Datasheet

Viettel Endpoint Detection & Response
(VCS-aJiant phiên bản EDP)

"Giải pháp toàn diện bảo vệ, phát hiện và xử lý chủ động trước các nguy cơ tấn công mạng, đảm bảo an toàn cho thiết bị đầu cuối của doanh nghiệp và tổ chức."

THÁCH THỨC

Các cuộc tấn công mạng ngày nay ngày một đa dạng về quy mô và mục đích, không chỉ đơn thuần là những hành vi xâm nhập hệ thống, khai thác thông tin, trục lợi vì mục đích cá nhân mà còn là những cuộc tấn công có tổ chức, có động cơ kinh tế và chính trị. Các cuộc tấn công có thể kéo dài hàng tháng, tới hàng năm; các loại mã độc được tạo ra, dành riêng để vượt qua các hệ thống bảo vệ của tổ chức, chiếm quyền và thực hiện tấn công leo thang gây ra những thiệt hại nặng nề đến tổ chức, doanh nghiệp.

GIẢI PHÁP

VCS - aJiant là giải pháp đảm bảo an toàn thiết bị đầu cuối một cách toàn diện, kết hợp trọn vẹn tính năng của Endpoint Detection & Response (EDR) và Endpoint Protection Platform (EPP). Giải pháp đáp ứng nhu cầu bảo vệ và phòng chống mã độc tại các doanh nghiệp và tổ chức; phản ứng, ngăn chặn, gỡ bỏ chương trình độ hại một cách triệt để trên toàn bộ hệ thống.
Bên cạnh đó, phát hiện các dấu hiệu tấn công sớm nhất với độ chính xác cao có thể điều tra, loang rộng để đánh giá quy mô, hậu quả của chiến dịch tấn công; tự động hóa các công việc một cách tối đa để tiết kiệm thời gian và giảm thiểu các thao tác vận hành với hệ thống.

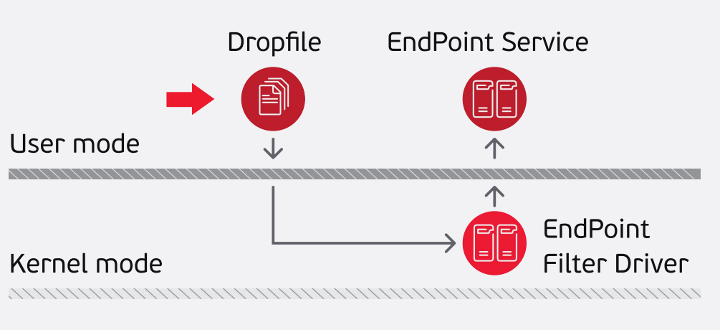
HIGHLIGHT VALUES

- Bảo vệ toàn diện các thiết bị đầu cuối.
- Giám sát các hành vi bất thường theo
- chuẩn MITRE ATT&CK.
- Bảo vệ chủ động và toàn diện đối với tấn công nâng cao có chủ đích APT (EDR) và tự động diệt mã độc thông thường (EPP)
- Phản ứng nhanh, chủ động, tự động.
- Phân tích & truy vết chuyên sâu bằng khả năng biểu diễn kill chain map trực quan.
- Tiết kiệm thời gian xử lý sự cố.
- Quản trị hiệu quả quy trình xử lý sự cố thông qua các chỉ số thời gian.

TÍNH NĂNG CHÍNH

Phòng chống mã độc toàn diện, chủ động

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



Giám sát hành vi mức driver

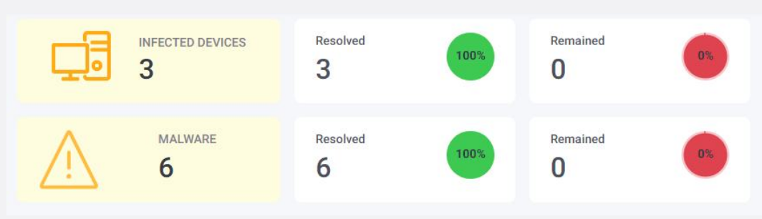
Sử dụng công nghệ Filter Driver giám sát tất cả các hành vi liên quan đến File, Process, Memory, Registry, Network trên máy tính người dùng và máy chủ. Các hành vi nghi ngờ được đẩy về thành phần server phân tích tập trung.

Tích hợp với các giải pháp bên thứ ba

Tích hợp với các nguồn tri thức bên thứ ba như Threat Intelligence, SOAR, SIEM.

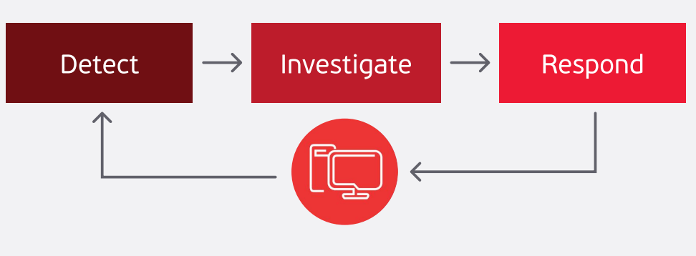
Báo cáo theo thời gian thực

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



Phản ứng sự cố nhanh chóng, chủ động

Luồng nghiệp vụ điều tra tấn công được thiết kế khép kín, hỗ trợ phát hiện và phân tích các dấu hiệu bất thường trên giao diện điều khiển. Cung cấp chức năng điều tra truy vết (Forensic) chuyên sâu trên thiết bị endpoint. Ngay khi xác minh được bất thường, cung cấp các công cụ gỡ bỏ mã độc diện rộng.

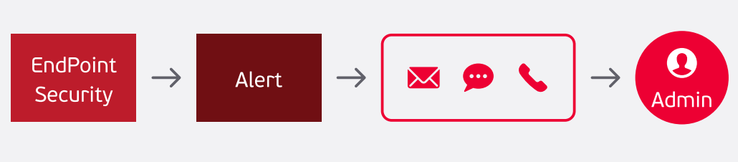


Tích hợp và hỗ trợ đa nền tảng

Hỗ trợ đa nền tảng gồm Windows, Linux

Giao diện quản trị thân thiện

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



Thiết lập chính sách ATTT

Hỗ trợ các chính sách An toàn thông tin như: Kiểm soát thiết bị ngoại vi, cung cấp remote an toàn (Security Helpdesk) giảm thiểu nguy cơ lây nhiễm mã độc.

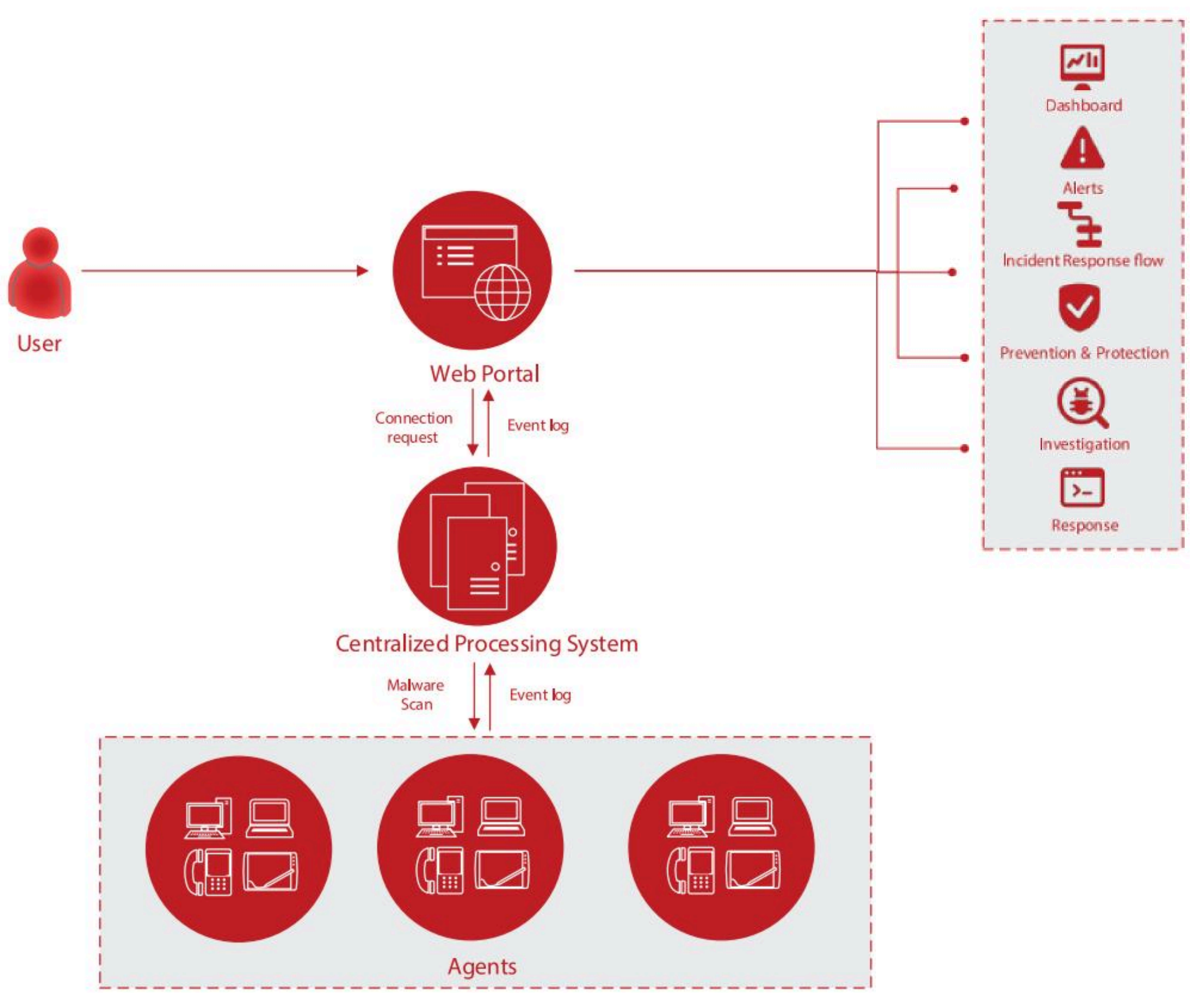
Phân tích tập trung

Áp dụng nhiều công nghệ như phát hiện bất thường theo IOC/IOAs, mô hình hóa hành vi, xâu chuỗi các mối quan hệ giữa các đối tượng nghi ngờ và làm nổi bật bất thường, mã độc chưa từng được biết trên thế giới.

Hoạt động nhẹ nhàng

Thiết kế tối ưu với người dùng, hoạt động nhẹ nhành và hoàn toàn trong suốt.

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 trên máy tính, gửi log về server tập trung.

Cụm máy chủ xử lý tập trung và lưu trữ

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

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.

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				
Dashboard	*Biểu đồ thống kê trực quan giúp theo dõi, báo cáo tình hình giám sát ATTT trong tổ chức*	✓	✓	✓
Software Statictis	*Thống kê danh sách phần mềm cùng phiên bản đang cài đặt ở máy tính*	✓		✓
2. Tính năng hỗ trợ cấu hình, cài đặt, quản trị hệ thống				
Agent Management	*Quản lý thông tin máy tính, hỗ trợ gỡ cài đặt agent từ xa*	✓	✓	✓
Agent Policy Management	*Quản lý và thiết lập cấu hình của agent từ xa*	✓	✓	✓
Group Management	*Cho phép tạo nhóm và phân loại máy tính theo nhóm định nghĩa*	✓	✓	✓
Account Management	*Hỗ trợ tạo tài khoản người dùng, phân quyền theo vai trò*	✓	✓	✓
Role & Permission Management	*Hỗ trợ phân quyền tài khoản người dùng theo vai trò*	✓	✓	✓
Agent Recovery Handler	*Tính năng hỗ trợ khôi phục từ xa hoạt động của agent trong trường hợp agent bị lỗi*	✓	✓	✓
Update Management	*Tính năng quản lý cập nhật phiên bản cho sản phẩm, hỗ trợ cập nhật thủ công, tự động, lập lịch, cập nhật theo nhóm agents*	✓	✓	✓
Performance Control	*Tính năng kiểm soát hiệu năng agent (CPU, RAM, DiskIO, Network) đảm bảo agent hoạt động không quá hiệu năng cho phép*	✓	✓	✓
Self Defense	*Tính năng tự bảo vệ thành phần agents, tránh bị tác động trái phép*	✓	✓	✓
3. Tính năng ngăn chặn sự cố				
IOC Management	*Cho phép user thêm các IOCs (dạng hash, ip) để:* *+ Chặn các ứng dụng độc hại hoạt động trên máy trạm bằng cách định nghĩa path/hash* *+ Chặn kết nối độc hại từ máy trạm*	✓		✓
4. Tính năng cảnh báo và xử lý cảnh báo				
Monitor & Detection	*Phát hiện hành vi tấn công cao cấp APT theo MITRE ATT&CK*	✓		✓
Alerts Management	*Theo dõi và quản lý cảnh báo*	✓	✓	✓
Rule Correlation Management	*Tính năng quản lý tập luật sinh alert, cho phép định nghĩa và tạo điều kiện phát sinh cảnh báo ATTT*	✓		✓
5. Tính năng điều tra và săn lùng				
Process Analysis	*Phân tích tiến trình đang chạy từ xa trên máy mục tiêu*	✓		✓
Events Search	*Tìm kiếm log event trên toàn bộ máy tính*	✓	✓	✓
Deploy Tools	*Quản lý & triển khai công cụ điều tra/xử lý sự cố trên máy tính trong tổ chức*	✓		✓
Threat Hunting	*Chủ động săn lùng phần mềm độc hại và mối đe dọa theo IOC*	✓		✓
Network Isolate	*Hỗ trợ cô lập (network) tạm thời các máy phục vụ điều tra*	✓		✓
6. Tính năng phản ứng nhanh				
Live Response	*Thực hiện remote console từ xa tới máy mục tiêu để điều tra xử lý*	✓	✓	✓
7. Tính năng diệt mã độc				
Real-time Protection	*Tự động phát hiện và tiêu diệt mã độc trên máy tính*		✓	✓
Auto Backup	*Tự động sao lưu file trước khi diệt mã độc, cho phép khôi phục mã độc từ file sao lưu*		✓	✓
Malware Report	*Báo cáo số liệu mã độc theo thời gian, file mã độc, loại mã độc*		✓	✓
Exclusion List	*Cho phép người dùng cấu hình danh sách loại trừ theo thư mục hoặc theo loại tệp tin khỏi việc quét mã độc*		✓	✓
Scan On-Demand	*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 tống tiền*		✓	✓
Endpoint Firewall	*Thiết lập chính sách & kiểm soát truy cập mạng trong tổ chức*		✓	✓
Scan Scheduler	*Thiết lập lịch quét mã độc trên các máy tính từ xa*		✓	✓
Device Control	*Kiểm soát, bảo vệ dữ liệu quan trọng thông qua thiết bị ngoại vi: USB, CD, DVD, thiết bị Bluetooth*		✓	✓
Host Intrusion Prevention System (HIPS)	*Phòng vệ chủ động dựa trên phân tích hành vi*		✓	✓