Viettel Endpoint Detection & Response
(VCS-aJiant EPP version)

viettel security

"A solution to protect and prevent malwares, ensuring the safety of organizations' endpoints."

▶ CHALLENGES

Today, it is more and more challenging for organizations to detect, identify, investigate and reduce advanced attacks on systems.

Regarding large enterprises and organizations, they have to encounter targeted, organized and highly complex attacks that make conventional solutions undetectable.

Regarding small and medium enterprises, with the lack of necessary cybersecurity equipment, experience and management skills, their main concern is malwares causing slow down, crashes, and ransomware.

▶ SOLUTION

The VCS - aJiant solution provides a compact version of the Endpoint Protection Platform (EPP) that is suitable for anti-malware protection and prevention in businesses and organizations. This solution includes a group of features related to anti-malware to be able to thoroughly respond, prevent, and remove malicious programs on the entire system without affecting users.
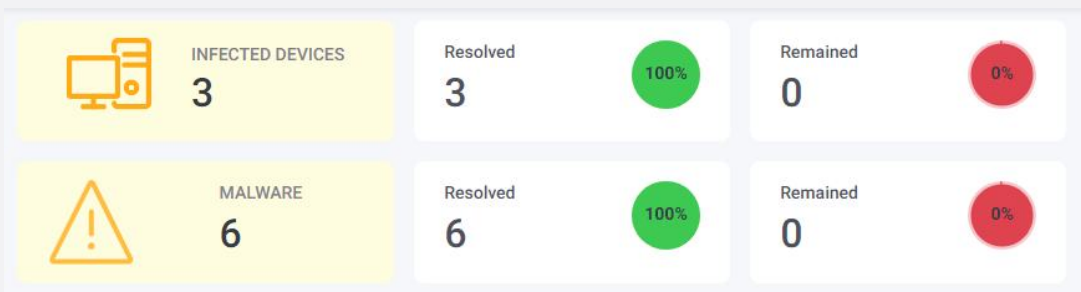
▶ HIGHLIGHT VALUES

- Active and automatic defense with high accuracy rate.

- Simplification of monitoring & processing flow.

- Visual grasp of the organization's network security situation at the endpoint layer.

- Maximum automation to save time and simplify operation.

- Low resource consumption.

▶ KEY FEATURES

■ Real-time Reporting

Cybersecurity situation is visually displayed on the whole system and on each user's machine.

| INFECTED DEVICES 3 | Resolved 3 | 100% | Remained 0 | 0% |
| MALWARE 6 | Resolved 6 | 100% | Remained 0 | 0% |

■ Comprehensive Protection

There is a mechanism that automatically detect and remove malwares, and proactively scan with unlimited scope, ensuring a safety for the organization.

Device by status

- Critical — 0 (0%)
- Alert — 0 (0%)
- Normal — 87 (100%)
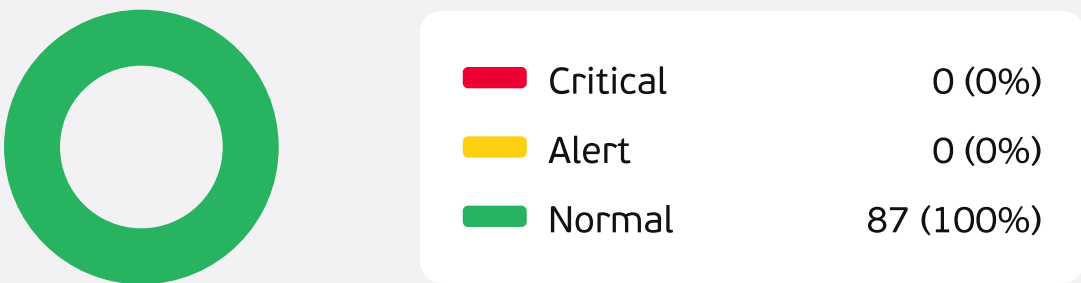
■ Defense Enhancement

There is also a mechanism that allows the agent component to actively monitor in kernel mode, and automatically and immediately catch events when malware enters and destroy.

Dropfile   EndPoint Service

User mode

Kernel mode   EndPoint Filter Driver
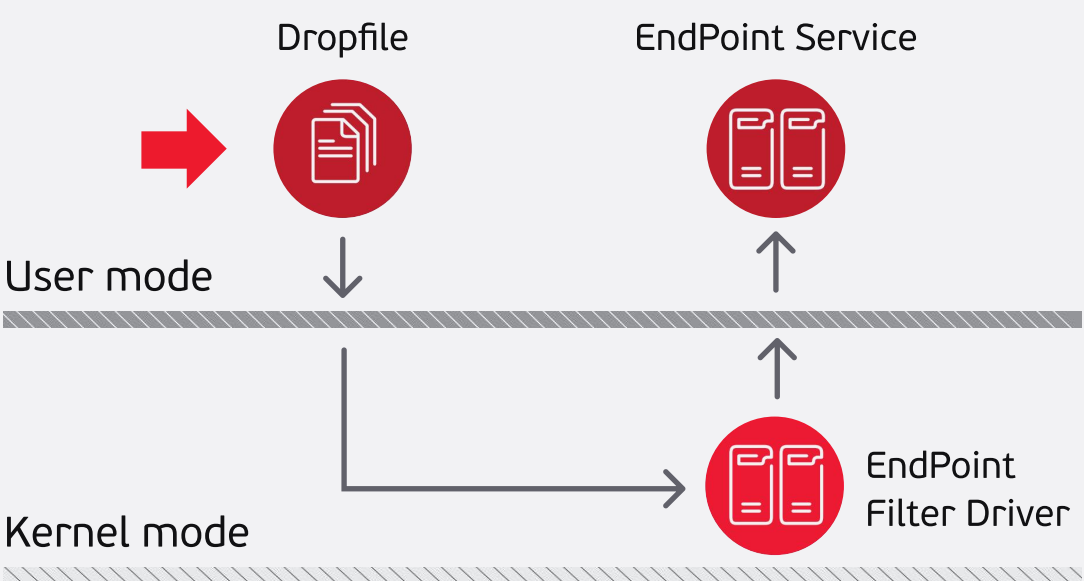
■ Friendly Admin Interface

The design of the control interface is optimized so that the operating team can easily monitor the system without performing multiple operations.
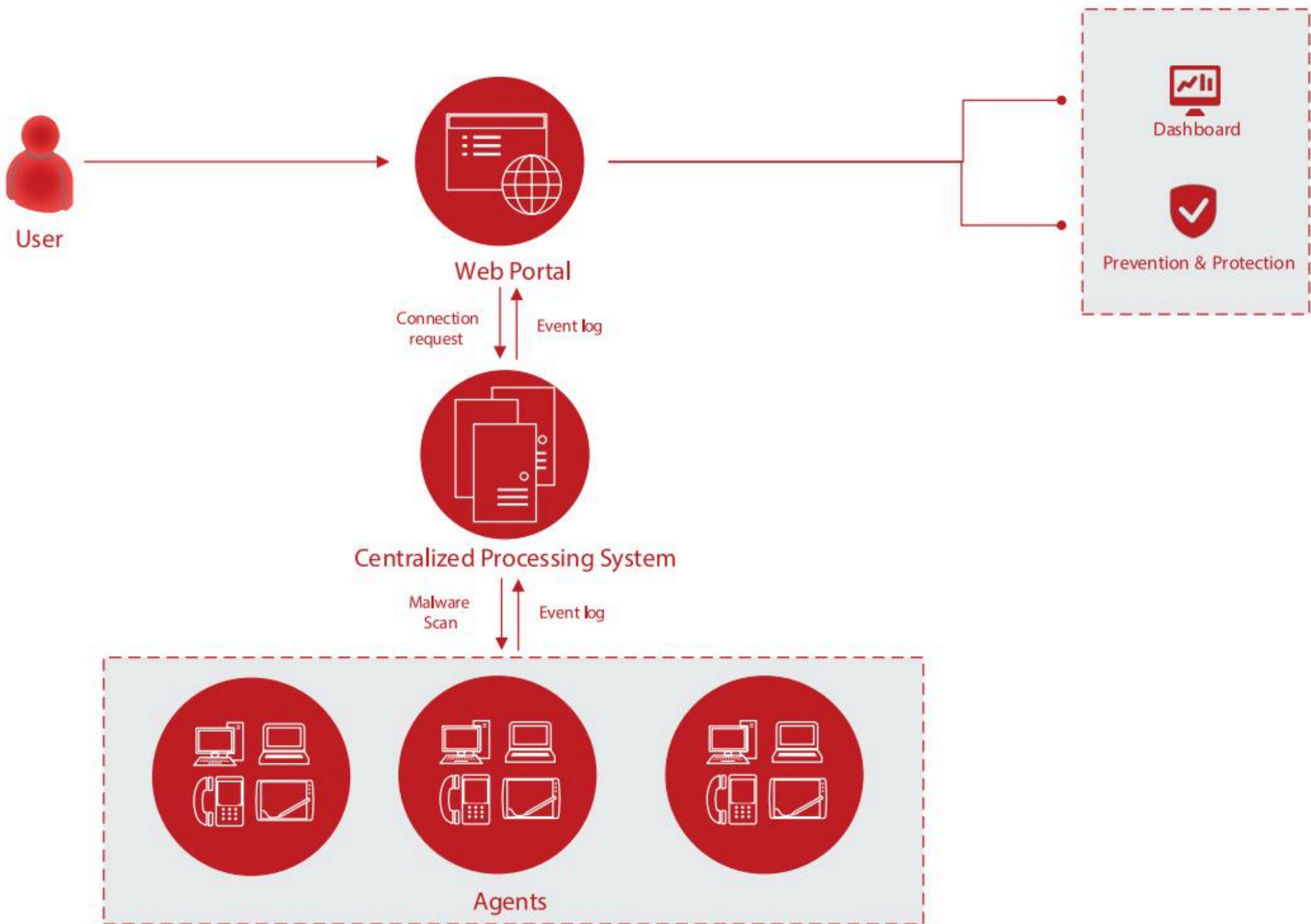
■ Smooth Operation

The solution provides a user-optimized design, lightweights operation, and low resource consumption.

Viettel Endpoint Detection & Response
(VCS-aJiant EPP version)

viettel security

▶ DEPLOYMENT MODEL

User → Web Portal → Dashboard / Prevention & Protection

Connection request / Event log

Centralized Processing System

Malware Scan / Event log

Agents

VCS - aJiant system includes 03 main components:

Agents

A component installed on each computer, responsible for monitoring anomaly, thoroughly preventing and removing malicious programs on the system and sending logs to a centralized server.

Cluster of servers for centralized processing and storage

A component to process data sent from Endpoint, playing a key role in analyzing and processing data in real-time.

Web Portal

A component for administrators, used to monitor and analyze system information.