Datasheet

Viettel Endpoint Detection & Response

(VCS - aJiant)

viettel
security

> "A solution to quickly and proactively detect and deal with cyber-attack threats, ensuring the safety of organizations' endpoints."

HIGHLIGHT VALUES

- Monitoring for abnormal behavior according to MITER ATT&CK standards.
- In-depth analysis & tracing with an intuitive kill chain map representation.
- Compliance monitoring with organization's policies.
- Quick, proactive, and automatic response.
- Visual grasp of the organization's network security situation at the endpoint layer.
- Reducing of incident response time as well as false positive rate.
- Effective process management of incident response by time metrics.

CHALENGES

Today, it is more and more challenging for organizations to detect, identify, investigate and reduce advanced attacks on systems. Traditional anti-malware technologies such as signature-based antivirus also succumb to highly skilled professional attackers with targeted and customized malware and attack toolkits.

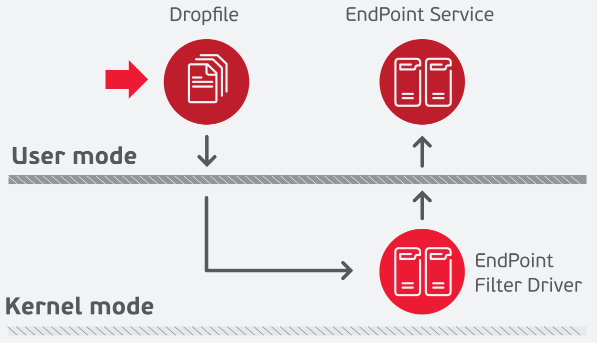
SOLUTION

Viettel Endpoint Detection & Response (VCS-aJiant), a solution to detect and prevent targeted attacks on the endpoint layer, is built based on the latest technologies in the world and suitable for all types of organizations and businesses. This solution ensures that all risks of exploitation and hijacking are eliminated.

KEY FEATURES

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 backend component.



Centralized Analysis

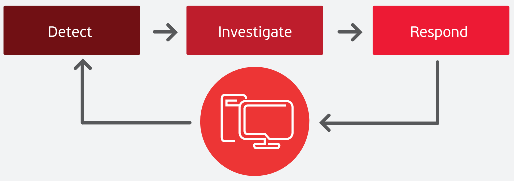
The Filter Driver technology can monitor all related-behavior of File, Process, Memory, Registry, Network on personal computers and servers. Suspicious behavior will be pushed to the centralized analysis backend component.

Cybersecurity Policy Support

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

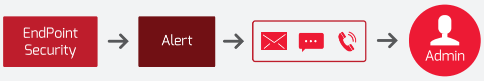
Quick and Proactive Incident Response

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 tool.



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 design is lightweight and the system is completely transparent.

Cross-platform Solutions Support and Integration

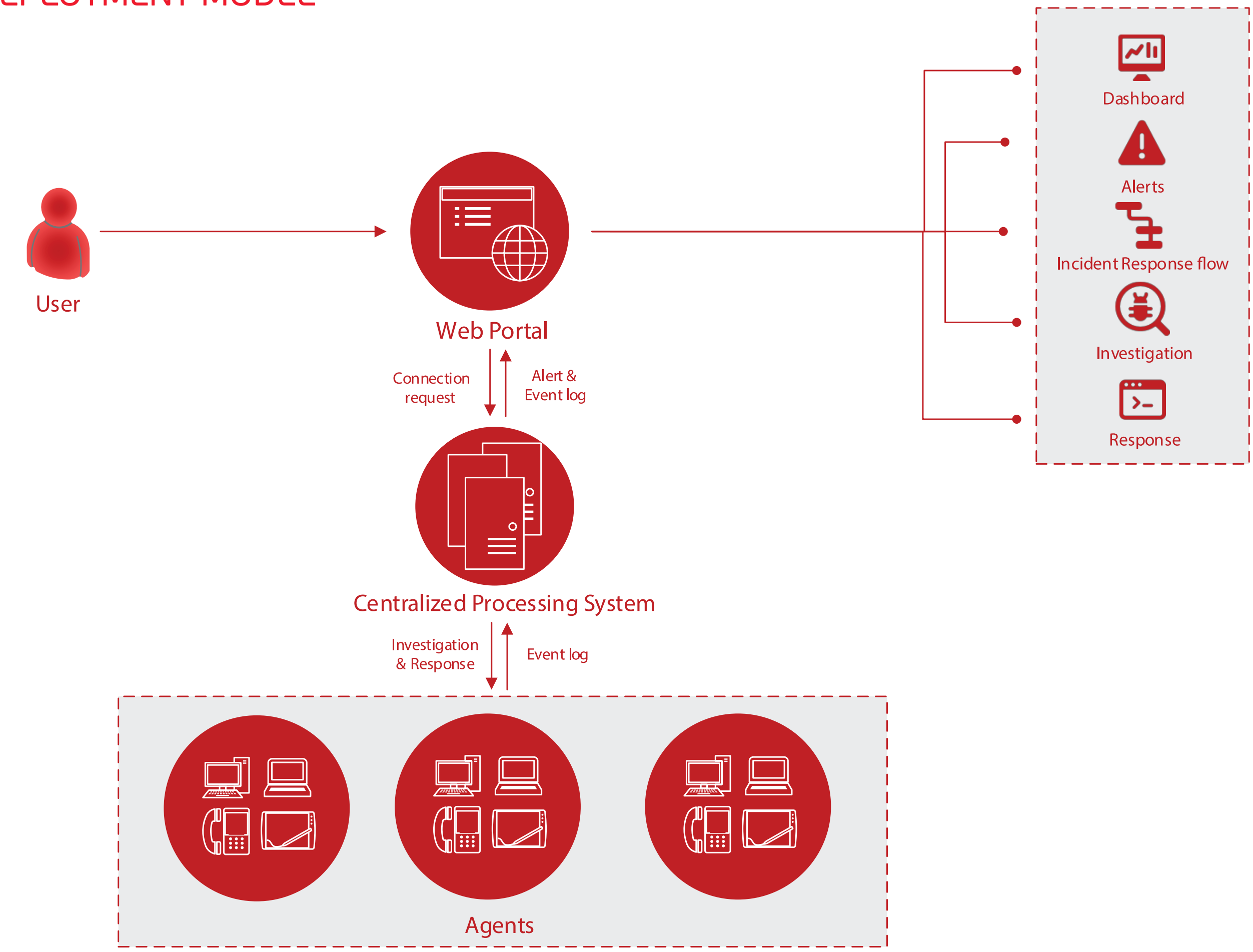
This solution is also integrated with third-party knowledge sources such as Threat Intelligence, Advanced Malware Analysis, SOAR, and SIEM.

Viettel Cyber Security

For more information, go to ▸ www.viettelcybersecurity.com

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

Cluster of servers for centralized processing and storage
A data processing component, playing a key role in analyzing and processing data sent by the Agent 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*		✓	✓