Datasheet

Viettel Endpoint Detection & Response

(VCS - aJiant)

viettel security

"Giải pháp bảo vệ và phòng chống mã độc trong các tổ chức, doanh nghiệp, gỡ bỏ triệt để chương trình độc hại trên toàn bộ hệ thống."

THÁCH THỨC

Ngày nay, các tổ chức, doanh nghiệp gặp rất nhiều khó khăn trong việc phát hiện, xác định, điều tra và giảm thiểu các phần mềm độc hại trong hệ thống. Đối với các doanh nghiệp, tổ chức lớn thường là mục tiêu của các cuộc tấn công chủ đích, có tổ chức, độ phức tạp cao, các giải pháp thông thường không phát hiện được.

Đối với các doanh nghiệp vừa và nhỏ, mối lo chính là các mã độc gây chậm, treo máy, ransomware. Trong khi đó, trong hệ thống các doanh nghiệp này thường không có nhiều trang bị ATTT cần thiết, kinh nghiệm và kỹ năng ATTT của quản trị chưa đáp ứng được nhu cầu.

GIẢI PHÁP

Giải pháp VCS-aJiant cung cấp phiên bản nhỏ gọn Endpoint Protection Platform (EPP) phù hợp với nhu cầu bảo vệ và phòng chống mã độc tại các doanh nghiệp và tổ chức, bao gồm nhóm tính năng liên quan đến phòng chống mã độc (anti-malware) nhằm phản ứng, ngăn chặn, gỡ bỏ chương trình độc hại một cách triệt để trên toàn bộ hệ thống và không ảnh hưởng đến người dùng

GIÁ TRỊ MANG LẠI

- Phòng thủ chủ động, tự động với tỷ lệ chính xác cao.
- Đơn giản hóa luồng giám sát & xử lý.
- Nắm bắt trực quan tình hình an ninh mạng của tổ chức ở lớp thiết bị đầu cuối.
- Tự động hóa tối đa giảm thời gian, thao thác vận hành.
- Tiêu tốn ít tài nguyên.

TÍNH NĂNG CHÍNH

Báo cáo theo thời gian thực

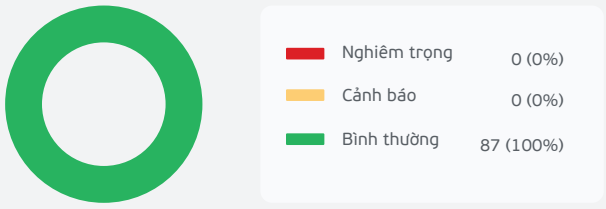
Hiển thị trực quan tình hình an toàn thông tin trên toàn hệ thống và trên từng máy người dùng

Khả năng bảo vệ toàn diện

Cung cấp cơ chế tự động phát hiện và diệt mã độc, hoặc chủ động quét với phạm vi không giới hạn, đảm bảo trạng thái an toàn cho tổ chức

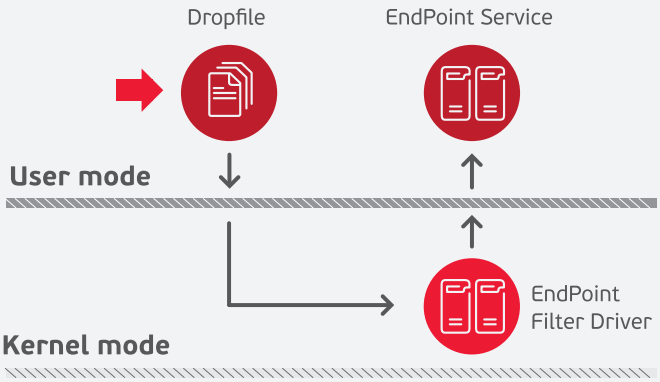
CÁC MÁY THEO TRẠNG THÁI

Hiện thị trạng thái của các máy trong mạng



Tăng cường khả năng phòng thủ

Cung cấp cơ chế cho phép thành phần agent giám sát chủ động dưới kernel mode, bắt các sự kiện khi mã độc xâm nhập và tiêu diệt tự động và ngay lập tức



Giao diện thân thiện, dễ sử dụng

Giao diện điều khiển được thiết kế tối ưu nhất cho đội ngũ vận hành giúp cho việc dễ dàng giám sát hệ thống mà không phải thực hiện nhiều thao tác.

Hoạt động nhẹ nhàng

Thiết kế tối ưu với người dùng, hoạt động nhẹ nhàng, tiêu tốn ít tài nguyên.

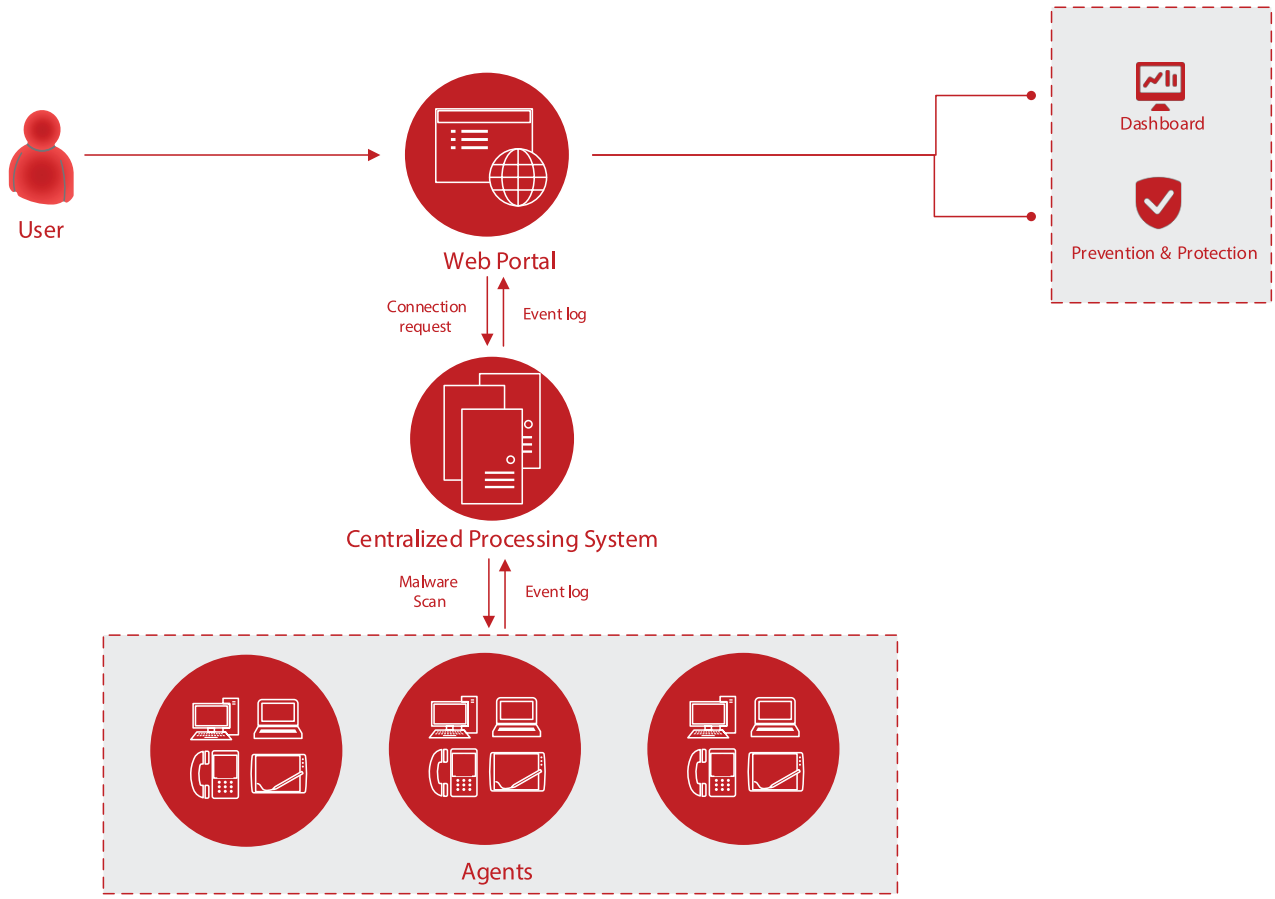
Datasheet

Viettel Endpoint Detection & Response

(VCS - aJiant)

viettel security

MÔ HÌNH TRIỂN KHAI



Hệ thống VCS-aJiant bao gồm 03 thành phần chính:

Agents

Là thành phần được cài đặt trên từng máy tính, có nhiệm vụ giám sát các dấu hiệu bất thường, ngăn chặn, gỡ bỏ chương trình độc hại một cách triệt để trên hệ thống và gửi kết quả về máy chủ tập trung.

Cụm máy chủ xử lý tập trung và lưu trữ

Là thành phần xử lý dữ liệu do Agent gửi về, đóng vai trò chính trong việc phân tích và xử lý dữ liệu theo thời gian thực.

Web Portal

Là thành phần người quản trị sẽ sử dụng để theo dõi, giám sát và phân tích các thông tin của hệ thống.

Viettel Endpoint Detection & Response
(VCS - aJiant)

viettel security

GIẢI PHÁP

VCS-aJiant kết hợp đầy đủ tính năng của Giải pháp phát hiện & chống tấn công có chủ đích lớp endpoint (Endpoint Detection & Response - EDR) và Giải pháp bảo vệ & phòng chống mã độc trên toàn bộ hệ thống (Endpoint Protection Platform - EPP). Được xây dựng dựa trên công nghệ tiên tiến trên thế giới, phù hợp với mọi mô hình tổ chức & doanh nghiệp, VCS – aJiant đảm bảo loại bỏ tất cả nguy cơ bị khai thác & chiếm quyền điều khiển cũng như đáp ứng đầy đủ nhu cầu phòng chống mã độc tại doanh nghiệp & tổ chức, nhằm phản ứng, ngăn chặn, bảo vệ một cách triệt toàn bộ hệ thống mà không ảnh hưởng đến người dùng. Đồng thời, tự động hóa tác vụ, từ đó tiết kiệm thời gian & giảm thiểu thao tác điều hành trong hệ thống.

TÍNH NĂNG CHÍNH	MÔ TẢ TÍNH NĂNG	PHIÊN BẢN ĐÁP ỨNG		
		EDR	EPP	EDP
1. Tính năng hỗ trợ theo dõi, thống kê				
Agent Management	*Quản lý thông tin máy trạm, hỗ trợ gỡ cài đặt agent từ xa*	✓	✓	✓
Group Management	*Cho phép tạo nhóm và phân loại máy trạm theo nhóm định nghĩa*	✓	✓	✓
Account Management	*Hỗ trợ tạo tài khoản người dùng, phân quyền theo vai trò*	✓	✓	✓
2. Tính năng ngăn chặn sự cố				
Application IOCs Block	*Cấu hình chặn ứng dụng độc hại hoạt động trên máy trạm*	✓		✓
Network IOCs Block	*Cấu hình chặn kết nối độc hại từ máy trạm*	✓		✓
3. Tính năng cảnh báo và xử lý cảnh báo				
Detection	*Phát hiện dấu hiệu tấn công nâng cao APT theo MITRE ATT&CK*	✓		✓
Alert Management	*Theo dõi và quản lý cảnh báo*	✓		✓
Incident Response Flow	*Cho phép điều tra phản ứng trên một giao diện duy nhất*	✓		✓
4. Tính năng điều tra				
Process Analysis	*Phân tích tiến trình đang chạy từ xa trên máy mục tiêu*	✓		✓
Event Search	*Tìm kiếm log event trên toàn bộ máy trạm*	✓		✓
Deploy Tools	*Quản lý & triển khai công cụ điều tra/xử lý sự cố trên máy trạm trong tổ chức*	✓		✓
Containment	*Hỗ trợ cô lập (network, process) tạm thời các máy phục vụ điều tra*	✓		✓
5. Tính năng phản ứng nhanh				
Live Response	*Thực hiện remote console từ xa tới máy mục tiêu để điều tra xử lý*	✓		✓
Response Scenario	*Cho phép định nghĩa kịch bản xử lí sự cố trên diện rộng một cách tự động*	✓		✓
6. Tính năng Diệt mã độc				
Real-time Protection	*Tự động phát hiện và tiêu diệt mã độc trên máy trạm*		✓	✓
Scan OnDemand	*Cho phép người dùng chủ động quét mã độc bằng quét nhanh, quét toàn bộ, quét thư mục theo nhu cầu*		✓	✓
Anti Ransomware	*Phát hiện và tiêu diệt mã độc mã hóa tống tiền*		✓	✓
Endpoint Firewall	*Thiết lập chính sách để kiểm soát truy cập mạng trong tổ chức*		✓	✓
Scan Scheduler	*Thiết lập lịch quét mã độc dưới các máy trạm từ xa*		✓	✓
Device Control	*Kiểm soát, bảo vệ dữ liệu quan trọng thông qua thiết bị ngoại vi: USB, CD, DVD, thiết bị Bluetooth*		✓	✓