BITURN VIETNAM

SOVAR DLP

www.biturnvn.com

SOVAR DLP

Giải pháp SOVAR DLP (Data Loss Prevention) là hệ thống phần mềm giúp ngăn chặn rò rỉ, thất thoát dữ liệu nhạy cảm từ thiết bị đầu cuối của người dùng. SOVAR DLP được triển khai nhằm giám sát, ghi log và kiểm soát mọi hành vi liên quan đến dữ liệu trên máy tính cá nhân và laptop nội bộ. Hệ thống tích hợp với Active Directory, công cụ phân loại dữ liệu và SIEM để đảm bảo quản lý tập trung, cảnh báo và xử lý kịp thời theo chính sách bảo mật đã thiết lập.

GIÁ TRỊ CỐT LÕI

1. Bảo vệ dữ liệu nhạy cảm ở mọi thời điểm
SOVAR DLP giúp kiểm soát dữ liệu trong toàn bộ vòng đời – từ khi tạo ra, sử dụng, chia sẻ đến lưu trữ hoặc di chuyển, đảm bảo dữ liệu luôn được bảo vệ đúng theo mức độ nhạy cảm và chính sách tổ chức.

2. Tăng cường khả năng kiểm soát và tuân thủ
Nhờ vào tính năng giám sát chi tiết và khả năng ghi log đầy đủ, hệ thống hỗ trợ tổ chức đáp ứng các yêu cầu tuân thủ pháp lý, quy định nội bộ và tiêu chuẩn bảo mật quốc tế một cách hiệu quả.

3. Chủ động phát hiện và phản ứng với rủi ro
SOVAR DLP không chỉ phát hiện hành vi bất thường mà còn có khả năng ngăn chặn kịp thời tại thiết bị đầu cuối, giúp tổ chức chủ động giảm thiểu thiệt hại từ các sự cố rò rỉ dữ liệu – dù là vô tình hay cố ý.

TÍNH NĂNG CHÍNH

1. GIÁM SÁT THIẾT BỊ ĐẦU CUỐI (ENDPOINT MONITORING)

- Theo dõi hoạt động người dùng: USB, email, in ấn, chia sẻ mạng, upload cloud, file, ứng dụng và mạng.
- Hoạt động cả khi thiết bị offline.

2. QUẢN TRỊ TẬP TRUNG

- Quản lý chính sách, log và cấu hình qua giao diện Web UI.
- Hỗ trợ phân quyền RBAC, xác thực 2FA hoặc SSO.

3. TÍCH HỢP VỚI HỆ THỐNG KHÁC

- Active Directory (AD): Đồng bộ người dùng, nhóm, đơn vị tổ chức.
- SIEM (QRadar): Gửi log tập trung, hỗ trợ phân tích và cảnh báo.
- Công cụ phân loại dữ liệu (Classification): Gắn nhãn và xác định mức độ nhạy cảm của dữ liệu.
- Email Gateway (tùy chọn): Giám sát luồng email nội bộ.

4. BẢO MẬT VÀ XÁC THỰC

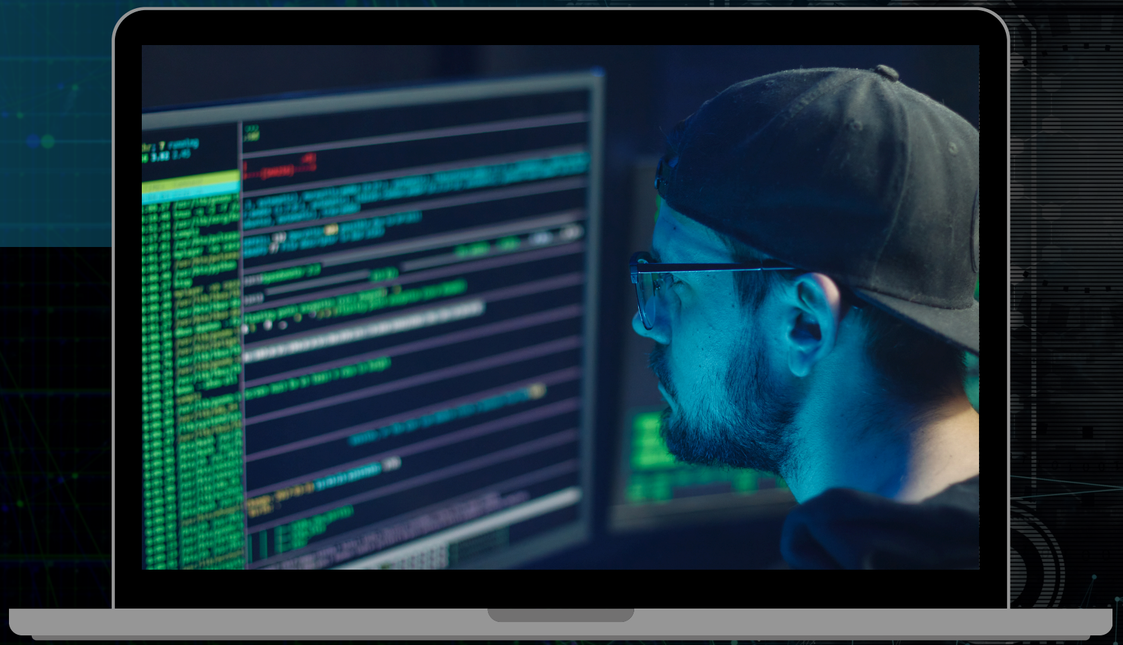
- Sử dụng TLS 1.2+, token hoặc PKI để bảo mật giao tiếp giữa các thành phần.
- Ghi nhật ký mọi hành động quản trị (audit log).

GIÁM SÁT THIẾT BỊ ĐẦU CUỐI

Giám sát thiết bị đầu cuối là chức năng cốt lõi của giải pháp SOVAR DLP, cho phép theo dõi và kiểm soát toàn diện mọi hoạt động liên quan đến dữ liệu trên máy tính cá nhân và laptop của người dùng. Thông qua SOVAR DLP Agent được cài đặt trên mỗi thiết bị, hệ thống có thể giám sát liên tục các hành vi như sao chép dữ liệu ra USB, gửi email, in ấn, chia sẻ qua mạng nội bộ hoặc tải dữ liệu lên các dịch vụ lưu trữ đám mây.

Tính năng này giúp tổ chức phát hiện sớm các hành vi có nguy cơ làm rò rỉ dữ liệu nhạy cảm, từ đó áp dụng chính sách xử lý phù hợp như cảnh báo, ghi log hoặc chặn hành động ngay tại thời điểm xảy ra. Đặc biệt, SOVAR DLP Agent vẫn hoạt động hiệu quả ngay cả khi thiết bị không kết nối mạng, đảm bảo việc giám sát không bị gián đoạn.

QUẢN TRỊ TẬP TRUNG



1. GIAO DIỆN QUẢN TRỊ TRỰC QUAN

Toàn bộ hoạt động cấu hình, giám sát và quản lý chính sách đều được thực hiện thông qua một giao diện Web thân thiện, bảo mật. Quản trị viên có thể truy cập từ xa để theo dõi tình trạng hệ thống, thiết lập chính sách mới hoặc xử lý các sự kiện bảo mật kịp thời.

2. PHÂN QUYỀN QUẢN TRỊ LINH HOẠT (RBAC)

Hệ thống hỗ trợ mô hình phân quyền theo vai trò (Role-Based Access Control), cho phép gán quyền hạn phù hợp cho từng nhóm hoặc cá nhân quản trị. Điều này giúp kiểm soát chặt chẽ quyền truy cập và giảm thiểu nguy cơ thao tác sai hoặc bị lạm dụng quyền quản trị.

3. XÁC THỰC BẢO MẬT NÂNG CAO (2FA/SSO)

Hệ thống hỗ trợ xác thực hai yếu tố (Two-Factor Authentication) hoặc tích hợp đăng nhập một lần (Single Sign-On), đảm bảo chỉ người dùng hợp lệ mới có quyền truy cập hệ thống quản trị. Mọi thao tác đều được ghi log (audit log) để phục vụ kiểm tra và truy vết khi cần thiết.

TÍCH HỢP VỚI HỆ THỐNG KHÁC

TÍCH HỢP VỚI ACTIVE DIRECTORY (AD)

SOVAR DLP kết nối với AD thông qua LDAP/LDAPS để đồng bộ danh tính người dùng, nhóm và đơn vị tổ chức (OU). Nhờ đó, hệ thống có thể tự động áp dụng chính sách bảo mật theo cơ cấu tổ chức mà không cần cấu hình thủ công. Đây là nền tảng quan trọng để quản trị chính sách nhất quán và quy mô lớn

TÍCH HỢP VỚI CÔNG CỤ PHÂN LOẠI DỮ LIỆU VÀ EMAIL GATEWAY

SOVAR DLP tích hợp với các công cụ phân loại dữ liệu như Titus, MIP để nhận diện và gắn nhãn mức độ nhạy cảm cho dữ liệu. Ngoài ra, có thể tích hợp với Email Gateway (tùy chọn) để kiểm soát nội dung email ra/vào, đảm bảo không có dữ liệu nhạy cảm bị rò rỉ qua kênh thư điện tử

TÍCH HỢP VỚI HỆ THỐNG SIEM

SOVAR DLP Server gửi log sự kiện bảo mật đến hệ thống SIEM (như IBM QRadar) qua chuẩn Syslog hoặc CEF. SIEM sẽ phân tích, phát hiện hành vi bất thường và đưa ra cảnh báo sớm. Sự tích hợp này giúp tăng cường khả năng phản ứng và xử lý sự cố trong thời gian thực

BẢO MẬT VÀ XÁC THỰC

Để đảm bảo an toàn tuyệt đối cho dữ liệu và ngăn chặn các rủi ro tấn công từ bên ngoài, giải pháp SOVAR DLP được thiết kế với các cơ chế bảo mật nghiêm ngặt cho toàn bộ quá trình truyền thông và xác thực giữa các thành phần trong hệ thống.

Tất cả các kết nối giữa DLP Agent, DLP Server, và các hệ thống tích hợp (AD, SIEM...) đều sử dụng giao thức mã hóa TLS 1.2 trở lên để bảo vệ dữ liệu trong quá trình truyền. Đồng thời, các Agent phải thực hiện xác thực bảo mật với Server bằng token hoặc hạ tầng khóa công khai (PKI) để đảm bảo danh tính và ngăn truy cập trái phép.

Bên cạnh đó, hệ thống quản trị cung cấp cơ chế phân quyền linh hoạt (RBAC), hỗ trợ xác thực hai yếu tố (2FA) hoặc đăng nhập một lần (SSO), cùng với tính năng ghi nhật ký đầy đủ mọi hành động quản trị nhằm phục vụ công tác kiểm tra, truy vết và tuân thủ.

TÍNH NĂNG ƯU VIỆT

1. GIÁM SÁT TOÀN DIỆN – KIỂM SOÁT THEO THỜI GIAN THỰC

SOVAR DLP giám sát liên tục mọi hành vi liên quan đến dữ liệu trên thiết bị đầu cuối, bao gồm USB, email, cloud, in ấn... và có thể cảnh báo hoặc ngăn chặn ngay lập tức khi phát hiện rủi ro, kể cả khi thiết bị offline

2. TÍCH HỢP LINH HOẠT – QUẢN LÝ TẬP TRUNG

Hệ thống dễ dàng tích hợp với AD, SIEM, công cụ phân loại dữ liệu và Email Gateway, giúp đồng bộ quản trị người dùng, nâng cao khả năng phân tích, cảnh báo và áp dụng chính sách từ một điểm điều phối trung tâm

3. BẢO MẬT CAO – HIỆU SUẤT TỐI ƯU

SOVAR DLP sử dụng giao thức mã hóa mạnh (TLS 1.2+), hỗ trợ xác thực 2FA, phân quyền chi tiết (RBAC) và lưu log đầy đủ để truy vết. Đồng thời, giải pháp được tối ưu nhẹ, xử lý log thời gian thực với khả năng mở rộng lên hàng chục nghìn thiết bị mà vẫn đảm bảo hiệu năng

TRIỂN KHAI & HỖ TRỢ

1. Triển khai nhanh chóng, đúng chuẩn
   - Tư vấn giải pháp phù hợp theo nhu cầu thực tế.
   - Lập kế hoạch triển khai chi tiết, rõ ràng từng giai đoạn.
   - Đảm bảo hệ thống hoạt động ổn định ngay từ lần đầu cấu hình.

2. Đào tạo và chuyển giao đầy đủ
   - Hướng dẫn sử dụng cho quản trị viên và người dùng.
   - Tài liệu kỹ thuật, quy trình vận hành và xử lý sự cố được cung cấp đầy đủ.
   - Đào tạo thực hành trên môi trường triển khai thực tế.

3. Hỗ trợ kỹ thuật toàn diện
   - Hỗ trợ 24/7 với đội ngũ chuyên gia giàu kinh nghiệm.
   - Cập nhật phần mềm, vá lỗi và nâng cấp định kỳ.
   - Dịch vụ bảo trì và giám sát hệ thống theo yêu cầu SLA (Service Level Agreement).

GET IN TOUCH WITH US!

www.biturnvn.com