Datasheet

# Viettel Endpoint Detection & Response

(VCS - aJiant)

viettel security

*"Giải pháp toàn diện giúp bảo vệ, phát hiện, phòng chống mã độc 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; đồng thời các loại mã độc được tạo ra nhằm mục đích vượt qua các hệ thống bảo vệ, chiếm quyền và thực hiện tấn công leo thang gây ra những thiệt hại nặng nề cho các tổ chức, doanh nghiệp.

## GIÁ TRỊ MANG LẠI

- Bảo vệ toàn diện các thiết bị đầu cuối, giám sát tuân thủ chính sách của tổ chức.
- 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 và tự động diệt mã độc thông thường.
- Phân tích và truy vết chuyên sâu bằng khả năng biểu diễn kill chain map trực quan.
- Phản ứng nhanh chóng, chủ động, tự động, tỷ lệ chính xác cao.
- Tiết kiệm thời gian xử lý sự cố, giảm thiểu tỷ lệ cảnh báo sai (false positive).
- Quản trị hiệu quả quy trình xử lý sự cố, tiết kiệm thời gian, tối ưu vận hành.

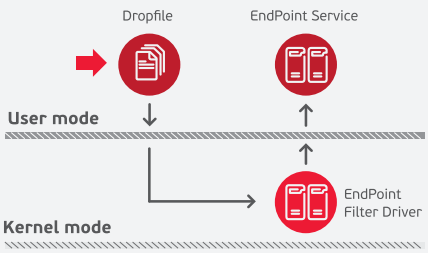
## TÍNH NĂNG CHÍNH

### 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 backend phân tích tập trung.




### Phân tích tập trung

Áp dụng nhiều công nghệ như phát hiện bất thường theo IOC/IOAs, mô hình hóa hành vi, xâu chuỗi mối quan hệ giữa các đối tượng nghi ngờ & làm nổi bật bất thường, mã độc chưa từng được biết trên thế giới. Hỗ trợ cấu hình tự động hoặc bằng tay gom nhóm cảnh báo theo các chuỗi tấn công.

### Báo cáo theo thời gian thực

Hiển thị trực quan tình hình ATTT trên toàn hệ thống & 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 thông qua việc phân tích các tiến trình, tìm kiếm log hoàn toàn từ xa. Ngay khi xác minh được bất thường, cung cấp các công cụ gỡ bỏ mã độc diện rộng và cho phép thiết lập chính sách chặn các ứng dụng và kết nối độc hạ.


### Hỗ trợ đa nền tảng

Hỗ trợ đa nền tảng: Windows, Linux, MacOS.

### 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. Người quản trị dễ dàng thực hiện quản lý tập luật bảo vệ bằng các hành động thêm/xóa/tinh chỉnh/tìm kiếm/kích hoạt/vô hiệu. Các tập luật được hỗ trợ export/import bằng các tệp tin, và được cập nhật liên tục từ nhà sản xuất qua thao tác tự động hoặc bằng tay.


### 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. Cho phép áp dụng chính sách cấu hình agent theo từng nhóm khác nhau.

### Hoạt động nhẹ nhàng

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

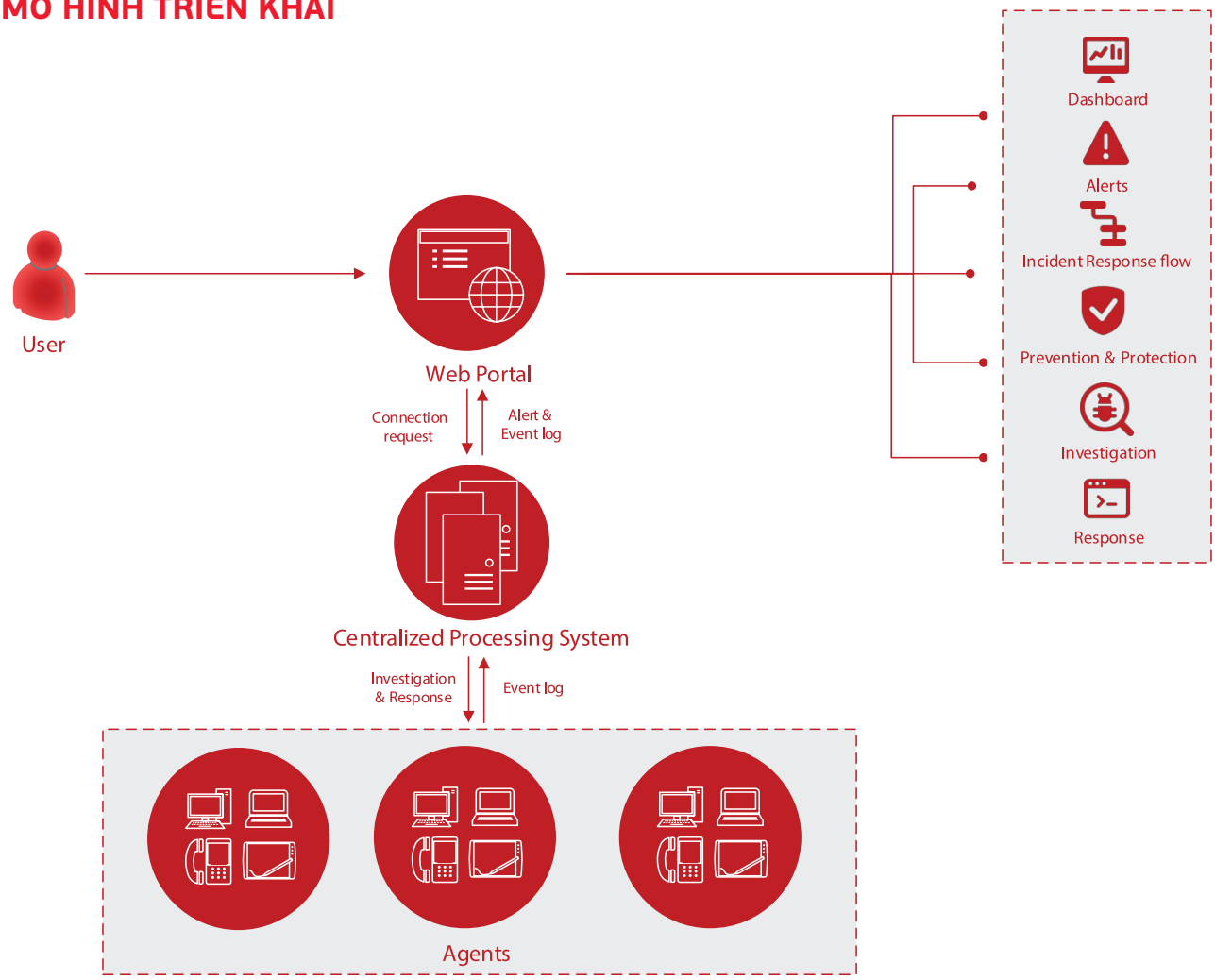
### Tích hợp với các giải pháp bên thứ ba

Tích hợp với các nguồn tri thức bên thứ ba như Threat Intelligence, Advanced Malware Analysis (Phân tích mã độc chuyên sâu), SOAR, SIEM.

# 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 trên máy tính, gửi log về máy chủ xử lý tập trung trên kết nối có xác thực và được mã hóa SSL.

**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 mà người quản trị sẽ sử dụng để theo dõi, giám sát và phân tích thông tin của hệ thống. Web Portal cung cấp giao diện trực quan, giúp người quản trị theo dõi, xem thông tin cảnh báo, điều tra và phản ứng trên một giao diện tập trung duy nhất. Người quản trị thực hiện quản lý tập trung, cấu hình từ xa thành phần Agent tùy theo mục đích sử dụng.

# 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* | | ✓ | ✓ |