Datasheet

Viettel Endpoint Detection & Response

(VCS - aJiant)

viettel security

"A solution to protect, detect and prevent malwares; proactively deal with cyber-attack threats, ensuring the safety of organizations' endpoints."

CHALLENGES

Today's cyberattacks are increasingly diverse in scale and purpose, not only acts of penetrating, exploiting information, profiteering for personal purposes, but also organized, economically and politically motivated attacks.

These attacks can last months to years; besides, malwares are created for the purpose of passing through the protection systems, taking over and performing escalation attacks, causing severe damage to organizations and businesses.

HIGHLIGHT VALUES

- Comprehensive protection of endpoint devices, compliance monitoring with organization's policies.
- Monitoring for abnormal behavior according to MITRE ATT&CK standards.
- Comprehensive and proactive protection against advanced APT targeting attacks and automatic remove common malwares.
- In-depth analysis & tracing with an intuitive kill chain map representation.
- Quick, proactive, automatic and highly accurate response.
- Reducing of incident response time as well as false positive rate.
- Effective management of incident response process, time saving, and optimal operation.

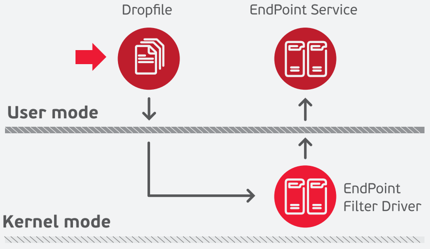
KEY FEATURES

Comprehensive and proactive malware protection

There is a mechanism that allows the agent component to actively monitor in kernel mode, capture events when malwares enter and destroy automatically and immediately.

Behavior Monitoring by Filter Driver

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

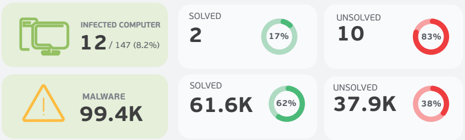


Centralized Analysis

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

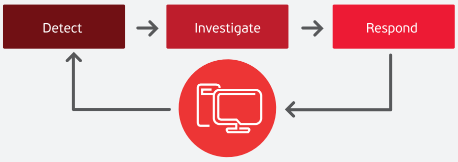
Real-time reporting

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



Fast 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.

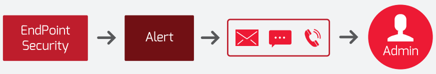


Multi-platform support

This solution is available in following platforms: 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.

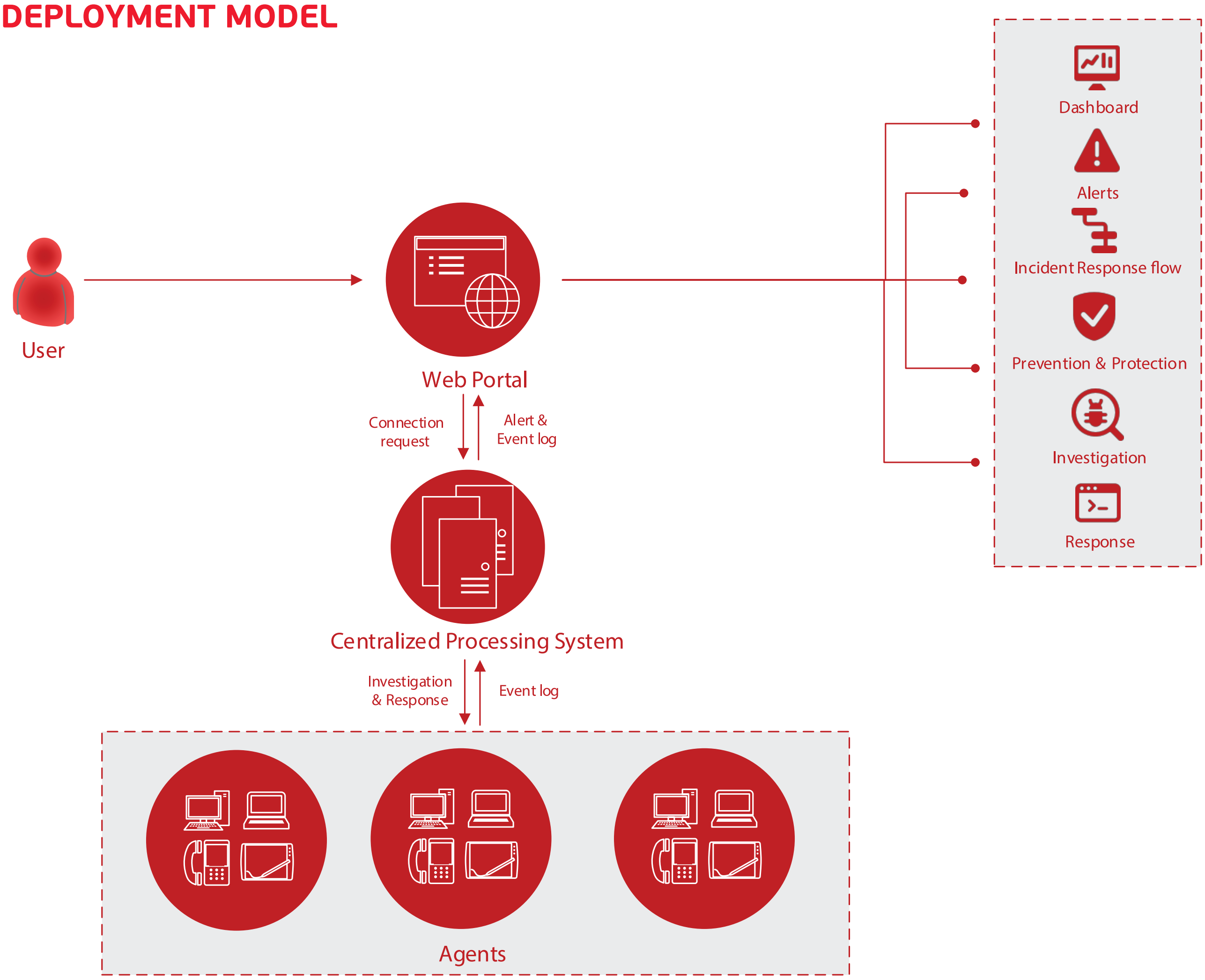
Smooth Operation

The design is lightweight and the system is completely transparent.

Integration with Third-party Solutions

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

DEPLOYMENT MODEL



VCS-aJiant system includes 03 main components:

Agents

A component installed on each computer, responsible for monitoring abnormal sigs on the computer and sending logs to a centralized server.

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				
Rule Correlation	*Manage alert rulesets*	✓		✓
Agent Management	*Manage workstation information, support remotely agent uninstallation*	✓	✓	✓
Group Management	*Group and classify workstations by defined groups*	✓	✓	✓
Account Management	*Support to create user accounts, authorization by roles*	✓	✓	✓
2. Incident prevention feature				
Anti-malware	*Detect, prevent and destroy malware, support to report the malware removal status from users' computers*		✓	✓
Application Control	*Set to block malicious applications from operating on workstations*	✓		✓
Endpoint Firewall	*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*	✓		✓
Alert 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*	✓		✓
Event 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*	✓		✓