

“A solution to quickly and proactively detect and deal with cyber-attack threats, 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. 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.

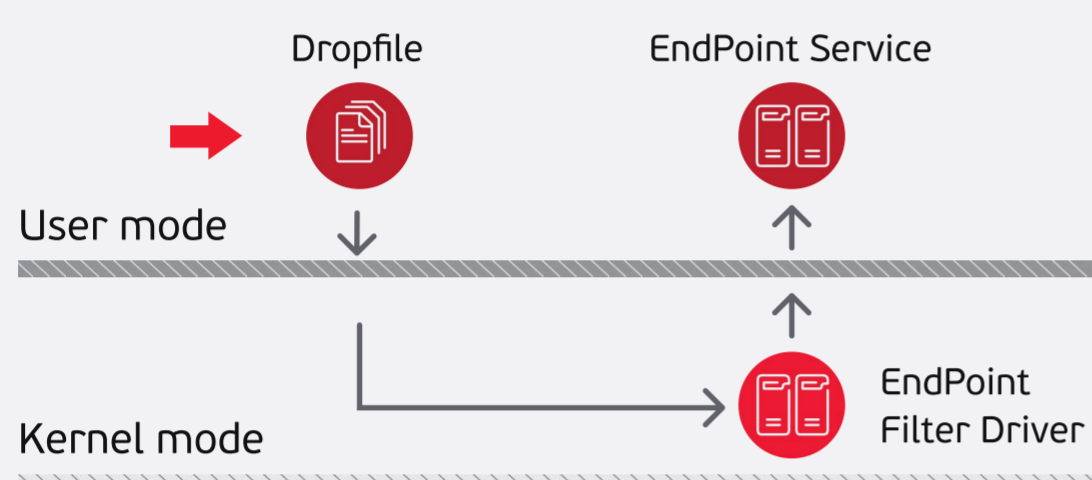
HIGHLIGHT VALUES

- Monitoring for abnormal behavior according to MITRE 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

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 server 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.

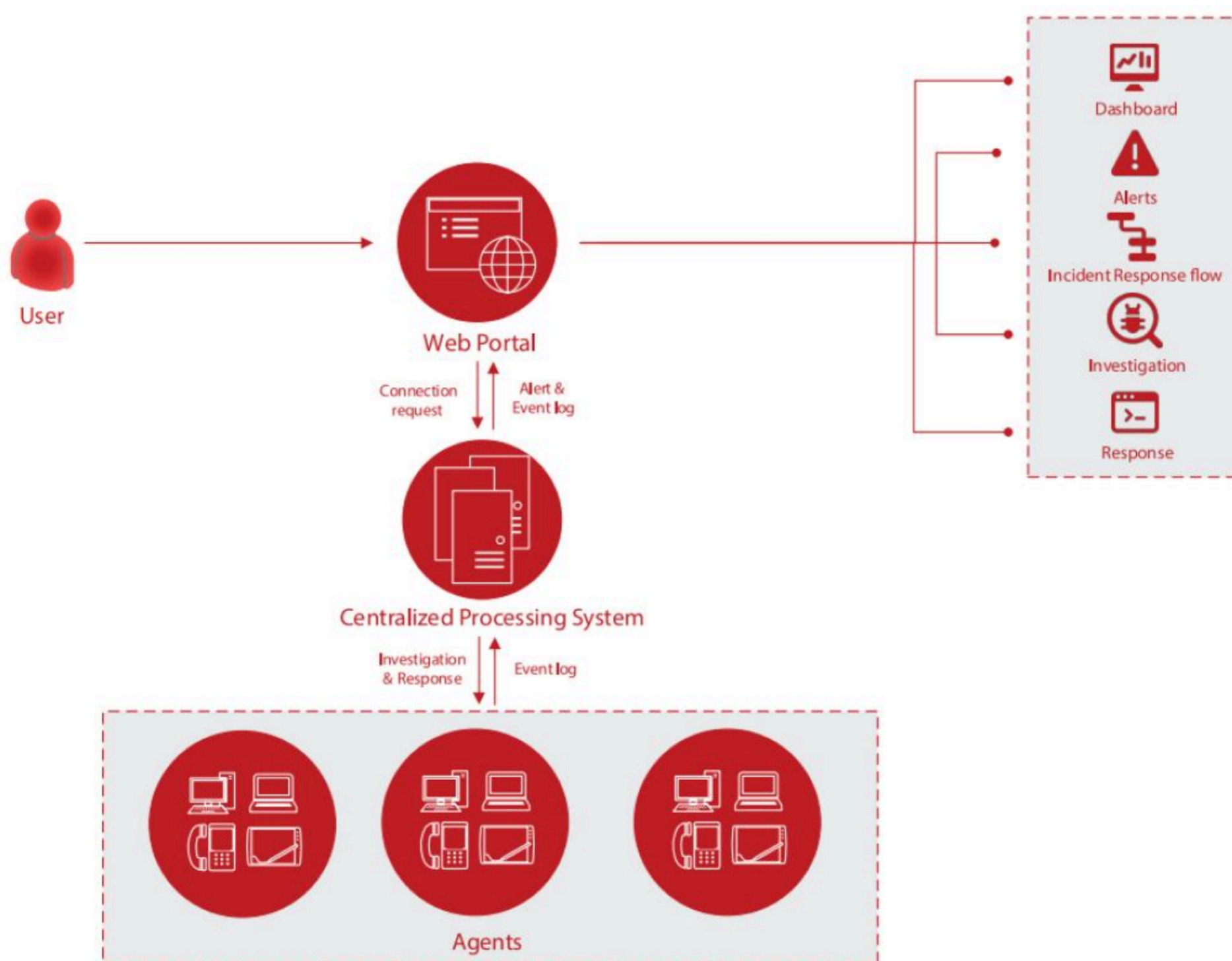
Cross-platform Solutions Support and Integration

Integrate with Threat Intelligence, SIEM, SOAR. Support multi OS platform: Windows, Linux, MacOS.

Viettel Cyber Security

For more information go to > www.viettelcybersecurity.com

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.

Viettel Cyber Security

For more information go to > www.viettelcybersecurity.com