CACTER-Email Security Gateway System

Product White Paper

Copyright statement

Disclaimer

This document only provides periodical information. Its content may be updated from time to time according to physical products without further notice. We will not assume any responsibility for direct or indirect loss resulting from improper use of this document.

Document updating

This document was finally revised by Coremail HongKong Company Limited in October 2022.

Company website

https://www.coremail.hk/

Sales hotline: 400-000-1631

Technical support hotline: 400-888-2488

Contents

1. Status of Email Security

Malicious emails cause extremely great harm, and their interception is critical for email security. Coremail Anti Spam Center (CAC) classifies malicious emails into three major categories as follows:

- **Infected emails:**

Viruses are mainly spread through malicious email attachments or download links in these attachments. New forms of infected emails evade detection by anti-spam and anti-virus systems with different techniques in combination with features of phishing and social work. Infection will cause serious security accidents such as data loss (malicious data deletion or encryption) and disclosure of important information once it occurs.

- **Phishing emails:**

Entice users to enter their account pins by themselves via a falsified page to steal their login information, thus endangering data security. This is a relatively common way for the black industry chain to acquire information on user accounts.

- **BEC:**

Attackers pass themselves as personnel of a social chain to deceive users to join groups and receive subsidies by social engineering techniques, to cheat users out of their money.

2. Profile of CACTER-Email Security Gateway System

2.1 Profile of CACTER Email Security Gateway System Products

CACTER-Email Security Gateway System fully detects and intercepts (blocks or isolates) malicious emails such as spam, phishing, infected and BEC emails based on the capacity of CAC - NERVE 1.0 for detecting malicious emails. The accuracy for filtering anti-spam emails is up to 99.8% and the misjudgment rate is below 0.02%.

2.2 Working Principle of CACTER-Email Security Gateway System

Internally, CACTER-Email Security Gateway System is integrated with multiple algorithms. It efficiently filters spam emails with a multilevel flexible deep protection and filtration system.

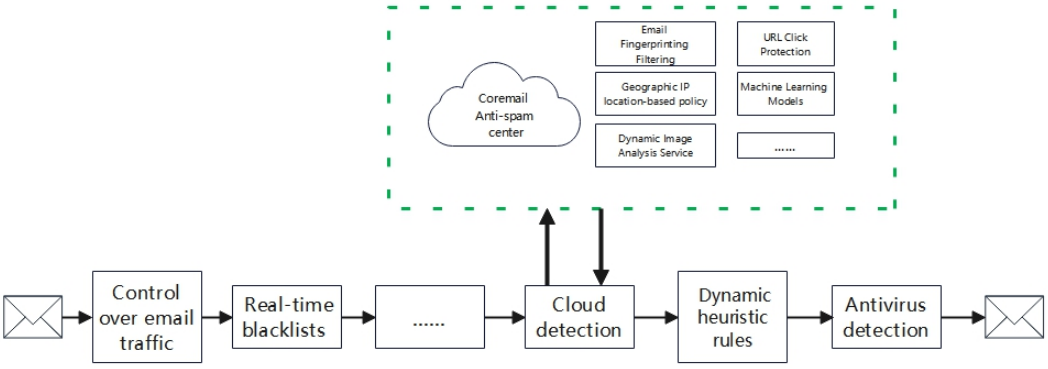


Fig. 2-1

2.3 Forms of CACTER-Email Security Gateway System Products

CACTER-Email Security Gateway System products exist in multiple forms to satisfy different customer requirements for deployment.

Product forms	Descriptions
Hardware gateway	Standard X86 industrial computer
Software gateway	Compatible with multiple kinds of network environment
Cloud gateway	Hosted cloud operation and maintenance

Table 2-1

3. Technical Strengths of CACTER-Email Security Gateway System

3.1 CAC - NERVE 1.0 (a Neural Network Platform)

CAC has embarked on email security since 2000. It has been always committed to developing anti-spam technologies from the earliest manual review of rules to today's deep machine learning technologies based on big data and artificial intelligence. Through over two decades of constant research and development efforts, CAC - NERVE 1.0 has emerged at the right time as a neural network platform and become China's biggest email security data center. It has approximately deployed ten thousand servers in different parts of the world and millions of spam traps all over China. Through 22 years of experience accumulation in operation and maintenance, it has possessed an enormous amount of samples of spam emails.

Dependent upon machine learning algorithms/models plus expert review rules, CAC - NERVE 1.0 can rapidly and accurately identify spam emails. It possesses incomparable strengths in anti-spam technologies based on big data. It can identify spam emails at a ratio of 99.8% and its misjudgment ratio is below 0.02%.

3.2 Anti-spam Hybrid Cloud Engine

CAC - NERVE 1.0, with a policy database for anti-spam hybrid cloud engines, can rapidly and accurately identify and intercept spam emails. Under clients' extreme conditions such as Internet disconnection, the gateways still maintain their capacity for protection against spam emails.

NERVE 1.0 also analyzes data of the latest spam emails on a non-stop basis to update the "big database of spam emails" and the "policy database for anti-spam cloud engines" in real time, to further guarantee the accuracy for intercepting spam emails.

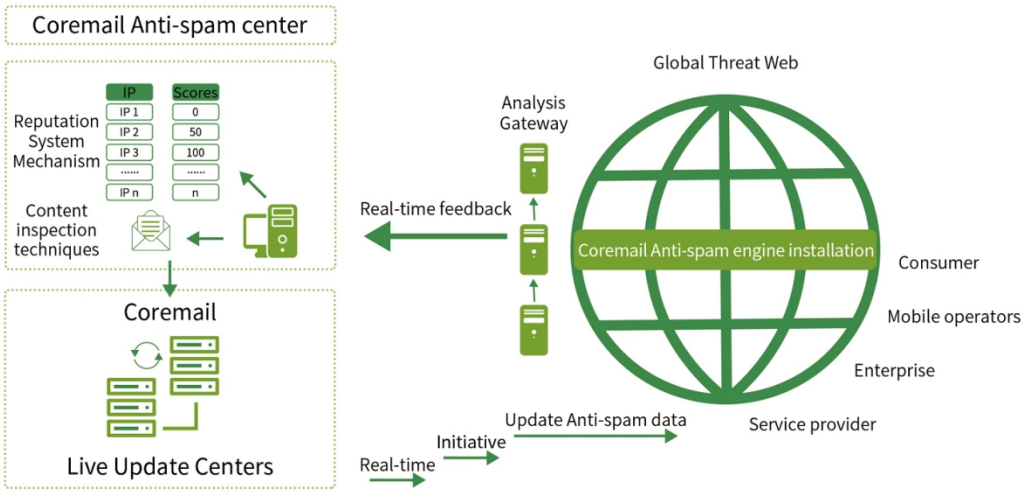


Fig. 3-1

3.3 Research and Development Strengths in Email Security - Technology Patents and Qualifications

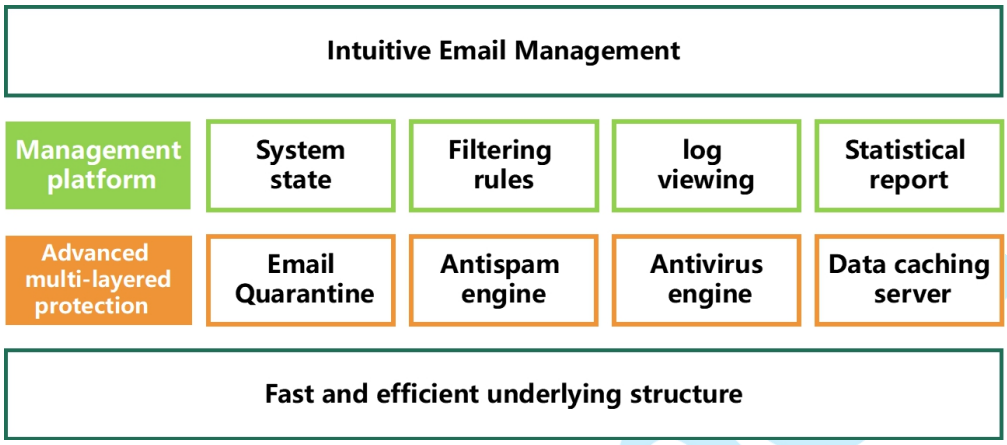
Fig. 3-2

CACTER-Email Security Gateway System, which has been deeply engaged in the email industry for a few years, owns multiple leading email processing/anti-spam technology patents:

- A method and system for identifying graphic spam emails
- An email transfer method and system
- An email withdrawal method and system
- A method for saving filtered email information, email server and email system
- A method for filtering spam emails
- A method and setting for filtering spam emails based on short texts
- An email classification method and device
- A method for generating senders' reputation value and filtering spam emails
- A script-based assisted business implementation method
- An email processing method and system
- A method and device for extracting numbers from emails
- A method, device, equipment and storage medium for detecting email login anomalies
- A method and system for detecting phishing emails based on feature extraction

4. Detailed Functional Descriptions of CACTER-Email Security Gateway System

4.1 Functional Architecture of CACTER-Email Security Gateway System



CACTER-Email Security Gateway System divides the whole system into multiple modules, including SMTP gateway, anti-spam engine, anti-virus engine, cache server and management platform, which run relatively independently, to improve system stability.

4.2 Introduction to Email Functions of CACTER-Email Security Gateway System

1. Protection of mainstream email systems

CACTER-Email Security Gateway System supports mainstream email systems, including Coremail, Exchange, O365, Gmail, IBM Domino and lotus notes.

2. Protection against spam emails

Dependent upon anti-spam capacity of NERVE 1.0 and in combination with the anti-spam hybrid engine, the Email Security Gateway System can perform multilevel filtration of spam emails, including inspection by SPF, domain name detection, IP filtration, sender filtration, recipient filtration, content feature detection technology and secondary link detection.

3. Protection against phishing emails

CACTER-Email Security Gateway System creatively proposes visual image analysis algorithms, to enhance the capacity for detecting phishing emails. It supports rapid judgment of known

malicious links through Coremail Safe Browing (CSB) - a cloud detection center, and performs secondary detection of unknown links.

4. Protection against infected emails

CACTER-Email Security Gateway System employs domestic and foreign top corporate anti-virus products - Qi'anxin and Kaspersky parallel antivirus engines. In combination with its independently developed technology for detecting maliciously executed documents, it accurately intercepts infected emails, thus effectively guaranteeing security of email systems.

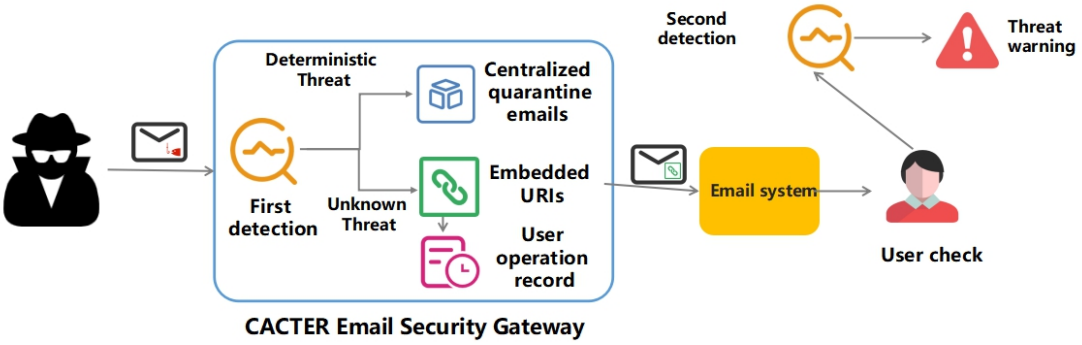
5. Protection against high-frequent email attacks

When an email server receives many emails over an extremely short period of time, it will cause an increase in network traffic, occupation of processor time and consumption of system resources. As a result, the email system will collapse. CACTER-Email Security Gateway System controls IP's emailing frequency within unit time and upper limit upon number of single connection commands, and supports detection by SPF, thus playing favorable roles in protecting against high-frequency email attacks.

6. Creation of filtration policies

CACTER-Email Security Gateway System supports administrators' creation of email filtration policies such as senders, domain names, IP, black and white lists apart from anti-spam hybrid cloud engines. It also supports independent creation of combined filtration policies.

7. Link protection



For initially detected unknown links, CACTER-Email Security Gateway System has launched a function for link protection as the second security detection threshold. Through this function, an administrator can rapidly track operations of users who have received phishing emails, including which users have visited phishing links and phishing links with the highest page view within a domain.

8. Accurate isolation of malicious emails

The malicious emails detected by CACTER-Email Security Gateway System will be precisely isolated in the quarantine, to prevent the email system from harm. Support the administrator's re-delivery and the users' self-service reception. In addition, the administrator is allowed to set the time for saving emails in the quarantine, and decide whether to enable or disable the notification function.

9. Statistical data analysis

CACTER-Email Security Gateway System can perform statistical analysis on email traffic in different period of time, including statistical analysis on filtration results, types of spam emails and IP connections. It can also intuitively present statistical statements. In addition, it supports log export from CACTER-Email Security Gateway System for the convenience of the administrator's individualized data analysis.

10. High service availability

When the email system malfunctions, CACTER-Email Security Gateway System will save emails and send emails again once the email system functions normally. This guarantees service continuity of the email system. Besides, it has a built-in local anti-spam engine. Under extreme conditions like Internet disconnection, the clients can automatically switch to the local anti-spam engine, in order that the gateway can maintain high availability of its anti-spam capability.

11. Post hoc analysis

CACTER-Email Security Gateway System retains all email security logs, distinguishes malicious email logs for the convenience of the administrator's post hoc analysis, and rapidly, accurately locates malicious threat emails. Besides, it tracks results and reasons of email delivery, to make it convenient for the administrator to swiftly identify status of email delivery.

12. Secondary authentication + credit granting terminal

CACTER-Email Security Gateway System supports secondary identity authentication of an administrator (including SMS and email authentication), to prevent others from others to pass themselves off as the administrator to log in to the administration platform. Otherwise, security of corporate critical systems will be threatened. Furthermore, it supports settings of the credit granting terminal, to reinforce security of the administrator's login.

13. Protection against group emails

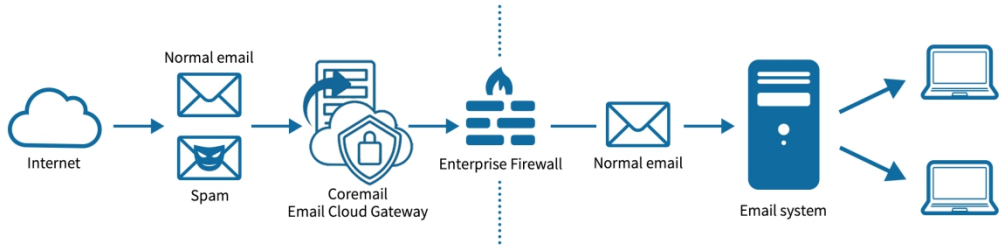
CACTER-Email Security Gateway System can "block, isolate, quarantine, review and discard" group emails to be received. It can decide whether to resend the emails in respect of different recipients.

5. Product Deployment and Services

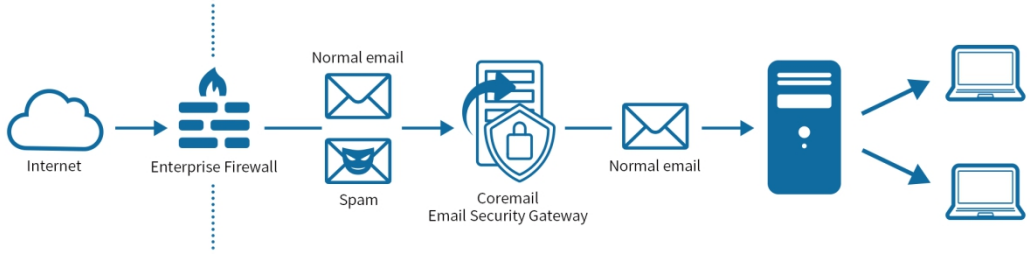
5.1 System Architecture

CACTER-Email Security Gateway System has the email gateway connected with the email server in series by replacing the Simple Mail Transfer Protocol monitored by the email service without changing the existing email system. Before entering the email system, all external emails shall undergo security inspection by the email gateway. Only normal emails passing such detection will be delivered to the email system. To send emails out from the email system, the emails have to be detected by the gateway in terms of security, to promptly intercept abnormal emails. In this way, spam and infected emails cannot be delivered into and out of the email system. The email gateway offers reliable guarantee to security of the email system.

• Coremail Email Security Gateway-Cloud Deployment •



• Coremail Email Security Gateway-Hardware/Software Deployment •



5.2 Cloud Detection Services of the Product

To guarantee timeliness and accuracy of its email detection capacity, the gateway has to make its cloud detection services accessible during its operation, in order that it can be updated on a real-time basis to detect the latest spam and malicious emails most completely.

5.3 Software Version Updating Services of the Product

During the service term of the product, the minor version up to the gateway standard can be updated for free. The administrator can contact the engineer to obtain an upgrade patch for self-service grade or engineer-assisted upgrade.

5.4 Access to Email Reporting Services

We encourage the administrator to report neglected samples of spam and malicious emails. The administrator can pack the email samples and send them to the reporting email (cac-team@coremail.cn) together. The reviewers of CAC will screen the reported emails and promptly update the features to the cloud rule base. Besides, regular return visits will be paid to clients, to ensure effective problem solving.

5.5 Manual Maintenance Services

Coremail makes two kinds of standard services available, including remote service support (for such remote service support, enterprises must provide Coremail with safe login approach and necessary environment) and field service support (value-added).

The enterprises can report problems with Coremail products through the service channels available from their service packages they've purchased.

Service channels and time:

Channel	Service entry	Service time
Hotline	400-888-2488	Business days (9:00-18:00)
Email	support@coremail.cn	Business days (9:00-21:00)
Online self-service	Administrator Community of the Coremail Cloud Service Center	7*24 h