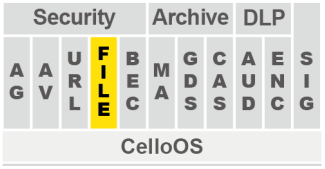
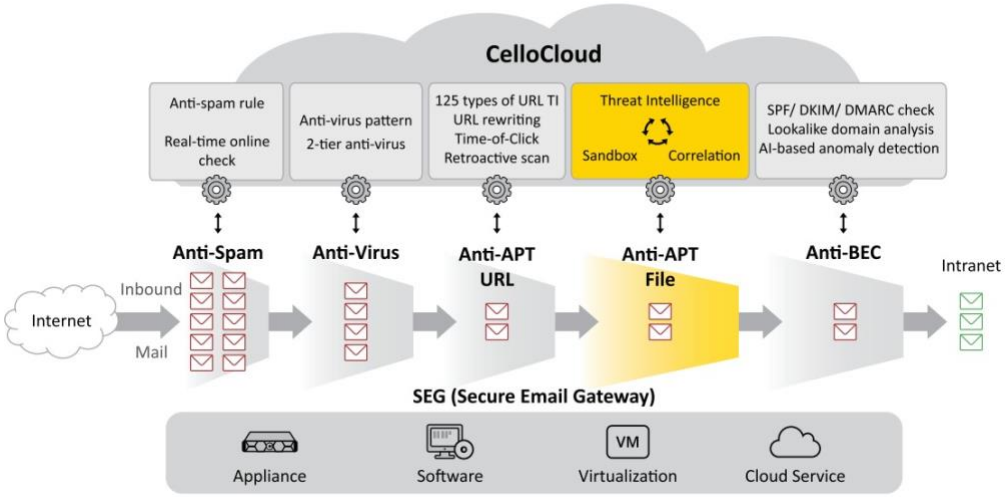
Inbound Email Protection

Anti-APT-File

In response to the increasing advanced malware infiltrating organizations, government agencies, educational institutions, enterprises, and financial institutions via email attachments, Cellopoint has introduced a new Advanced Persistent Threat (APT) defense solution. This solution provides in-depth detection and scanning of email attachments, helping your organization enhance email security management and improve the email security.





How Anti APT-File Works

For unknown attachment threats, Anti-APT-File protection combines the following methods to ensure effective detection:

Real-time Threat Intelligence updates

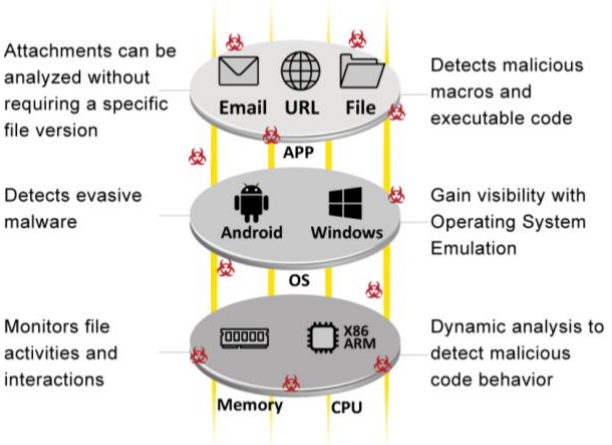
Utilizes up-to-date whitelist and blacklist from the Threat Intelligence (TI) to swiftly compare and detect the latest known threats.

Static code analysis

Analyzes the source code of attachments and compares it with known malware to identify similarities.

Dynamic sandbox scanning

Suspicious attachments are securely encrypted and sent to CelloCloud's sandbox for software execution and monitoring.



Features

- Full system emulation
- Correlation and threat scoring
- Risk assessment
- Cloud-based dynamic analysis
- Real-time threat intelligence updates
- Zero-day malware detection

Benefits

- Detects unknown malware
- Filters malicious software
- Stops APT attacks
- Intercepts ransomware
- Enhances cybersecurity
- Reduces the risk of cyberattacks

Full-system emulation

Within the sandbox, simulates and executes entire computer systems, including Windows, Android, Office documents, and PDF files, swiftly detecting and capturing latent malicious programs.

Anti-Evasion Technology

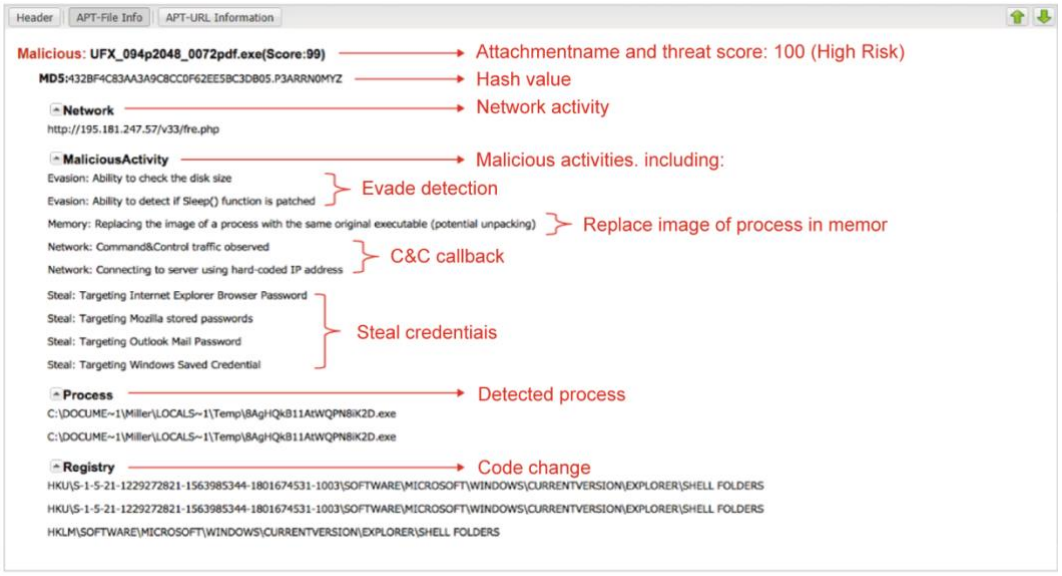
Unique sandboxing technique in the industry. Effectively monitors malicious behaviors without detection. As a result, it is capable of triggering and capturing hidden malicious programs in a short period of time.

Correlation and Threat Scoring

Conducts threat level analysis and provides feedback to the SEG for quarantine or release decisions.

Professional Forensic Summary Report

Includes threat scoring, the software's names and actions, network activities, process histories, and registry changes.



※Cloud-based sandbox is used by default and it automatically deletes files after scanned.
※For on-premises sandbox, please contact us at sales.tw@cellopoint.com to get a quote.

Supported Email Systems

- Microsoft Exchange 2016 / 2019 / 2022 / Microsoft 365 / Exchange Online
- HCL Note
- Google Workspace
- Sendmail, Qmail, Postfix
- Zimbra