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

viettel security

"A comprehensive solution to protect security and proactively detect & deal with cyber-attack threats, ensuring the safety of organizations' endpoints."

CHALLENGES

Today, cyber-attacks are increasingly diverse in both scale and purpose. They are not only individual attacks for personal purposes (infiltrating the system, exploiting information, and profiting), but also organized attacks with economic and political motives.
These attacks can last for months or even years. The malwares are created specifically to bypass the protection systems of the organization, in order to take over and carry out the attack to escalate, resulting in heavy damage to the organization.

SOLUTION

VCS - aJiant is a comprehensive endpoint security solution, with a full-feature combination of Endpoint Detection & Response (EDR) and Endpoint Protection Platform (EPP). The solution can meet the needs of anti-malware prevention in businesses and organizations; helps to respond, prevent, and remove malicious programs thoroughly on the entire system.
Besides, the solution can also detect signs of attack from the very beginning with high accuracy; investigate and spread to assess the scale and consequences of the attack campaign; automate tasks thoroughly to save time and minimize operating operations in the system.

HIGHLIGHT VALUES

- Comprehensive protection of endpoint devices.
- Monitoring for abnormal behavior according to MITRE ATT&CK standards.
- Comprehensive and proactive protection against Advanced Persistent Threat (EDR) and automatic removal of malware (EPP).
- Quick, proactive, and automatic response.
- In-depth analysis & tracing with an intuitive kill chain map representation.
- Incident response time savings.
- Effective process management of incident response by time metrics.

KEY FEATURES

Comprehensive and Proactive Anti-malware

There is a mechanism that allows the agent component to actively monitor in kernel mode and automatically capture and remove events that have been compromised by malwares.

Behavior Monitoring by Filter Driver

The Filter Driver technology can monitor all related-behavior of File, Process, Memory, Registry, Network on personal computers and servers. Suspicious behavior will be pushed to the centralized analysis server component.

Integration with Third-party Solutions

This solution is also integrated with third-party knowledge sources such as Threat Intelligence, SOAR, and SIEM.

Real-time Reporting

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

Quick and Proactive Incident Response

Thanks to the closed business flow to investigate attack, this solution provides the detection and analysis of anomalies on the console and an in-depth Forensic function on endpoints. As soon as the anomaly is verified, the function provides extensive malware removal tools.

Cross-platform Integration and Support

Support multi OS Platform: Windows, Linux, MacOS

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.

Cybersecurity Policy Support

The Information Security policies are supported, such as Control peripheral devices and Security Helpdesk to reduce the risk of malware infection.

Centralized Analysis

This solution applies some technologies such as anomaly detection according to IOC/IOAs, behavior modeling, chaining relationships between suspect objects, and highlighting anomalies and malwares that have never been known in the world.

Smooth Operation

The design is lightweight and the system is completely transparent.

viettel security

Datasheet

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

viettel security

DEPLOYMENT MODEL

VCS-aJiant system includes 03 main components:

Agents

A component installed on each computer, responsible for monitoring

abnormal signs on the computer 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.

Viettel Cyber Security
For more information go to ▸ www.viettelcybersecurity.com

viettel security

Datasheet

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

viettel security

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 Correltation	*Manage alert rulesets*	√		√
Agents Management	*Manage endpoint information, support remotely agent uninstallation*	√	√	√
Group Management	*Group and classify endpoint by defined groups*	√	√	√
Accounts Management	*Support to create user accounts, authorization by roles*	√	√	√
2. Incident prevention feature				
IOC Management	*Allows users to add IOCs (hash, IP addresses) to block malicious applications*	√		√
3. Alert and alert processing feature				
Detection	*Detect signs of advanced APT attacks according to MITRE ATT&CK*	√		√
Alerts Management	*Monitor and manage alerts*	√		√
4. Investigation & hunting feature				
Process Analysis	*Analyze the process remotely on the target computer*	√		√
Events Search	*Search event log on the entire endpoint*	√	√	√
Deploy Tools	*Manage and deploy investigating/troubleshooting tools on endpoint in the organization*	√		√
Threat Hunting	*Proactive hunting for malware and threat*	√		√
Network Isolate	*Support temporary isolation (network) of investigating devices.*	√		√
5. Quick response feature				
Live Response	*Execute remote console to the target computer for investigating and processing purposes*	√	√	√
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*		√	√

Viettel Cyber Security
For more information go to ▸ www.viettelcybersecurity.com

viettel security