của tổ chức ra ngoài thông qua hai kênh phổ biến là Web và Email. Do đó, thiết bị này sẽ tác nghiệp cùng hai thiết bị Web Gateway và E-mail Gateway sẵn có trong hệ thống của tổ chức.

- **DLP Prevent tích hợp với Email Gateway giám sát và bảo vệ dữ liệu trên luồng Mail**

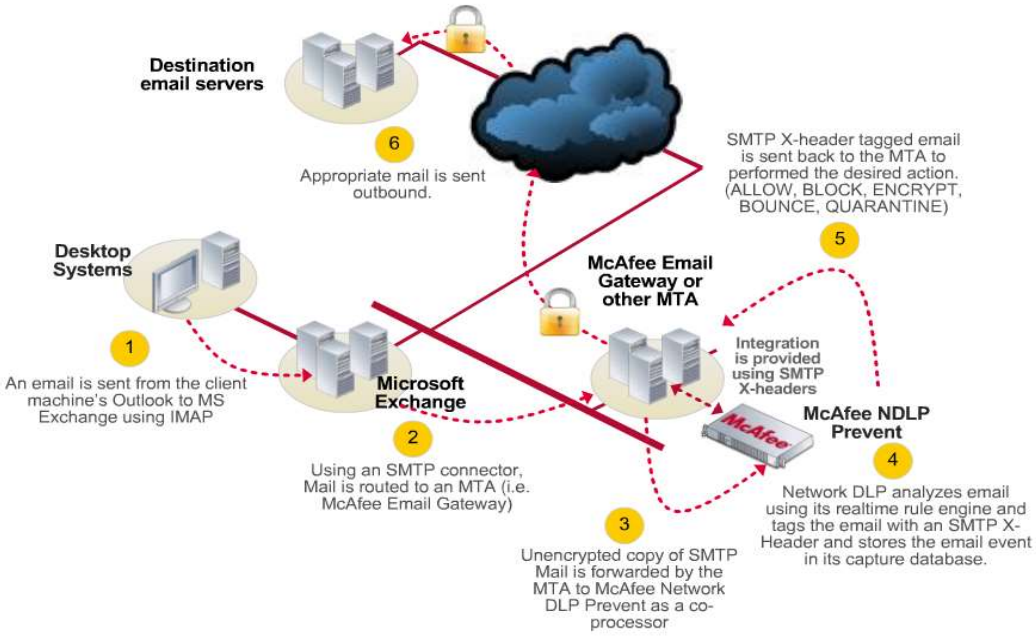


Figure 11: DLP Prevent - DLP for Mail

- Người dùng gửi Mail, Mail sẽ gửi tới máy chủ Mail Server của hệ thống.
- Máy chủ Mail Server sẽ gửi Mail tới hệ thống Email Gateway
- Hệ thống Email Gateway được cấu hình gửi Mail tới DLP Prevent.
- DLP Prevent thực hiện kiểm tra mail, phân tích, phát hiện các mail truyền gửi thông tin nhạy cảm và xác định actions tương ứng (cho phép, ngăn chặn, mã hóa, cách ly,…). Sau đó, gắn thẻ tag (chứ action tương ứng) vào SMTP X-header rồi gửi trả lại cho Email Gateway
- Hê thống Email Gateway sẽ đọc X-header của Mail rồi thực hiện theo Action (cho phép, ngăn chặn, mã hóa, cách ly,…)

- **DLP Prevent tích hợp với Web Proxy giám sát và bảo vệ dữ liệu trên luồng Web.**

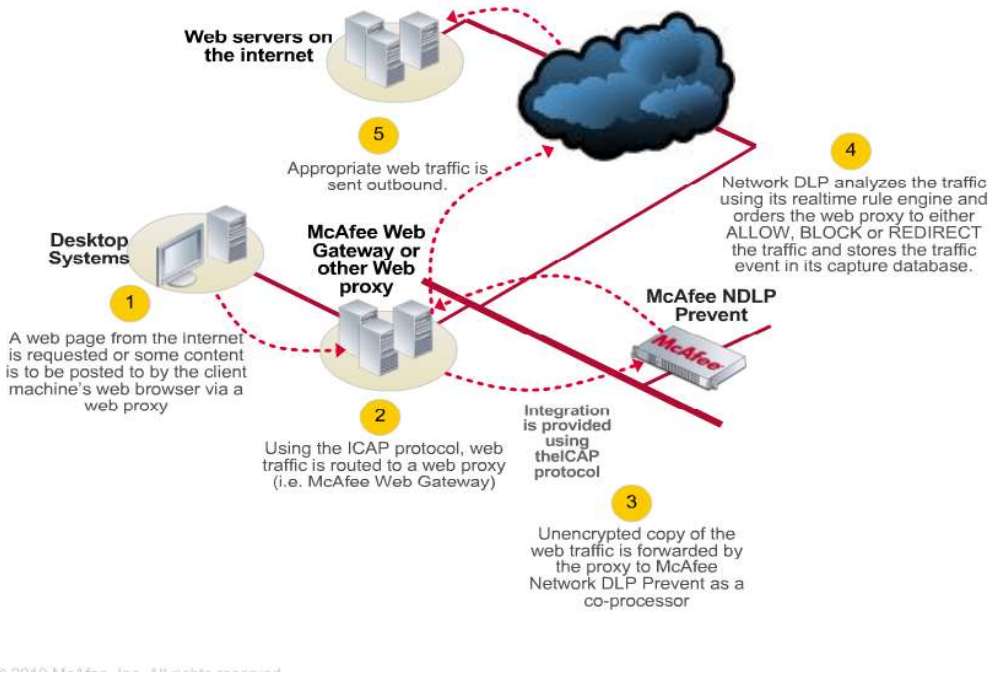


Figure 12: DLP Prevent - DLP for Web

  - Người dùng tiến hành request truy cập internet và upload dữ liệu
  - Request này sẽ được định tuyến tới thiết bị Web Proxy.
  - Thiết bị Web Proxy sẽ gửi request tới thiết bị DLP Prevent theo giao thức ICAP (Bluecoat/Websense/…) hoạt động là ICAP Client, DLP Prevent hoạt động là ICAP Server – Chế độ ICAP hoạt động là Request Mode).
  - DLP Prevent sẽ thực hiện kiểm tra request, phân tích và phát hiện các request có chứa thông tin nhạy cảm, đồng thời đưa ra các action tương ứng (Ngăn chặn, cho phép,…) vào trường X-Header của request. Sau đó DLP Prevent chuyển lại request về cho Web Proxy.
  - Thiết bị Web Proxy nhận lại Request từ DLP Prevent, kiểm tra và thực hiện hành động (action) trong trường X-Header.
- **Khả năng capture, tối ưu chính sách và điều tra an ninh**

Tương tự trên thành phần NDLP Monitor, các thành phần NDLP Prevent có khả năng capture và lưu trữ toàn bộ luồng traffic (bao gồm cả traffic vi phạm và không vi phạm) và cho phép:

- Xây dựng chính sách mới, kiểm tra chính sách mới với các luồng traffic cũ, giúp tối ưu hóa chính sách DLP (Tunning DLP Policy) một cách nhanh chóng.
- Điều tra các hành vi truyền gửi gây thất thoát dữ liệu trong quá khứ trong khi chính sách chưa được áp dụng trước đó.

3.4.3. DLP Endpoint - Chống thất thoát dữ liệu tại máy trạm

- **Dò quét định danh tài nguyên quan trọng trên máy trạm.**

Thành phần DLP Endpoint được cài đặt trên các máy trạm của người dùng. DLP Endpoint thực thi dò quét dữ liệu trên các máy trạm theo lịch thiết lập sẵn trên DLP Manager (việc thực thi dò quét có thể diễn ra khi máy trạm đang online hoặc offline khỏi hệ thống). Ngay sau khi dữ liệu được dò quét và định danh (theo các tiêu chí đặt ra), dữ liệu sẽ được thành phần DLP Endpoint thực thi bảo vệ ngay lập tức.

Thành phần DLP Endpoint của các vendor khác khi tiến hành dò quét dữ liệu trên máy trạm, chỉ khi nào thông tin dò quét được đẩy lên thành phần quản trị tập trung, và áp xuống các thành phần bảo vệ DLP Endpoint, DLP Prevent thì dữ liệu này mới được bảo vệ. Đây là điểm khác biệt của Trellix DLP Endpoint so với các vendor khác.

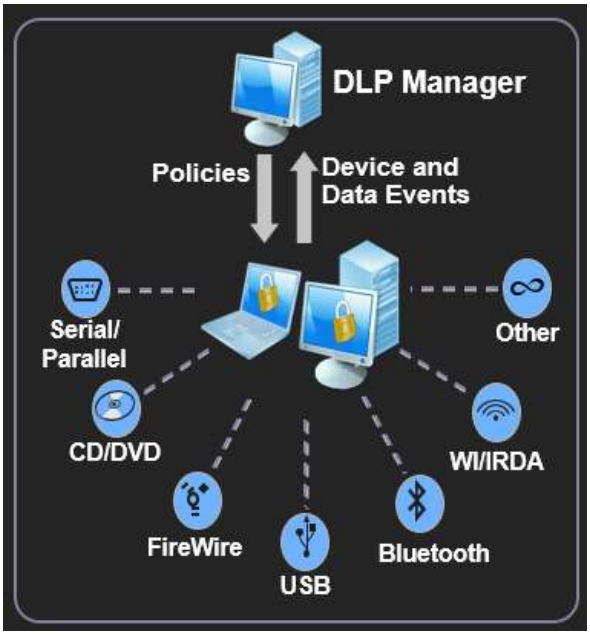
- **Chống thất thoát dữ liệu toàn diện cho máy trạm**

Thành phần DLP Endpoint của Trellix là DLP Endpoint duy nhất cung cấp khả năng bảo vệ bền bỉ và toàn diện trên các kênh truyền gửi của máy trạm bao gồm:

- **Bảo vệ trên tất cả các kênh truyền gửi:**
  - Ngăn chặn người dùng vô tình, cố tình upload, truyền gửi dữ liệu nhạy cảm lên Web/Internet sử dụng HTTP, HTTPs
  - Ngăn chặn người dùng vô tình, cố tình truyền gửi dữ liệu nhạy cảm ra bên ngoài tổ chức sử dụng Email (Outlook, Lotus Note…)

- Ngăn chặn người dùng vô tình, cố tình sử dụng các ứng dụng ngang hang (P2P), các ứng dụng IM (Yahoo, Skype…) truyền gửi dữ liệu nhạy cảm
- Ngăn chặn người dùng truyền gửi dữ liệu nhạy cảm bất hợp pháp ra bên ngoài tổ chức bất kể người dùng sử dụng giao thức nào (dựa trên TCP/UDP), dễ dàng định nghĩa chính sách cho từng dải mạng, giao thức , port, chiều (incoming, outgoing),…
- Ngăn chặn người dùng in ấn, truyền gửi ra USB, Copy/Paste và chụp màn hình dữ liệu (Capture Screen với phím PrintScreen hoặc sử dụng phần mềm của hãng thứ 3) bất hợp pháp.
- Giám sát người dùng truy cập vào các tài liệu, dữ liệu nhạy cảm của tổ chức.

- **Bảo vệ dữ liệu trong các trường hợp cố tình lẩn tránh của người dùng:**
  - Dữ liệu được DLP Endpoint định danh là quan trọng và cần bảo vệ. DLP Endpoint sẽ ngăn chặn các hành vi truyền gửi ra bên ngoài của người dùng kể cả trong các trường hợp: copy sang 1 file khác, thay đổi tên file, thay đổi định dạng (format/extension), nén (compress), và mã hóa (encrypt) với cơ chế tracking của riêng Trellix.
  - Bảo vệ và chống thất thoát dữ liệu trong cả trường hợp người dùng khởi động máy trạm với chế độ Safemode.
  - Chính sách (chi tiết đến từng Rule) có thể áp dụng khi máy trạm online, offline hoặc đồng thời online/offline khởi hệ thống.
- **Cung cấp sẵn tính năng kiểm soát người dùng sử dụng các thiết bị ngoại vi**
  - DLP Endpoint cung cấp sẵn khả năng kiểm soát tất cả các thiết bị ngoại vi khi kết nối đến máy trạm: Ai được phép sử dụng thiết bị ngoại vi nào trên máy trạm. Việc kiểm soát các thiết bị ngoại vi sẽ giảm thiểu số lượng kênh truyền gửi gây thất thoát dữ liệu, giúp phòng chống thất thoát dữ liệu hiệu quả hơn.



- Một số case cụ thể:
  - Chỉ một số người dùng nào đó được sử dụng các thiết bị USB do chính tổ chức phát/cho phép.
  - Kiểm soát việc sử dụng thiết bị wireless, Bluetooth, kết nối điện thoại smartphone (chỉ cho sạc điện, không cho truyền gửi dữ liệu).
  - Mọi hành vi sử dụng thiết bị ngoại vi đều được monitor và lưu thông tin bằng chứng.

3.4.4. 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 hạ tầng Cloud của khách hàng (Gsuite, O365, Box, Dropbox, …) giúp giám sát, phát hiện và ngăn chặn các hành vi truyền gửi / chia sẻ dữ liệu từ môi trường cloud ra bên ngoài qua kênh Email.

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

McAfee/Trellix Skyhigh thực hiện giám sát, phát hiện và thực thi xử lý đối với các trường hợp người dùng vô tình/ cố tình tạo ra, upload các dữ liệu quan trọng

của tổ chức lên môi trường lưu trữ cloud (One Drive, Google Drive, ...) vì phạm chính sách của tổ chức.

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

McAfee/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 (Google Drive, One Drive, ...):

  - Phát hiện và loại bỏ (revoke) các quyền truy cập vào link tài liệu (được chia sẻ/ forward ra bên ngoài theo link).
  - Phát hiện và ngăn chặn chia sẻ dữ liệu với tài khoản email cá nhân.
  - Loại bỏ các quyền truy cập của người dùng bên ngoài đối với các dữ liệu quan trọng đang được lưu trữ trên Cloud storage.

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

Giám sát liên tục mọi hành vi của người dùng tương tác trên hạ tầng Cloud, sử dụng công nghệ machine learning để định danh, phát hiện các trường hợp: Insider Threats (Người dùng xấu thực hiện các hành vi bất thường), compromised account (các tài khoản bị thỏa hiệp, đánh cắp), và các hành vi bất thường của người dùng đặc quyền trên hạ tầng cloud.

3.5. Giám sát, phân tích, phát hiện và xử lý đe dọa

Sau khi đã áp dụng các biện pháp về kiểm soát truy cập, kiểm soát việc người dùng truyền gửi và chia sẻ dữ liệu ra bên ngoài theo chính sách mã hóa và chống thất thoát dữ liệu, giải pháp tiếp tục thực hiện việc giám sát, phân tích chuyên sâu các hành vi tương tác, sử dụng đối với dữ liệu bên trong hệ thống, áp dụng machine learning để định danh các hành vi bất thường/ đe dọa (threat) và xử lý (response) liên quan đến dữ liệu. Với tính năng phân tích, phát hiện và xử lý đe dọa liên quan đến dữ liệu, giải pháp thiết kế để hỗ trợ:

- Phát hiện và định danh các bất thường liên quan đến truy cập vào dữ liệu.
- Phát hiện và định danh các đe dọa bên trong hệ thống (insider threat) và ransomware.

- Phát hiện và định danh cá trường hợp data exfiltration.
- Thực thi để tự động hóa xử lý/ sửa chữa khi phát hiện các đe dọa an ninh đối với dữ liệu.

- **Tự động và liên tục định danh các 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)

Figure 13: Continuous Inventory & Risk Assessment

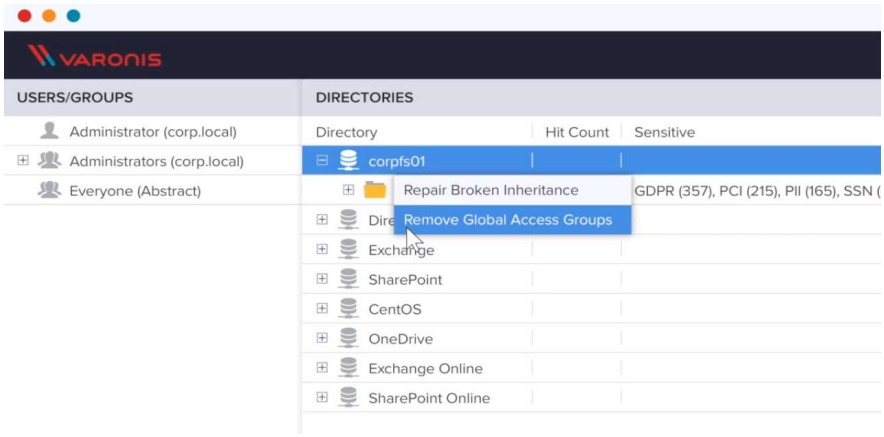


Figure 14: Risk Mitigation - Manual & Automation

- **Tự động giám sát và phân tích hành vi người dùng (UEBA), phát hiện bất thường (đe dọa) và thực thi xử lý.**

Giải pháp tự động thu thập thông tin từ nhiều nguồn khác nhau bao gồm không giới hạn:

- Tất cả hành vi truy cập dữ liệu của người dùng trên hệ thống lưu trữ dữ liệu (Access/Open, download, delete, modify, …) cho phép tổ chức có thể investigate khi cần thiết.

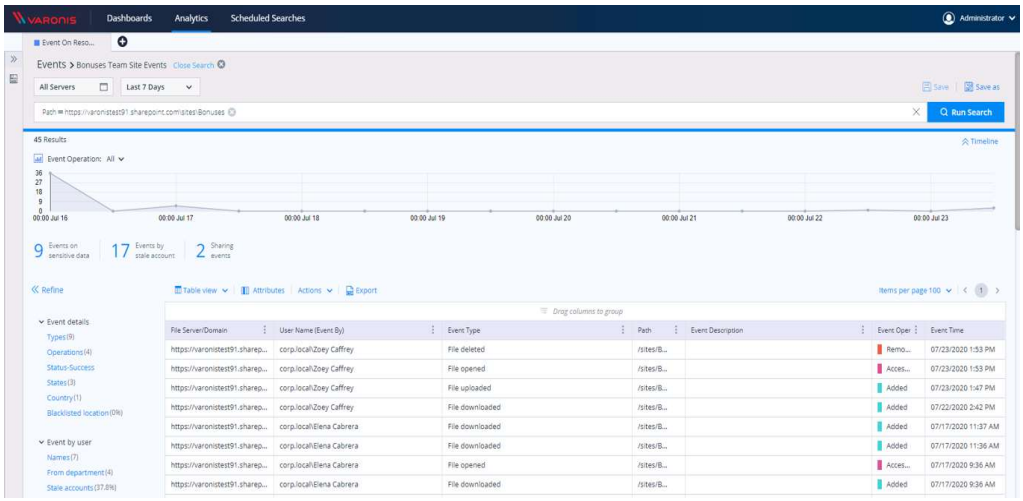


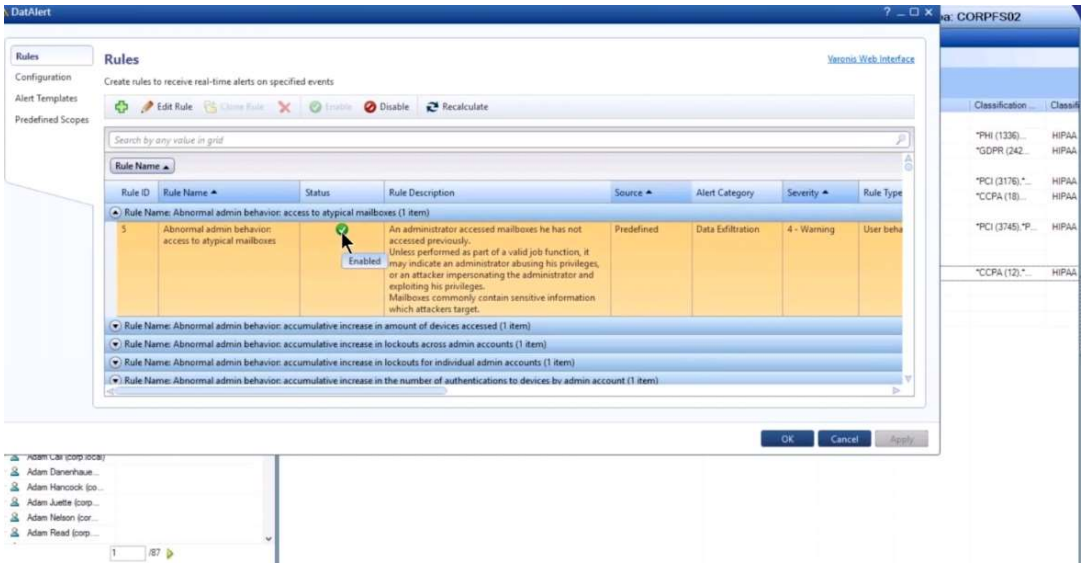
Figure 15: User Activity & Investigation

- Thông tin về định danh người dùng từ hệ thống định danh người dùng (AD, AzureAD), giúp mapping các sự kiện tương tác dữ liệu với người

dùng và vai trò trong tổ chức, cũng như paring với các thiết bị mà người dùng sử dụng, tương tác dữ liệu.

- Sử dụng threat intelligence để cập nhật liên tục những chiến thuật, kỹ thuật, thủ tục mới của tấn công APT, mapping vào tương quan để định danh các đe dọa mới tới dữ liệu tổ chức

Giải pháp thực thi phân tích hành vi (UEBA) 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. Với các trường hợp bất thường định danh, giải pháp cung cấp thông tin chi tiết về điều tra để tổ chức có thể dễ dàng review.



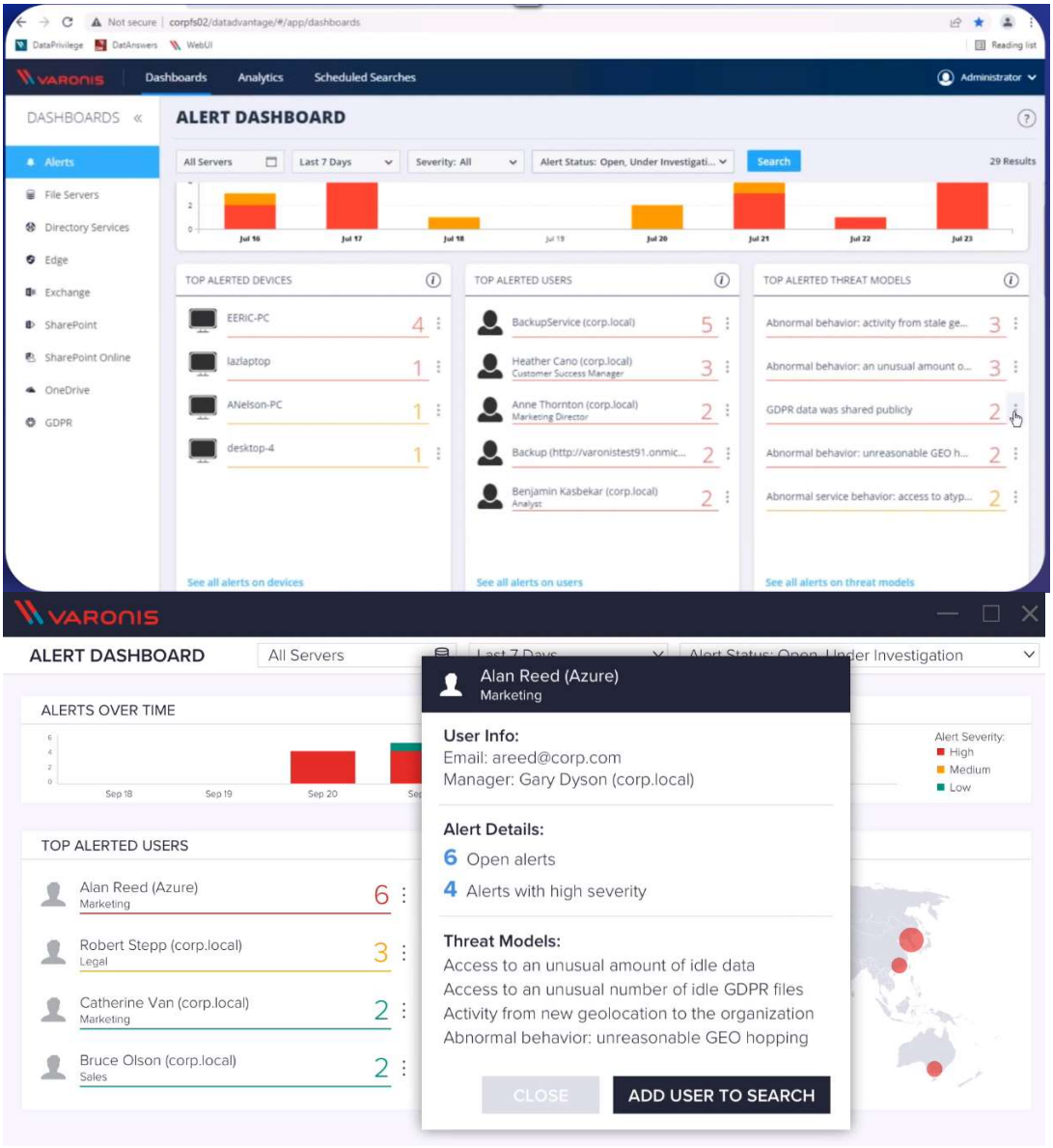


Figure 16: Threat Detection for Data

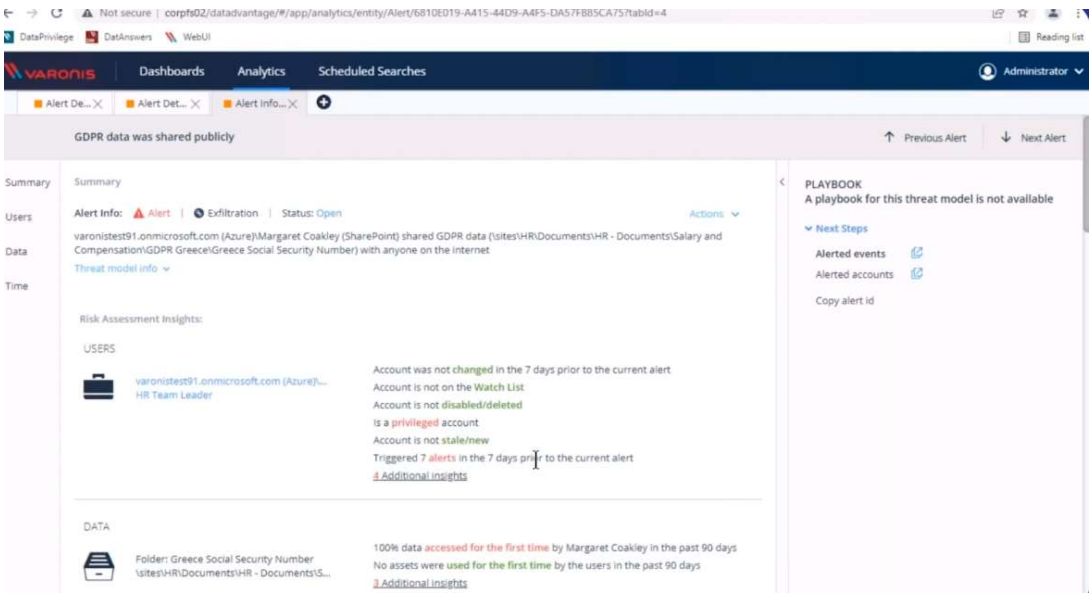


Figure 17: Threat Detection with detail information

- **Thực thi xử lý với playbook tối ưu từ chính hãng**

Với các sự cố / đe dọa đã được định danh, bên cạnh thông tin phân tích chi tiết, giải pháp cung cấp các suggestion dạng best practice để xử lý các de dọa an ninh này, đồng thời cung cấp khả năng thiết lập tự động hóa các hành động xử lý giúp tổ chức có thể chủ động và xử lý đe dọa một cách tự động hóa. Công cụ cũng cho phép tổ chức đảm bảo an toàn khi thực thi các hành vi xử lý tự động hóa bao gồm:

- Khả năng thiết lập request & approval để apply các hành vi xử lý tự động hóa.
- Cho phép review và đánh giá mức độ ảnh hưởng trước khi apply các hành vi xử lý tự động hóa.

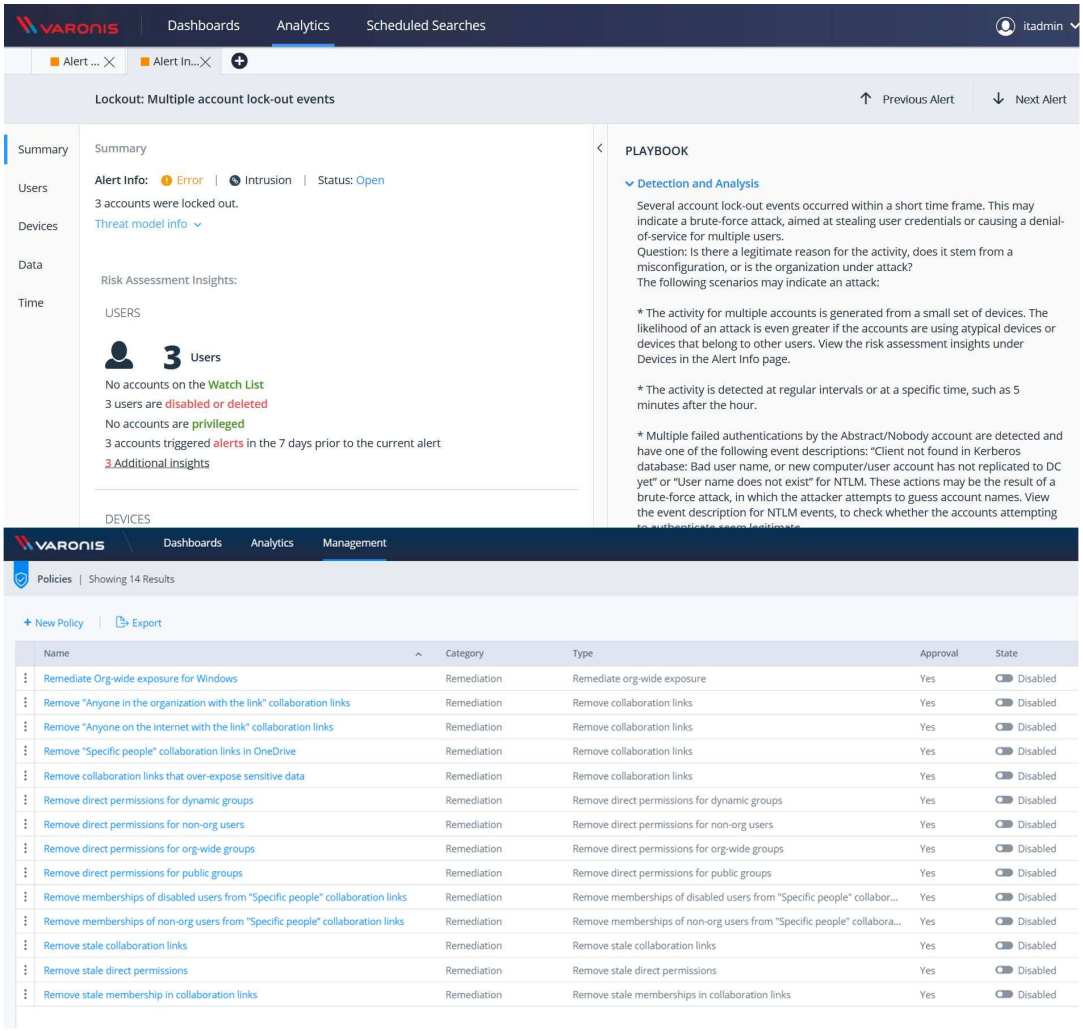


Figure 18: Incident Response with Playbook

3.6. Quản trị và vận hành tập trung

Hệ thống bảo mật dữ liệu toàn diện được quản trị, vận hành đơn giản và tối ưu thông qua 02 console quản trị:

- 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 cũng 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.