Datasheet

Viettel Endpoint Detection & Response

(VCS - aJiant)

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.

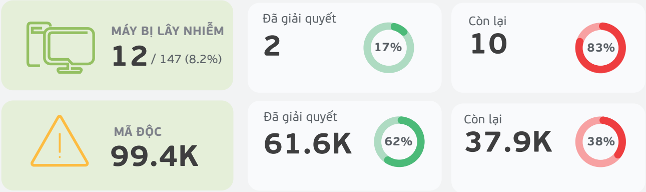
HIGHLIGHT VALUES

- 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.



MÁY BỊ LÂY NHIỄM 12 / 147 (8.2%)

Đã giải quyết 2 17%

Còn lại 10 83%

MÃ ĐỘC 99.4K

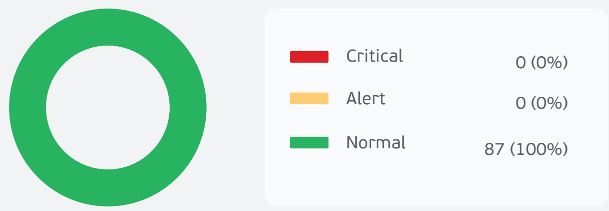
Đã giải quyết 61.6K 62%

Còn lại 37.9K 38%

Comprehensive Protection

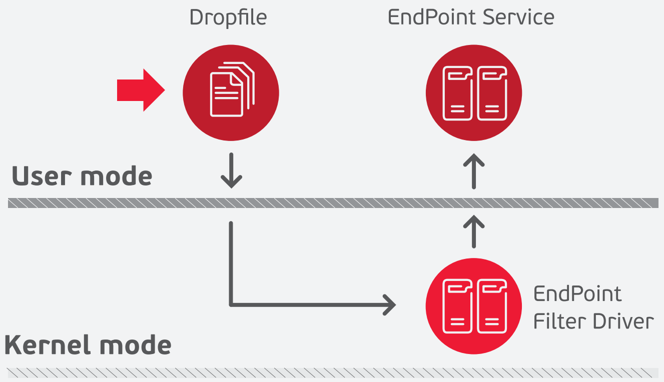
There is a mechanism that automatically detect and remove malwares, and proactively scan with unlimited scope, ensuring a safety for the organization.

Devices by Status



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.



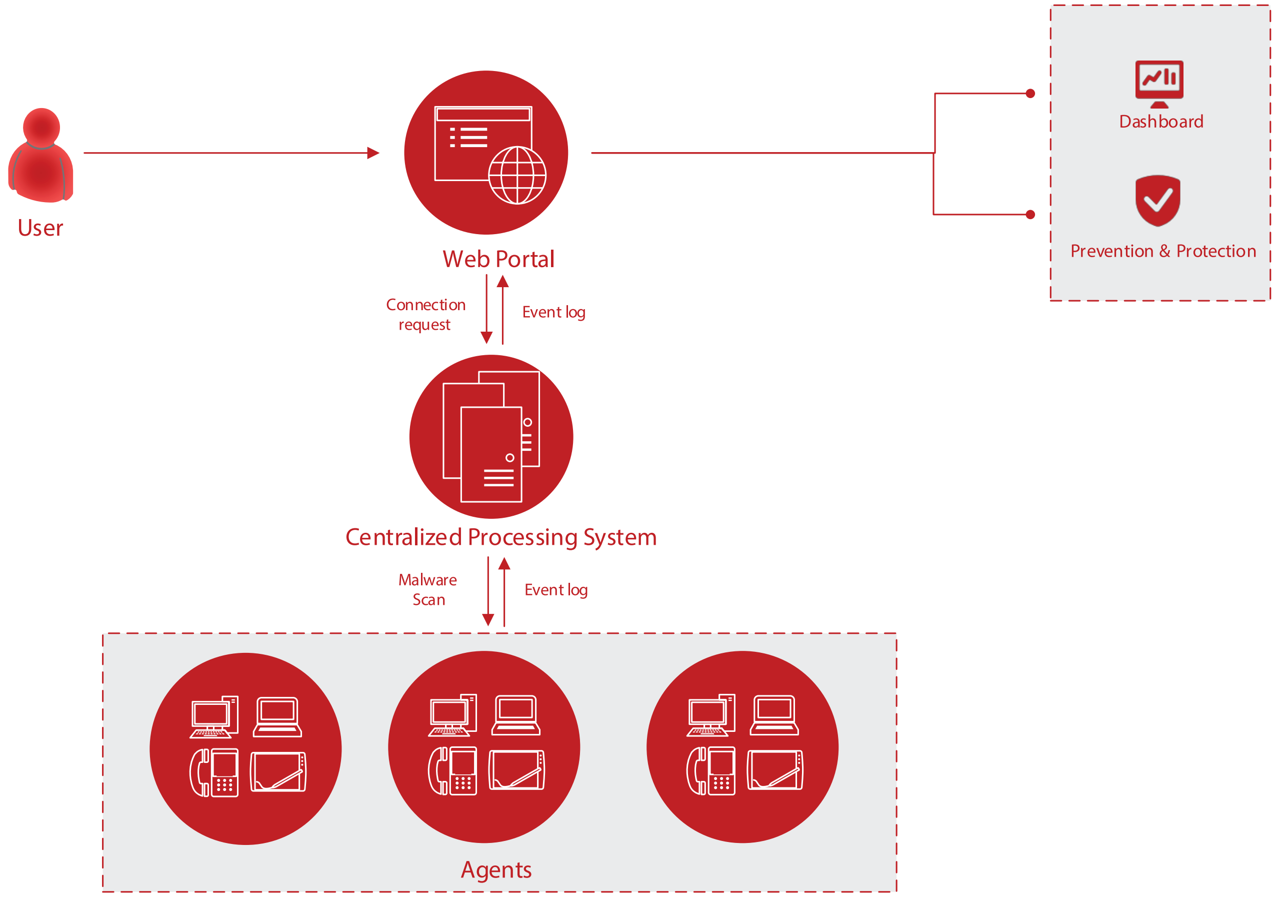
Friendly Admin Interface

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, lightweight operation, and low resource consumption.

DEPLOYMENT MODEL



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.

SOLUTION

The VCS-aJiant solution fully combine features of Endpoint Detection & Response - EDR and Endpoint Protection Platform - EPP. Built on the latest technologies in the world and suitable for all organization and business types, VCS – aJiant ensures that all risks of exploiting and hacking are eliminated and meets fully the demand for malware prevention in the enterprises and organizations, in order to respond, prevent and protect thoroughly the entire system without affecting users. Also, the solution can automate the tasks, save time and minimize operation tasks in the system.

KEY FEATURES	Features description	Version		
		EDR	EPP	EDP
1. Tracking and statistics support feature				
Rules Correlation	*Manage alert rulesets*	✓		✓
Agents Management	*Manage workstation information, support remotely agent uninstallation*	✓	✓	✓
Groups Management	*Group and classify workstations by defined groups*	✓	✓	✓
Accounts Management	*Support to create user accounts, authorization by roles*	✓	✓	✓
2. Incident prevention feature				
Applications IOCs Block	*Set to block malicious applications from operating on workstations*	✓		✓
Network IOCs Block	*Set to block malicious connections from workstations*	✓		✓
3. Alert and alert processing feature				
Detection	*Detect signs of advanced APT attacks according to MITER ATT&CK*	✓		✓
Alerts Management	*Monitor and manage alerts*	✓		✓
Incident Response Flow	*Investigate incident response on a single interface*	✓		✓
4. Investigation feature				
Process Analysis	*Analyze the process remotely on the target computer*	✓		✓
Events Search	*Search event log on the entire workstations*	✓		✓
Deploy Tools	*Manage and deploy investigating/troubleshooting tools on workstations in the organization*	✓		✓
Containment	*Support temporary isolation (network, process) of investigating devices.*	✓		✓
5. Quick response feature				
Live Response	*Execute remote console to the target computer for investigating and processing purposes*	✓		✓
Response Scenario	*Allows the definition of large-scale incident response scenarios automatically*	✓		✓
6. Anti-Malware feature				
Real-time Protection	*Automatically detect and destroy malware on agents*		✓	✓
Scan OnDemand	*Allows users to proactively scan for malware with quick scans, full scans and folder scans as needed*		✓	✓
Anti Ransomware	*Automatically detect and destroy ransomware on agents*		✓	✓
Endpoint Firewall	*Set up policies to control network traffic in the organization*		✓	✓
Scan Scheduler	*Set up the malware scanning schedule on agents remotely*		✓	✓
Device Control	*Control and protect important data through peripheral devices: USB, CD, DVD, Bluetooth devices*		✓	✓
HIPS	*Detect and prevent malware based on behavior analysis technology*		✓	✓
Web protection	*Protect users from malicious, phishing, scams, steal data... sites*		✓	✓