**ĐỀ XUẤT GIẢI PHÁP**

**CHỐNG THẤT THOÁT DỮ LIỆU**

**SAFETICA**

Hà Nội, 2025

1. **Vai trò của giải pháp chống thất thoát dữ liệu**
2. **Tổng quan**

**Tất cả những công ty đều có dữ liệu nhạy cảm.** Các dữ liệu mật có thể bao gồm dữ liệu về khách hàng, báo cáo, kế hoạch, bản vẽ… Hiện nay, các vụ rò rỉ dữ liệu đem lại những hậu quả nghiêm trọng cho các doanh nghiệp. Các dữ liệu nhạy cảm được công ty lưu trữ như thông tin cá nhân khách hàng, thông tin mật liên quan đến tài sản, tài chính,… khi bị lộ ra ngoài, rơi vào tay kẻ xấu có thể gây ảnh hưởng nghiêm trọng đến uy tín, thiệt hại tài chính lớn và khiến tổ chức chịu các khoản phạttheo luật định tùy vào mức độ quan trọng của thông tin rò rỉ. Trước tình trạng đó,giải pháp chống thất thoát dữ liệu (DLP) là nhu cầu thiết yếu, giúp doanh nghiệp bảo mật dữ liệu, phòng ngừa tối đa việc thông tin mật bị lộ hay đánh cắp.

1. **Hiện trạng thất thoát dữ liệu**

Những lỗ hổng trong dữ liệu càng trở nên đắt đỏ và phức tạp hơn. Trong năm 2023, trung bình một cuộc thất thoát dữ liệu trên thế giới tốn khoảng 4.4 triệu USD, tăng 15% so với năm 2020.

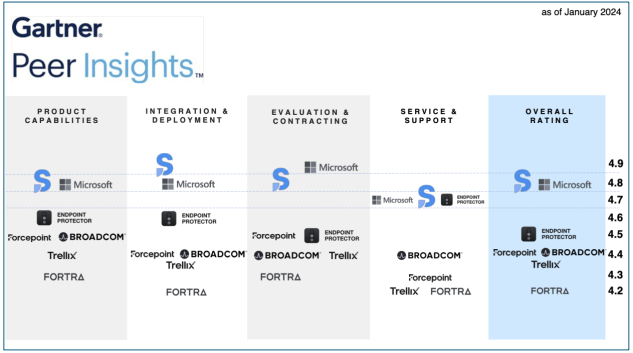
Tình trạng mua bán dữ liệu cá nhân ở Việt Nam rất nghiêm trọng; trong đó, có hai yếu tố là tội phạm đột nhập, đánh cắp dữ liệu cá nhân rất lớn. Theo thông tin của Viettel Threat Intelligence, năm 2023 đã ghi nhận 12 triệu tài khoản bị đánh cắp, với 40 vụ lộ lọt dữ liệu lớn và trên 100 triệu bản ghi dữ liệu bị rao bán. Theo Báo cáo của Bộ Công an trước Quốc hội ngày 21/11, số lượng tội phạm và vi phạm pháp luật trên không gian mạng tiếp tục tăng cao, trong đó vấn đề mua bán, lấy cắp thông tin, dữ liệu cá nhân là một vấn đề cực kì gây nhức nhối. Số vụ được phát hiện, xử lý là hơn 1.600 vụ và 478 đối tượng, với tỷ lệ tăng lần lượt là 203,61% và 48,91% so với năm 2022.

Ở Việt Nam, Nghị định 13 của Chính phủ về bảo vệ dữ liệu cá nhân với 4 chương, 44 điều vừa có hiệu lực từ 1/7/2023. Đây là bước tiến lớn đầu tiên trong nỗ lực xây dựng hành lang pháp lý nhằm bảo vệ dữ liệu cá nhân tại Việt Nam. Nhiều nội dung tương đồng với các quy định đã có từ lâu của Singapore hay của Liên minh châu Âu. Việc tuân thủ những quy định này góp phần rất lớn vào việc bảo vệ các dữ liệu nhạy cảm của các tổ chức.

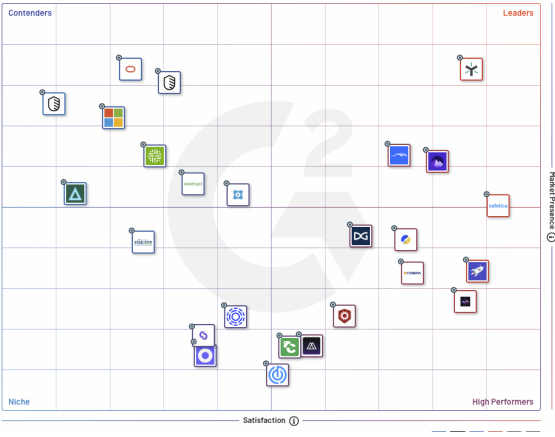
1. **Giải pháp chống thất thoát dữ liệu Safetica**
2. **Giới thiệu Safetica**

Safetica là công ty phần mềm của Séc được thành lập vào năm 2011. Công ty cung cấp các giải pháp Chống thất thoát dữ liệu (Data Loss Prevention - DLP) và Bảo vệ mối đe dọa nội bộ (Insider Risk Management - IRM) cho các doanh nghiệp từ nhỏ đến lớn trên thị trường hiện nay.

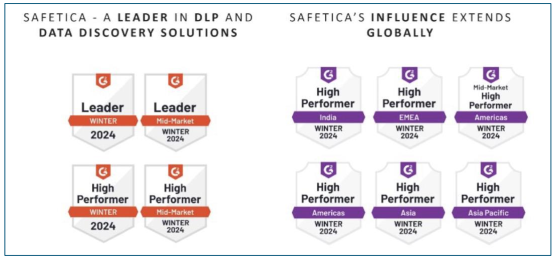
Trong suốt quãng thời gian ra mắt giải pháp Chống thất thoát dữ liệu, Safetica luôn được các trang đánh giá uy tín đánh giá như Gartner và G2 rất cao. Trong vòng 10 năm qua, Safetica đã nhận được sự công nhận từ cả các công ty nghiên cứu và khách hàng.

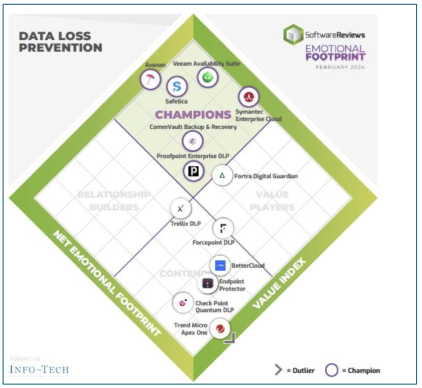


*Bảnh đánh giá của Gartner Peer Insights*

**

*Bảng đánh giá G2 Grid về Phát hiện dữ liệu nhạy cảm*

*  
Safetica luôn nhận được những huy hiệu Leader và High Perfomer từ G2*

  
*Safetica được đánh giá CHAMPIONS trên trang đánh giá SoftwareReviews của InfoTech 4/2024*

1. **Giải pháp Chống thất thoát dữ liệu của Safetica**

Safetica kết hợp giải pháp DLP và Quản lí rủi ro nội bộ (Insider Risk Management), điều này giúp khách hàng có thể xác định, phân loại và bảo vệ các dữ liệu nhạy cảm (DLP) cũng như phát hiện, phân tích và giảm thiểu rủi ro (Quản lí rủi ro nội bộ). Safetica lấy những ưu điểm của DLP và của IRM, kết hợp chúng tạo ra một sản phẩm Safetica ONE duy nhất có được tất cả những ưu điểm của các giải pháp trên.

- Không chỉ bảo vệ dữ liệu, Safetica còn tập trung vào AI sử dụng những dữ  
liệu này và sử dụng như thế nào.

- Safetica không chỉ tạo những quy tắc và chính sách mà còn đảm bảo những  
chính sách này giúp người dùng nâng cao nhận thức về an toàn thông tin.

- Safetica không chỉ phân tích luồng hoạt động của dữ liệu mà còn phân tích  
cách người dùng sử dụng chúng và hành vi của người dùng.

- DLP chủ yếu về cách phản hồi các sự cố, tuy nhiên, Safetica cũng tập trung  
vào cách phòng chống những sự cố có thể xảy ra.

Giải pháp Chống thất thoát dữ liệu của Safetica hiện tại hỗ trợ 2 phương án triển  
khai (On-premise và Cloud).

1. **Điều khiến Safetica nổi bật**

Trong số nhiều các giải pháp chống thất thoát dữ liệu, Safetica luôn được rất nhiều người dùng đánh giá tốt và ủng hộ. Các điều khác biệt và nổi bật của giải pháp Chống thất thoát dữ liệu của Safetica có thể kể đến:

- Safetica có thể triển khai nhanh chóng.

- Safetica tốn ít tài nguyên của hệ thống, tuy nhiên vẫn giữ được hiệu năng cao.

- Safetica chỉ yêu cầu lượng ít tài nguyên cho vận hành hệ thống và bảo trì.  
Safetica chỉ cần vài giờ mỗi tuần để bảo trì, trong khi các giải pháp DLP doanh  
nghiệp khác yêu cầu nhân viên IT chuyên dụng làm việc toàn thời gian.  
- Safetica không chỉ phát hiện dữ liệu nhạy cảm mà còn xác định nó một cách  
chính xác hơn bằng cách kết hợp kiểm tra nội dung với nhận thức về ngữ cảnh  
trong hệ thống phân loại thống nhất. Điều này có nghĩa là Safetica có thể nhận  
biết và bảo vệ dữ liệu không chỉ dựa trên nội dung mà còn dựa trên nguồn  
gốc, loại tệp và các yếu tố khác. Safetica nhận thấy rằng nhiều dữ liệu nhạy  
cảm ngày nay không có từ hoặc mẫu nhận dạng rõ ràng, một số là hình vẽ  
hoặc mã. Do đó, với hệ thống phân loại thống nhất của Safetica, giải pháp  
giúp giảm thiểu các kết quả dương tính giả bằng cách xem xét cả nội dung và  
ngữ cảnh.

- Safetica thể hiện cực kì ấn tượng trong việc nhận biết các rủi ro từ bên trong  
bằng cách hiểu ý định của người dùng. Theo Gartner, dữ liệu không tự mất  
mà là do cách người dùng sử dụng chúng. Phân tích hành vi người dùng giúp  
giảm thiểu rủi ro mà họ tạo ra.

- Safetica cũng tạo điều kiện thuận lợi cho các quản trị viên IT và đội ngũ an  
ninh thực thi chính sách và điều tra các sự cố. Mục tiêu của Safetica là làm  
cho việc bảo vệ dễ dàng và thân thiện với người dùng. Đó là lý do tại sao  
Safetica đã đơn giản hóa quy trình triển khai và làm cho việc thiết lập nhanh  
chóng và dễ dàng. Trọng tâm của Safetica là tăng cường khả năng phát hiện  
các rủi ro và đồng thời làm cho việc thực thi chính sách DLP dễ dàng hơn cho  
đội ngũ an ninh.

1. **Tính năng giải pháp**
   1. **Kiểm toán an toàn thông tin**

Với module UEBA (User and Entity Behavior Analytics) được tích hợp vào sản  
phẩm, tổ chức sẽ được cung cấp thông tin chi tiết về các tệp tin người dùng thao tác trên máy. Safetica tự động phân loại tệp chứa thông tin nhạy cảm với các tệp khác, hỗ trợ quản trị viên trong việc phòng ngừa lộ dữ liệu quan trọng.  
Bên cạnh đó, các website, ứng dụng do người dùng truy cập cũng được thống kê cùng với lượng thời gian họ sử dụng. Đặc biệt, chúng được phân loại thành các nhóm theo nội dung (Mã độc, Bị cấm, Game,…), giúp dễ dàng phát hiện người dùng truy cập ứng dụng, website độc hại. Ngoài ra, Safetica còn hỗ trợ theo dõi email được gửi đi và nhận tại email của người dùng, cũng như hiện tất cả các tệp đính kèm, tiêu đề, domain của người gửi và người dùng. Thêm nữa, phần mềm cũng liệt kê danh sách các thiết bị ngoài như USB, máy in, điện thoại,.., kết nối đến và lưu lượng mạng của máy.

* 1. **Phân loại dữ liệu**

Safetica nhận dạng dữ liệu và phân loại chúng dựa trên 4 yếu tố:  
- Nội dung nhạy cảm: Các tệp tin được lọc theo nội dung nhạy cảm được định  
nghĩa. Tổ chức có thể lựa chọn hoặc tự định thông tin nhạy cảm theo từ điển, thuật toán có sẵn của Safetica, từ khóa hoặc regex.

- Thuộc tính tệp: Phần mở rộng (.cad, .pdf,…); nhóm tệp (Hình ảnh, Bản thuyết trình,…); định dạng (TXT, XML, HTML,…).

- Metadata: Các tệp tin được tìm kiếm theo metadata của ứng dụng người dùng sử dụng để tạo tệp, ví dụ Microsoft Word, Microsoft Excel, Microsoft Powerpoint,…  
- Quy tắc ngữ cảnh: Các tệp tin được nhóm theo ứng dụng, website nguồn và đường dẫn chứa chúng.

* 1. **Bảo vệ dữ liệu thiết bị đầu cuối**

Safetica sử dụng chính sách DLP để bảo vệ dữ liệu trên các thiết bị đầu cuối và kiểm soát hành vi ứng dụng. Mỗi chính sách DLP bao gồm:

- Loại chính sách: Chính sách chung (quản lý các kênh truyền thông tin); chính  
sách dữ liệu (quản lý nhóm dữ liệu); chính sách ứng dụng (quản lý hành vi  
ứng dụng).

- Mode: vô hiệu hóa, ghi log, ghi log và thông báo, ghi log và chặn. Các mode  
này quyết định ảnh hưởng của quy định chính sách lên các thao tác với tệp  
của người dùng, từ đó bảo vệ và ngăn chặn các vụ lộ, mất dữ liệu. Ví dụ, ghi  
log và chặn sẽ cấm tất cả thao tác bị hạn chế và ghi log nếu người dùng thử  
thực hiện.

- Quy định chính sách: Safetica xây dựng nhiều quy định kiểm soát các hành  
động thao tác hàng ngày với tệp tin của người dùng trên mục lưu trữ từ Cloud  
drive đến thiết bị ngoài. Ví dụ, quy định Email sẽ quản lý việc gửi email từ  
email của người dùng.

* 1. **Cảnh báo và báo cáo vi phạm chính sách DLP**

Các cảnh báo giúp quản trị viên nhanh chóng phát hiện các hành vi bất thường của người dùng, vi phạm chính sách DLP, bao gồm:

- Vi phạm chính sách DLP: Cảnh báo mỗi lần người dùng vi phạm chính sách  
DLP.  
- Dữ liệu nhạy cảm không được bảo vệ di chuyển khỏi thiết bị đầu cuối: Cảnh  
báo số lần dữ liệu nhạy cảm không được bảo vệ bởi chính sách DLP và rời  
khỏi thiết bị cuối.

- Dữ liệu nhạy cảm không được bảo vệ di chuyển đến một điểm: Cảnh báo số  
lần dữ liệu nhạy cảm không được bảo vệ bởi chính sách DLP chuyển đến một  
điểm (địa chỉ email, web domain, cloud service,…).

- Ngoài ra, tổ chức có thể lựa chọn các mẫu báo cáo sự cố DLP có sẵn trên  
Safetica.

* 1. **Quản lý truy cập ứng dụng và website**

WebSafetica cho phép quản trị viên ngăn chặn người dùng truy cập vào các website hoặc ứng dụng độc hại. Tổ chức có thể tạo chính sách để ngăn chặn nhóm ứng dụng, website hoặc một ứng dụng, website cụ thể cho các thiểt bị đầu cuối.

* 1. **Phân vùng thiết bị**

Tính năng này hỗ trợ quản trị viên tạo môi trường an toàn cho việc lưu trữ các dữ liệu quan trọng. Cụ thể, có thể nhóm các thiết bị vào vùng cho phép và vùng không cho phép để lưu trữ, truyền tải hoặc xử lí thông tin. Tổ chức cũng sẽ dùng các vùng này để áp dụng chính sách DLP.

* 1. **Tích hợp SIEM, Office 365 và FortiGate**

Các cảnh báo sự cố và log có thể được gửi tự động đến hệ thống SIEM của doanh nghiệp. REST API cung cấp các dữ liệu được thu thập bởi Safetica cho các công cụ như Power BI hay Tableau cho việc phân tích nâng cao.

Safetica cũng bảo vệ dữ liệu trên Office 365 và SharePoint của các thiết bị đầu cuối, nhằm ngăn chặn chia sẻ và tải thông tin trái phép lên môi trường cloud. Hơn nữa, phần mềm còn có khả năng tích hợp vào thiết bị bảo mật mạng FortiGate, tối ưu việc bảo vệ dữ liệu.

1. **Mô hình triển khai giải pháp**

Hiện tại, Safetica hỗ trợ triển khai on-premises hoặc trên cloud.

1. **Triển khai On-premises**
   1. **Yêu cầu hệ thống**

- 1 Server cài đặt MS SQL Express server, Safetica Management Service và Safetica Management Console.

- Các máy tính người dùng cài đặt Safetica Client

* 1. **Yêu cầu kĩ thuật**

1. Máy sever cho 250 thiết bị

|  |  |
| --- | --- |
| **Hệ điều hành** | Microsoft Windows Server 2012 (64-bit) trở lên |
| **CPU** | Tối thiểu Quad-Core 2.4 GHz |
| **RAM** | Tối thiểu 8 GB |
| **Hard drive** | Tối thiểu 100 GB |
| **Database** | MS SQL 2012 trở lên (bao gồm bản Express) |
| **.NET Framework** | .NET 4.5.2 trở lên |

b) Máy tính người dùng

|  |  |
| --- | --- |
| **CPU** | Tối thiểu Quad-Core 2.4 GHz 32-bit hoặc 64-bit |
| **RAM** | Tối thiểu 2 GB |
| **Hard drive** | Tối thiểu 2 GB |

c) MS SQL Database

|  |  |
| --- | --- |
| **Hệ điều hành** | Microsoft Windows Server 2012 (64-bit) trở lên |
| **Dung lượng OS** | Tối thiểu 200 GB |

1. **Triển khai trên Cloud**
   1. **Yêu cầu hệ thống**

Safetica hỗ trợ triển khai Software as a service (SaaS) của Microsoft Azure. Ngoàira Safetica yêu cầu cài Client trên máy tính của người dùng.

* 1. **Yêu cầu kĩ thuật**

Máy tính người dùng

|  |  |
| --- | --- |
| **CPU** | Tối thiểu Quad-Core 2.4 GHz 32-bit hoặc 64-bit |
| **RAM** | Tối thiểu 2 GB |
| **Hard drive** | Tối thiểu 2 GB |