SEARCHINFORM

Giới thiệu về SearchInform:
Chúng tôi là ai và chúng tôi làm gì

SearchInform là một trong những nhà phát triển giải pháp quản lý rủi ro hàng đầu. Trong hơn một thập kỷ qua, công ty luôn tiên phong về công nghệ, tập trung vào việc xử lý các mối đe dọa nội bộ, bảo vệ doanh nghiệp và các tổ chức chính phủ trước nguy cơ đánh cắp dữ liệu, hành vi gây hại từ con người, vi phạm tuân thủ và những thiếu sót trong công tác kiểm toán.

1995 Thành lập đội ngũ gồm các nhà phát triển chuyên sâu về phần mềm an ninh thông tin.

2017 Giải pháp DLP của SearchInform đã được đưa vào Gartner Magic Quadrant. Đồng thời, công ty đã mở rộng hoạt động sang các thị trường Trung Đông và Bắc Phi.

2018 SearchInform gia nhập thị trường Brazil và Nam Phi.

2019 SearchInform tiếp tục mở rộng hiện diện tại các thị trường Ấn Độ, Indonesia và Malaysia.

2020 SearchInform tổ chức sự kiện Road Show tại Indonesia.

2021 SearchInform tham gia Triển lãm Quốc tế đổi mới sáng tạo Việt Nam 2021.

2023 SearchInform đã tổ chức sự kiện "Giảm thiểu mối đe dọa nội bộ" tại Malaysia.

Các giải pháp của SearchInform đã được đưa vào danh mục điện tử quốc gia của Indonesia.

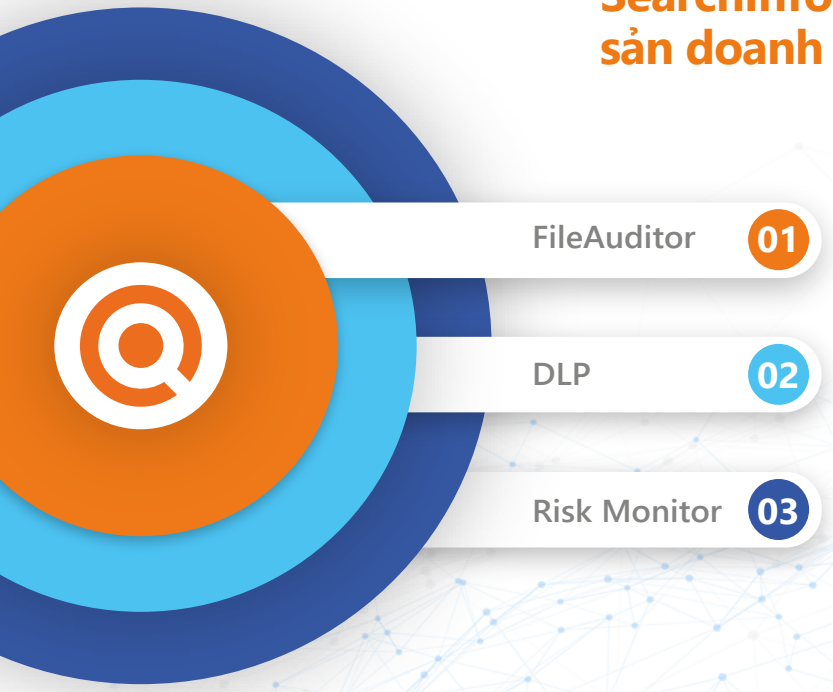
SearchInform đã mở văn phòng đại diện tại Các Tiểu vương quốc Ả Rập Thống nhất, đồng thời tham gia hàng loạt sự kiện tại Thái Lan và Indonesia.

2024 SearchInform gia nhập thị trường Việt Nam và Thổ Nhĩ Kỳ.

2025 SearchInform mở văn phòng đại diện tại Ả Rập Xê Út và Thổ Nhĩ Kỳ.

2026 SearchInform mở văn phòng đại diện tại Việt Nam và Malaysia.

SearchInform đảm bảo cơ chế bảo vệ tài sản doanh nghiệp theo mô hình ba lớp.



FileAuditor 01 — Phát hiện và bảo vệ dữ liệu ở cấp độ hệ thống tệp.

DLP 02 — Bảo vệ ở cấp độ máy trạm, trên các kênh dữ liệu và trước các rủi ro liên quan đến yếu tố con người.

Risk Monitor 03 — Cung cấp khả năng hiển thị toàn diện các quy trình nghiệp vụ, đồng thời hỗ trợ quản lý rủi ro một cách hiệu quả.

Hơn 4.000 khách hàng trên toàn cầu

1995 Công ty được thành lập

Hơn 3.000.000
máy tính được bảo vệ bởi phần mềm của SearchInform

6 sản phẩm mang lại khả năng bảo vệ dữ liệu toàn diện trước các mối đe dọa

The Radicati Group

đưa SearchInform vào báo cáo nghiên cứu Enterprise Data Loss Prevention Market, 2017–2021.

2017

Phần mềm của SearchInform được đưa vào

Gartner Magic Quadrant

2019

SearchInform bắt đầu cung cấp dịch vụ bảo mật.

Services

2020

SearchInform công bố các giải pháp điện toán đám mây.

2010

Trung tâm Đào tạo được thành lập.

16 Khóa đào tạo nâng cao dành cho chuyên gia an ninh thông tin

2 Khóa đào tạo an ninh mạng dành cho người dùng

Next-Gen DLP hoạt động như thế nào?

Giải pháp của SearchInform cung cấp cách tiếp cận ba lớp đối với an ninh thông tin.

PHÂN LOẠI DỮ LIỆU

Giải pháp DLP quét cả môi trường lưu trữ đám mây và lưu trữ vật lý, phân loại tệp bằng các nhãn nội dung, kiểm soát quyền truy cập tệp của người dùng và cung cấp khả năng hiển thị toàn diện đối với dữ liệu doanh nghiệp.

NGĂN NGỪA RÒ RỈ DỮ LIỆU

Giải pháp Next-Gen DLP cung cấp khả năng kiểm soát toàn diện tất cả các kênh truyền tải dữ liệu trong doanh nghiệp, đối chiếu dữ liệu với các chính sách bảo mật và ngăn chặn các vi phạm tiềm ẩn.

GIẢM THIỂU RỦI RO KINH DOANH

Hệ thống DLP của SearchInform đảm bảo khả năng bảo vệ 360° bằng cách kết hợp bảo mật dữ liệu và giảm thiểu các mối đe dọa nội bộ trên một nền tảng duy nhất.

Tuân thủ đầy đủ các yêu cầu quy định

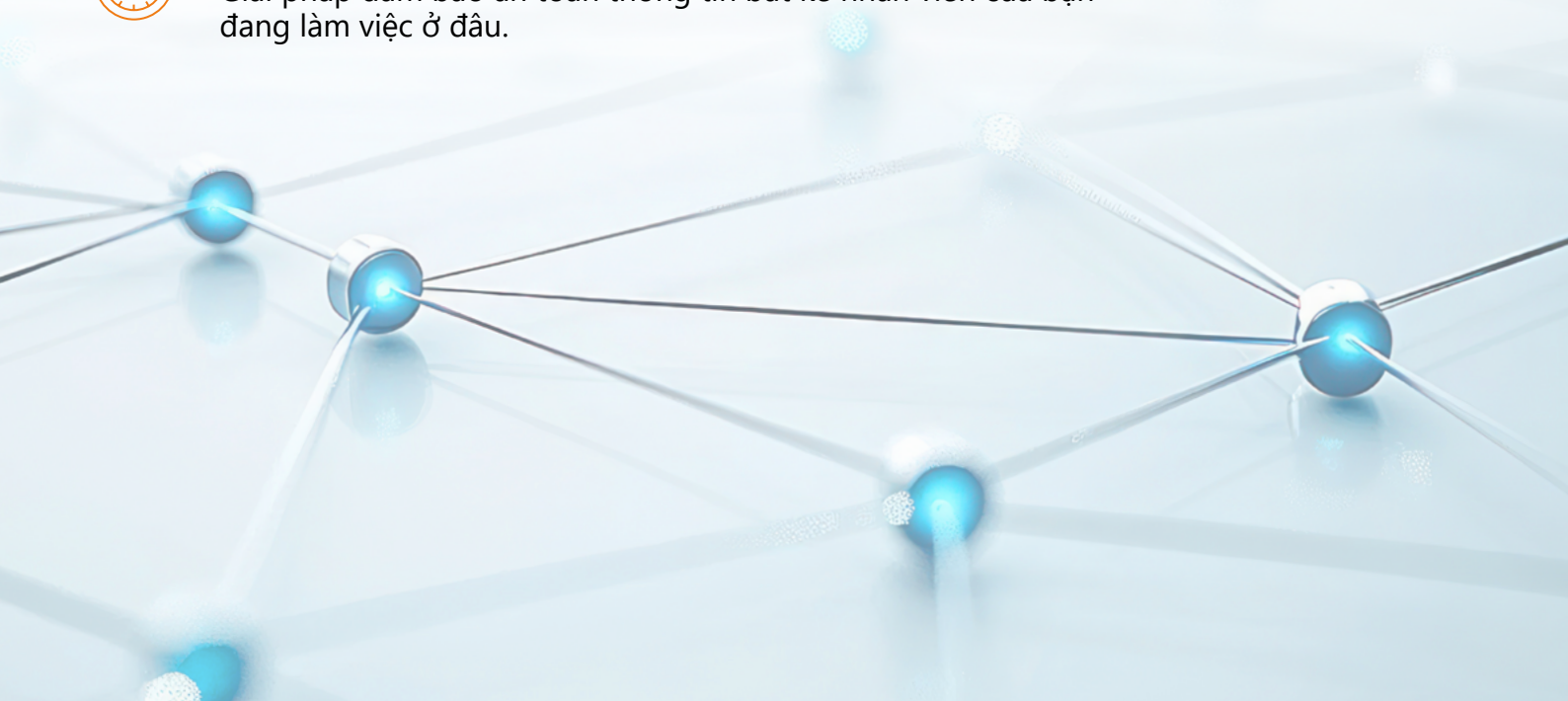
Giải pháp giúp đảm bảo việc tuân thủ được thực hiện một cách nhất quán trên toàn bộ tổ chức.

Bảo vệ dữ liệu toàn diện và ngăn ngừa mối đe dọa

SearchInform DLP xác định và phân tích các lỗ hổng trong quá trình truyền tải dữ liệu, đồng thời tận dụng các phương pháp phân tích nâng cao để tương quan hóa các mối đe dọa.

Bảo vệ dữ liệu doanh nghiệp 24/7

Giải pháp đảm bảo an toàn thông tin bất kể nhân viên của bạn đang làm việc ở đâu.



Chúng tôi cung cấp

- Bảo vệ dữ liệu (phân quyền truy cập, giám sát việc truyền tải và sử dụng dữ liệu, ngăn ngừa thất thoát dữ liệu)
- Giám sát liên tục và phát hiện vi phạm
- Ngăn chặn sự cố
- Điều tra sự cố
- Phân tích năng suất làm việc của nhân viên
- Phát hiện các vi phạm nội bộ (trộm cắp, nhận hoa hồng bất hợp pháp, làm việc ngoài không được phép)
- Kiểm soát chất lượng công việc (đảm bảo tính chính xác trong giao tiếp với khách hàng, các chuỗi quy trình nghiệp vụ)

Danh sách các ngành nghề

- Cơ quan chính phủ
- Sản xuất
- Dịch vụ tài chính
- Quốc phòng & An ninh
- Viễn thông & CNTT
- Năng lượng
- Logistics
- Bán lẻ

Các ngân hàng tại Việt Nam đã ghi nhận một sự cố nội bộ nghiêm trọng. Theo cơ quan thực thi pháp luật, nhân viên của 13 ngân hàng đã đánh cắp và lạm dụng dữ liệu mật của khách hàng. Các đối tượng đã lợi dụng vị trí công tác để thu thập trái phép và buôn bán dữ liệu liên quan đến tài khoản ngân hàng. Thông tin bị lộ bao gồm các dữ liệu cá nhân như số định danh, địa chỉ và số điện thoại. Giá bán dữ liệu dao động từ 300.000 đến 2,2 triệu VND cho mỗi tài khoản. Sự cố này đã gây ra tổn thất nghiêm trọng về uy tín cho các tổ chức liên quan, đồng thời dẫn đến các khiếu nại và hậu quả pháp lý.

Hệ thống DLP có thể làm gì?

Các hệ thống DLP cung cấp chức năng ngăn ngừa rò rỉ dữ liệu. Khi người dùng cố gắng thực hiện hành vi truyền tải dữ liệu trái phép, hệ thống sẽ ngay lập tức chặn thao tác đó.

Ví dụ, một nhân viên ngân hàng có quyền truy cập hợp pháp vào thông tin cá nhân của khách hàng phục vụ cho công việc. Tuy nhiên, nếu nhân viên này cố gắng sao chép dữ liệu sang thiết bị USB, tải lên lưu trữ đám mây hoặc gửi cho người không có quyền truy cập hợp lệ (bên ngoài tổ chức hoặc thậm chí là đồng phạm trong nội bộ ngân hàng), hệ thống DLP sẽ ngăn chặn hành vi truyền dữ liệu này, bất kể kênh truyền tải được sử dụng.

Đồng thời, hệ thống DLP sẽ cảnh báo cho nhân sự phụ trách để đảm bảo mối đe dọa được phát hiện và xử lý kịp thời, giúp ngăn chặn sự cố trước khi xảy ra.

Ngân hàng BCA có trụ sở tại Indonesia đã gặp phải một sự cố rò rỉ dữ liệu. Theo điều tra, một mối đe dọa nội bộ—là cựu nhân viên của ngân hàng—đã bị truy tố vì bán thông tin tài chính của khách hàng trên một diễn đàn DarkNet. Sự việc được phát hiện sau khi một nhân viên của ngân hàng BCA nhận được khiếu nại từ khách hàng. Bộ dữ liệu bị rò rỉ liên quan đến 20.000 người, bao gồm:

- Số tài khoản ngân hàng trực tuyến
- Số điện thoại di động
- Thông tin giao dịch của các tài khoản đó

Hệ thống DLP có thể làm gì?

Các hệ thống DLP đảm bảo tuân thủ thông qua cách tiếp cận lấy dữ liệu làm trung tâm và lấy người dùng làm trung tâm. Nhờ đó, mọi hoạt động của người dùng đối với dữ liệu nhạy cảm đều được giám sát chặt chẽ, đồng thời các vi phạm trong quá trình sử dụng và truyền tải dữ liệu được ngăn chặn hiệu quả.

Hệ thống DLP có khả năng phát hiện các hành vi sao chép dữ liệu, tự động chặn thao tác nếu vi phạm các chính sách bảo mật đã thiết lập, đồng thời cảnh báo cho bộ phận phụ trách. Nhờ vậy, dữ liệu sẽ không thể rời khỏi phạm vi kiểm soát của doanh nghiệp.

Năm 2025, Tòa án Công nghiệp tại Malaysia đã xem xét một vụ việc liên quan đến rủi ro nội bộ trong doanh nghiệp. Một cựu nhân viên của Petroliam Nasional Berhad (Petronas) đã đệ đơn khiếu nại với lý do bị sa thải không công bằng.

Trong quá trình xét xử, Petronas đã đưa ra bằng chứng cho thấy cựu trưởng bộ phận có mối quan hệ không minh bạch với CEO của một nhà thầu, đồng thời làm rò rỉ các tài liệu đấu thầu mật. Các tài liệu này đã được chuyển ra ngoài thông qua thiết bị USB, với lời khai xác nhận từ phía CEO.

Ngoài ra, các bằng chứng bổ sung được tìm thấy trong tài khoản email cá nhân của nhân viên, bao gồm các tin nhắn chứa vé máy bay, hình ảnh séc ngân hàng và thông tin tài khoản ngân hàng của vợ người này được sử dụng cho các giao dịch tài chính.

Hệ thống DLP có thể làm gì?

Các hệ thống DLP kiểm soát chặt chẽ các kênh truyền tải dữ liệu phổ biến như thiết bị USB, từ đó ngăn chặn việc sao chép các tệp tin nhạy cảm từ máy trạm. Bên cạnh đó, SearchInform DLP có thể được cấu hình để tự động mã hóa các tệp được chuyển sang thiết bị USB, đảm bảo rằng chúng chỉ có thể được mở trên các máy tính doanh nghiệp được cấp quyền.

Giải pháp Next-Gen DLP cũng giám sát cả hoạt động email nội bộ và email cá nhân. Khi phát hiện việc chia sẻ thông tin nhạy cảm, hệ thống sẽ ngay lập tức cảnh báo cho đội ngũ an ninh. Những khả năng này còn được tăng cường bởi các chính sách ứng dụng AI, giúp phát hiện các hành vi bất thường và cho phép đội ngũ bảo mật phản ứng nhanh chóng trước các mối đe dọa nội bộ tiềm ẩn.

ĐỐI TÁC CỦA CHÚNG TÔI

MADHAVA
vietsunshine "together we deliver"
VNDS DATA SECURITY
TKMT
VaciF Focusing On Value

KHÁCH HÀNG CỦA CHÚNG TÔI

SOCIALIST REPUBLIC OF VIET NAM
MINISTRY OF PUBLIC SECURITY

BANK BPD DIY
VTC DIGICOM
bapenda jakarta
wipro

LIÊN HỆ

vn.searchinform.com
+84 869019330
vn@searchinform.com
5th floor, East Tower Office, Lumiere Riverside Building, 277 Vo Nguyen Giap street, An Khanh Ward, Ho Chi Minh City

Nếu bạn muốn lên lịch trao đổi, vui lòng liên hệ với các đại diện của chúng tôi tại đây.