Netcore

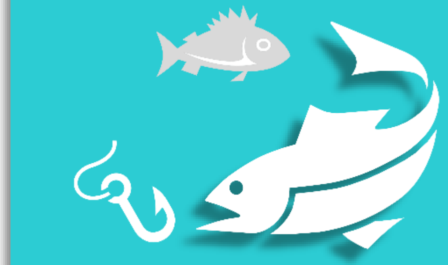
Netcore

The Future of Email Security with Netcore ATP

powered by Fortmail

About Netcore ATP

Email’s use as a primary threat vector…



36%↑

Percent of breaches involving phishing, up from 25% YoY.

15X↑

Increased use of “Misrepresentation” in Social Engineering-related incidents.

BEC

58%

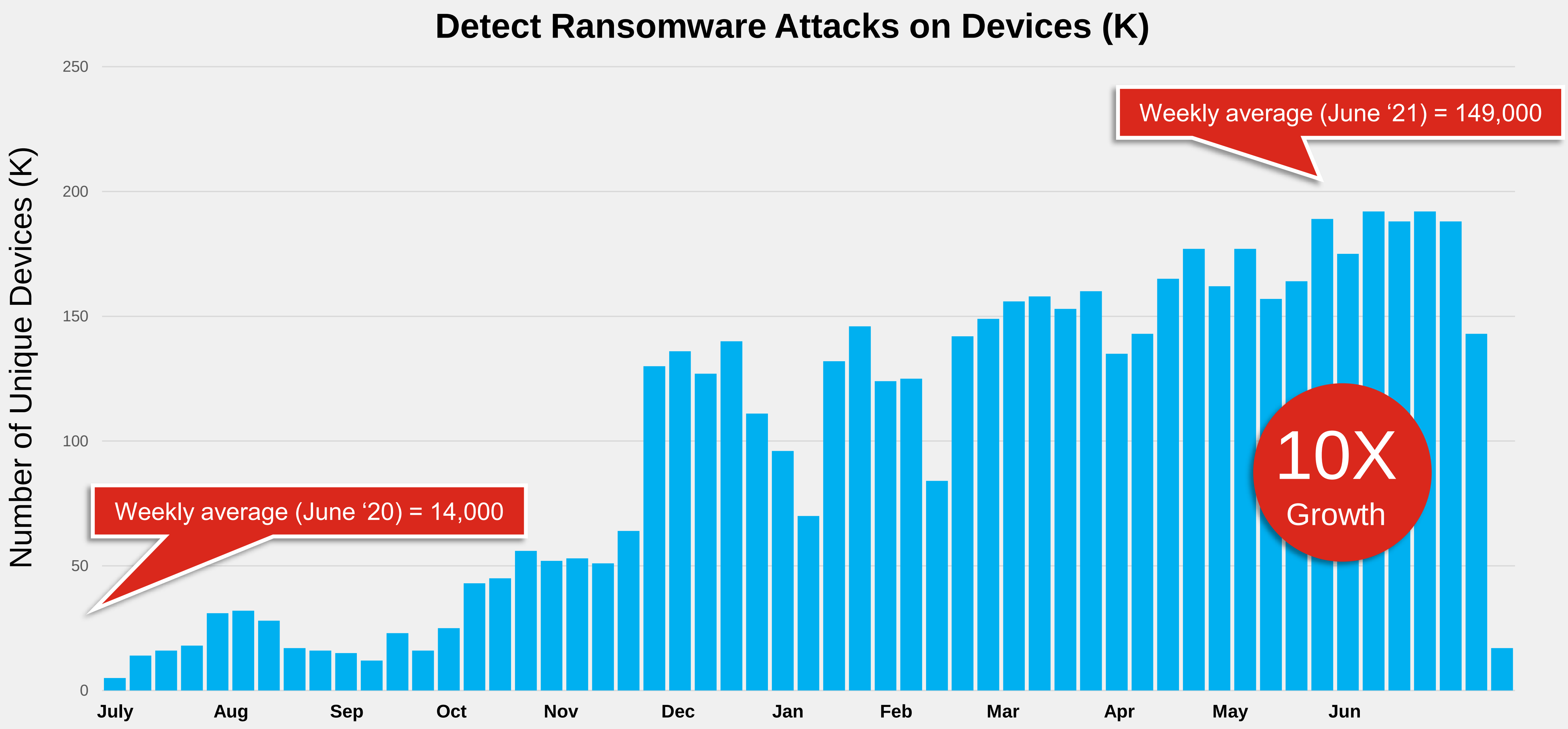
Percent of Business Email Compromise (BEC) attacks that resulted in loss of money.

10%↑

Percent of breaches involving ransomware, up from ~5% the prior year.*

Statistics from Verizon Data Breach Investigations Report 2021.

Ransomware intensity (FortiGuard Labs)



Weekly average (June ‘21) = 149,000

Weekly average (June ‘20) = 14,000

10X Growth

Source: Fortinet – July 2021

Introducing Netcore ATP

Advanced protection against the full spectrum of email-borne threats.

Cloud-based Email

Hybrid Email

- Comprehensive Protection
- Validated Performance
- Security Fabric Integration
- Powered by FortiGuard Labs
- Industry-Leading Cost to Performance

How We Are Different—Fabric-Enabled

Comprehensive Protection
Advanced integrated capabilities to protect against spam, malware, ransomware, impersonation, and Business Email Compromise attacks.

Validated Performance
Top-rated in independent testing to stop spam, malware, ransomware, and advanced email threats.

Security Fabric Integration
Integrated into the Fortinet Security Fabric to uncover the full attack lifecycle and share IoCs across your security infrastructure.

Industry-Leading Cost to Performance
Proven email threat protection at an industry-leading cost to performance.

Powered by FortiGuard Labs
World-class threat intelligence powers world-class efficacy.

Netcore ATP Use Cases

EMAIL SECURITY

Secure Inbound Emails

Stop spam, viruses/malware, ransomware, phishing, targeted attacks, business email compromise.

Mitigate #1 Threat Vector

*Prevent Outbound Threats

Protect PII, PHI, and other sensitive data from exfiltration or accidental disclosure. Address compliance.

Optimal Email Security Effectiveness

Enhance Cloud-based Controls

Bolster email security by addressing known gaps in the efficacy of cloud-based email services' native controls.

Optimal Email Security Effectiveness

Mitigate Email Outages

Minimize the impact to productivity and related cost when email services experience an outage.

Risk Mitigation and Cost Avoidance

Email Usage Insights

Quickly gain insights to understand security posture, drill-in via detailed logs.

Proactively Manage Email Use and Abuse

*Additional Charges

Comprehensive protection

SECURE INBOUND EMAILS

Phishing/Spear/Whale Phishing

Impersonation

Business Email Compromise

Advanced/Targeted Attacks

Email-based Ransomware Threats

Illicit/Adult Content

Spam

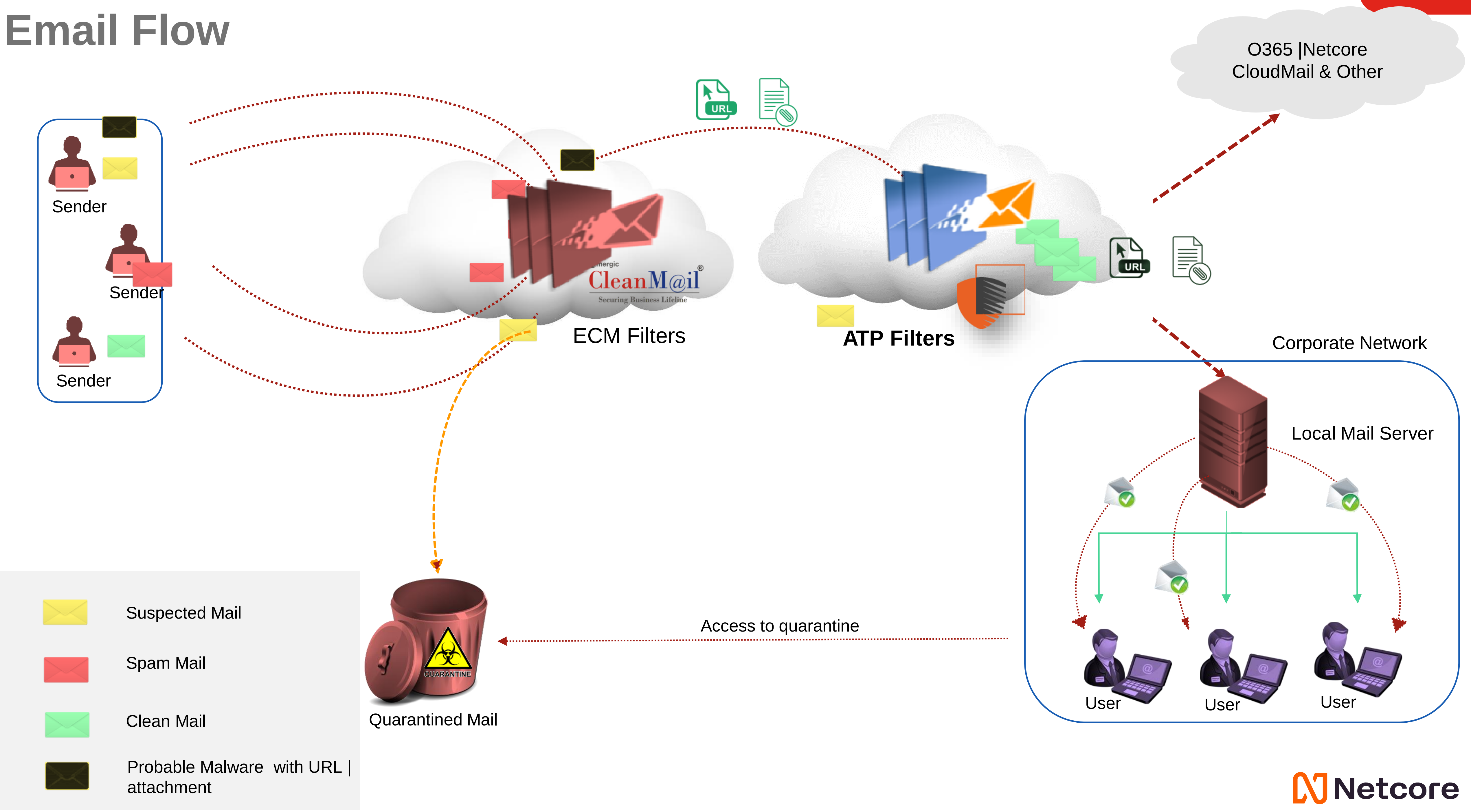
DETECT BUILDING BLOCKS

Malicious Content

Malicious Files

Malicious URLs

Email Flow



O365 |Netcore CloudMail & Other

Sender

Sender

Sender

ECM Filters

ATP Filters

Corporate Network

Local Mail Server

User

User

User

Access to quarantine

Quarantined Mail

🟨 Suspected Mail

🟥 Spam Mail

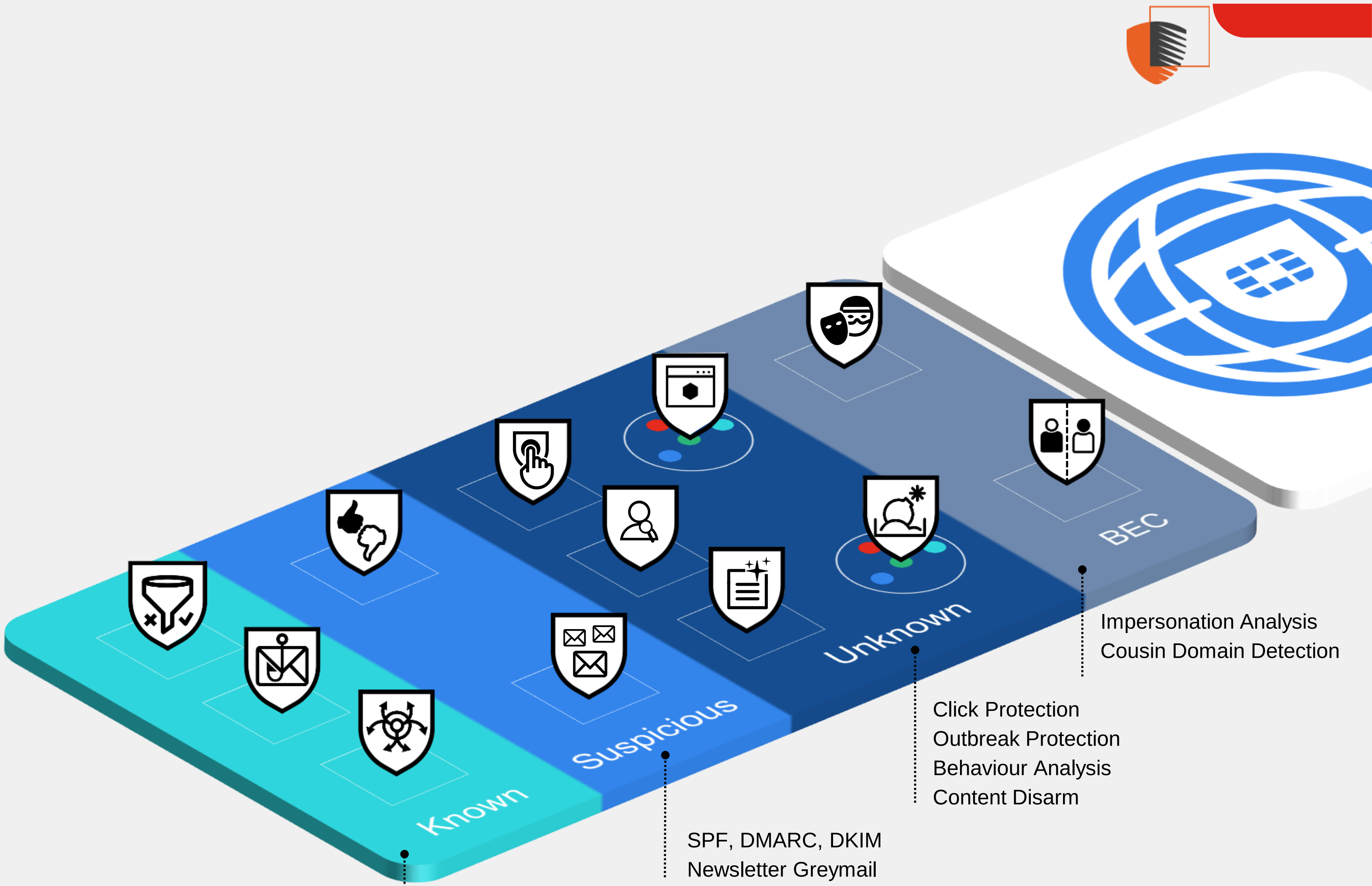
🟩 Clean Mail

⬛ Probable Malware with URL | attachment

Netcore ATP

Advanced multi-layer security against:

- Known threats
- Suspected threats
- Unknown threats/Zero-days
- Impersonation attempts
- Business Email Compromise



Impersonation Analysis
Cousin Domain Detection

Click Protection
Outbreak Protection
Behaviour Analysis
Content Disarm

SPF, DMARC, DKIM
Newsletter Greymail

FortiGuard URL Filtering
FortiGuard Anti-Spam
FortiGuard Antivirus

Netcore ATP

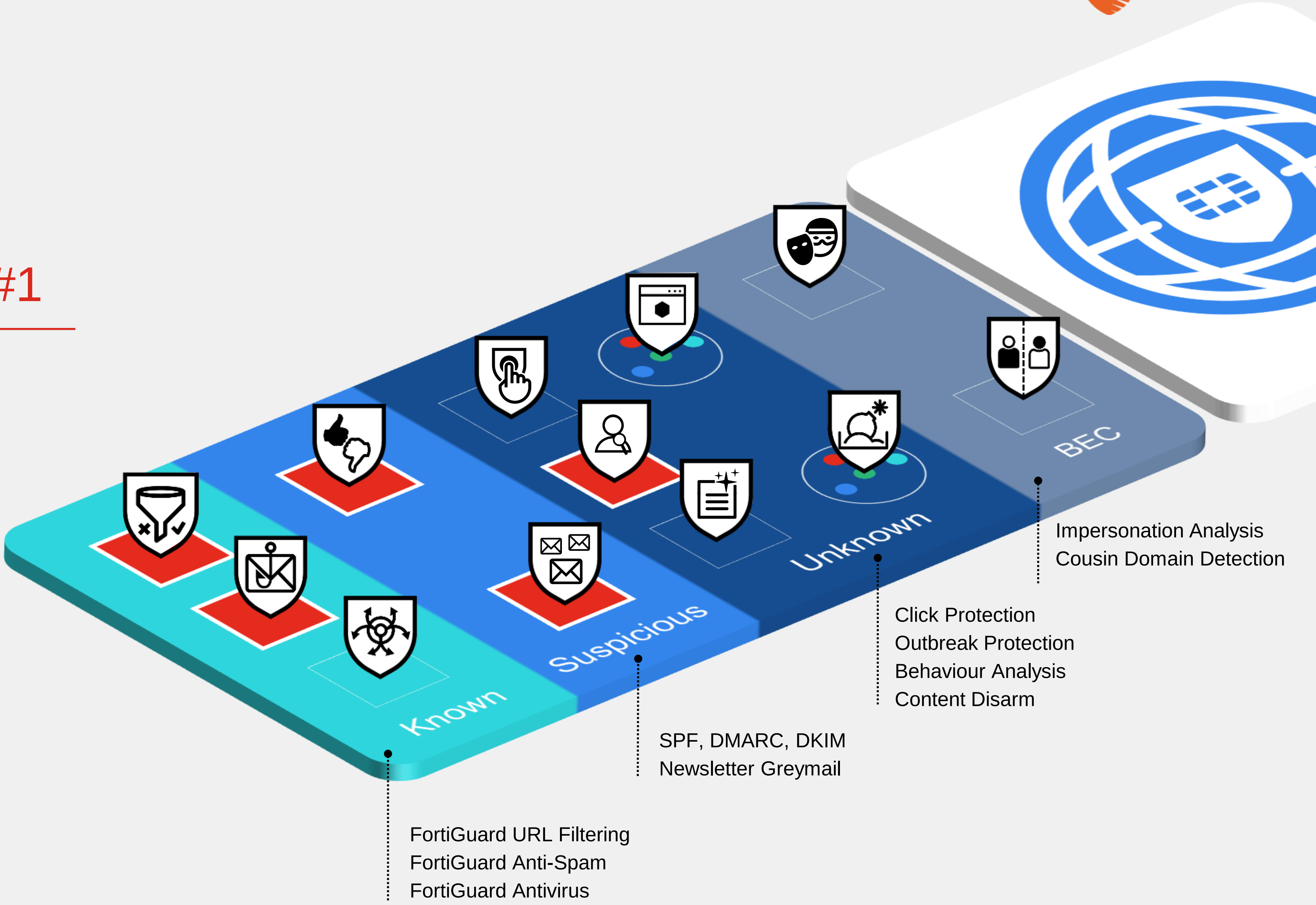
THREAT MITIGATION #1

Content-based Email Threat Defense

- Spam, phishing & greymail

Solution:

Deal with the volumetric spam problem quickly and efficiently.



Impersonation Analysis
Cousin Domain Detection

Click Protection
Outbreak Protection
Behaviour Analysis
Content Disarm

SPF, DMARC, DKIM
Newsletter Greymail

FortiGuard URL Filtering
FortiGuard Anti-Spam
FortiGuard Antivirus

Netcore ATP

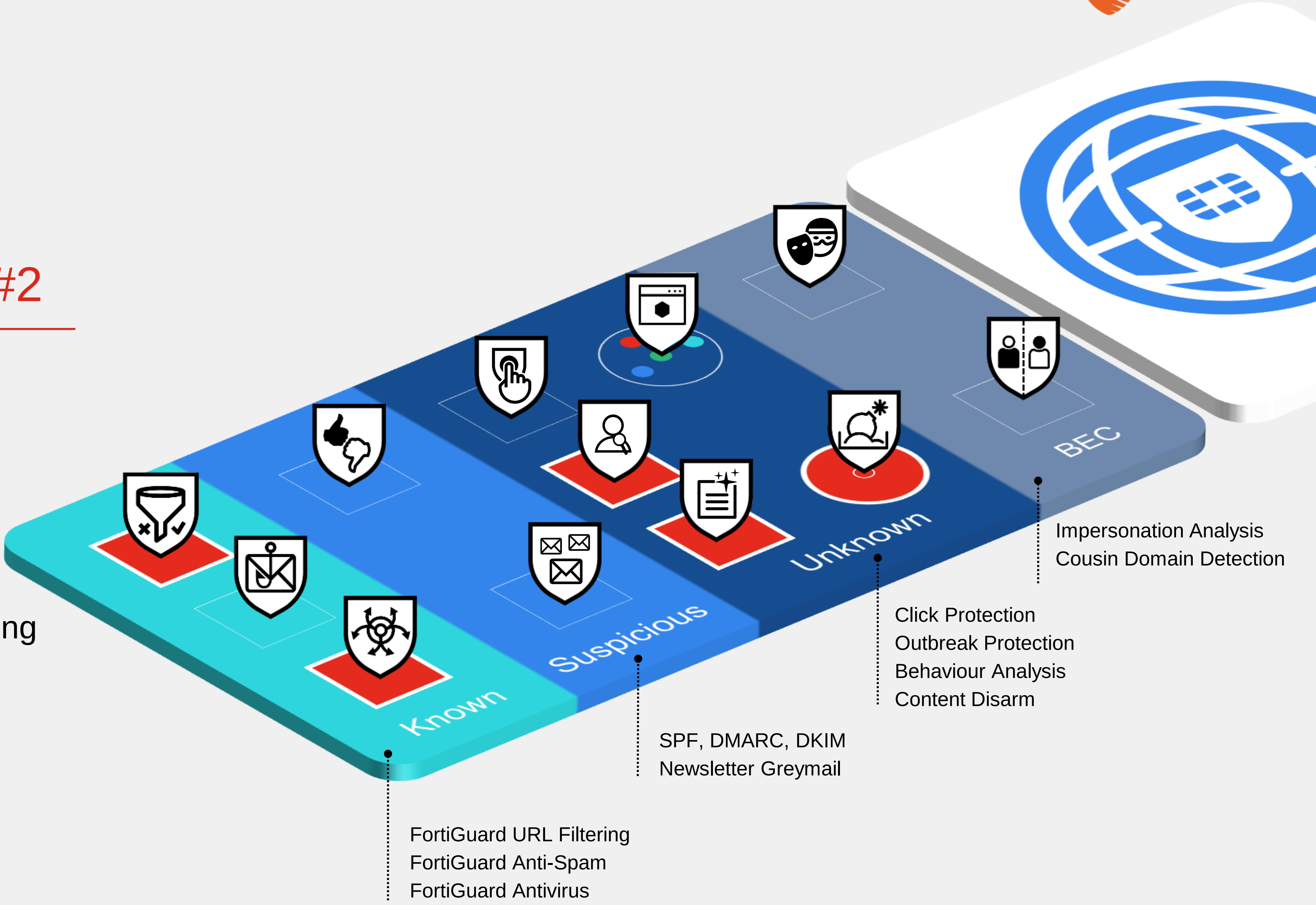
THREAT MITIGATION #2

Attachment-based Email Threat Defense

- Malware & Phishing

Solution:

Advanced capabilities like sandboxing analyze suspicious attachments.



FortiGuard URL Filtering
FortiGuard Anti-Spam
FortiGuard Antivirus

SPF, DMARC, DKIM
Newsletter Greymail

Click Protection
Outbreak Protection
Behaviour Analysis
Content Disarm

Impersonation Analysis
Cousin Domain Detection

Netcore

Netcore ATP

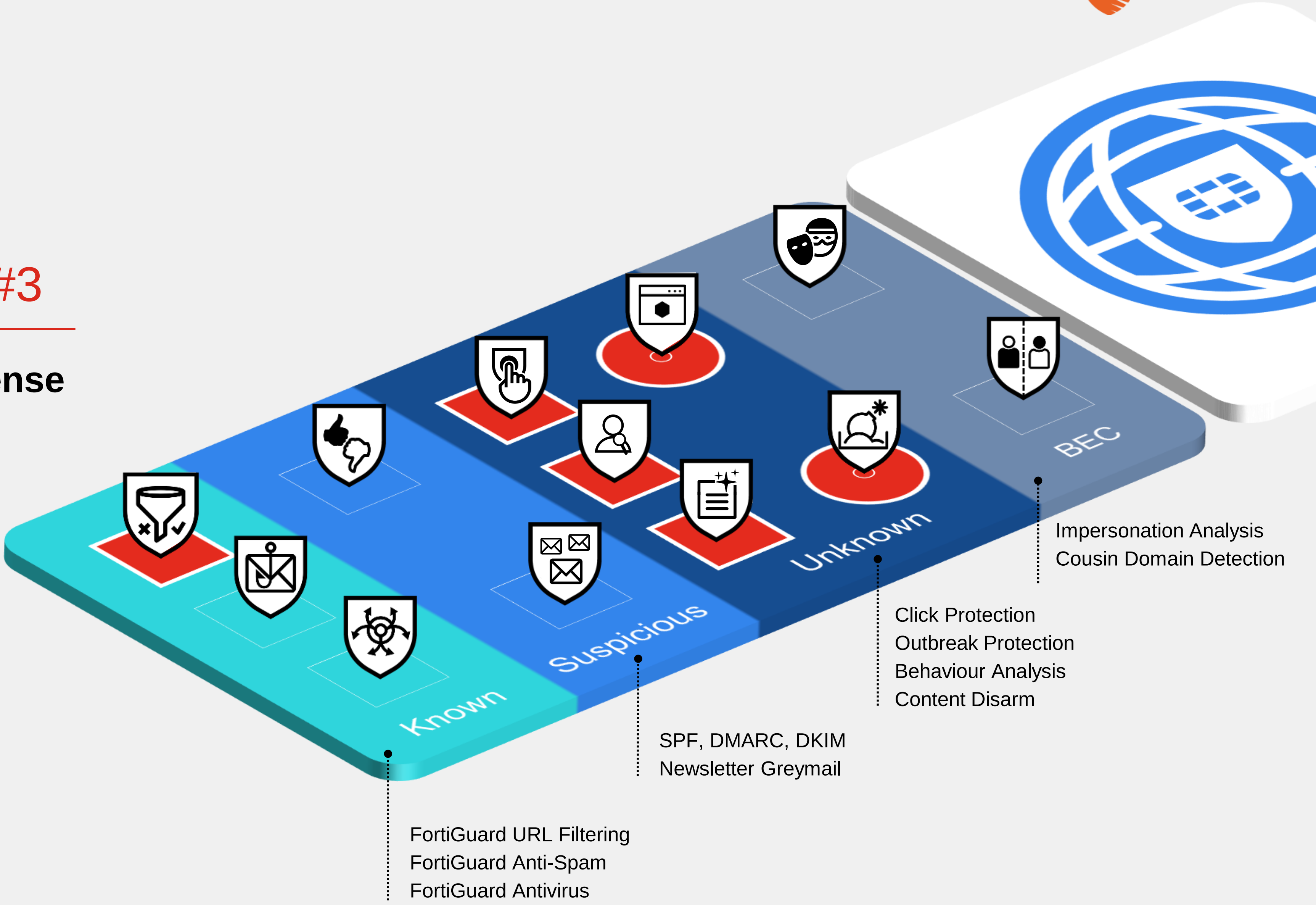
THREAT MITIGATION #3

URL-based Email Threat Defense

- Malsites & phishing
- Leveraging Web as an infection vector

Solution:

Tight security fabric integration to secure URLs while enabling business operations.



Impersonation Analysis
Cousin Domain Detection

Click Protection
Outbreak Protection
Behaviour Analysis
Content Disarm

SPF, DMARC, DKIM
Newsletter Greymail

FortiGuard URL Filtering
FortiGuard Anti-Spam
FortiGuard Antivirus

Netcore ATP

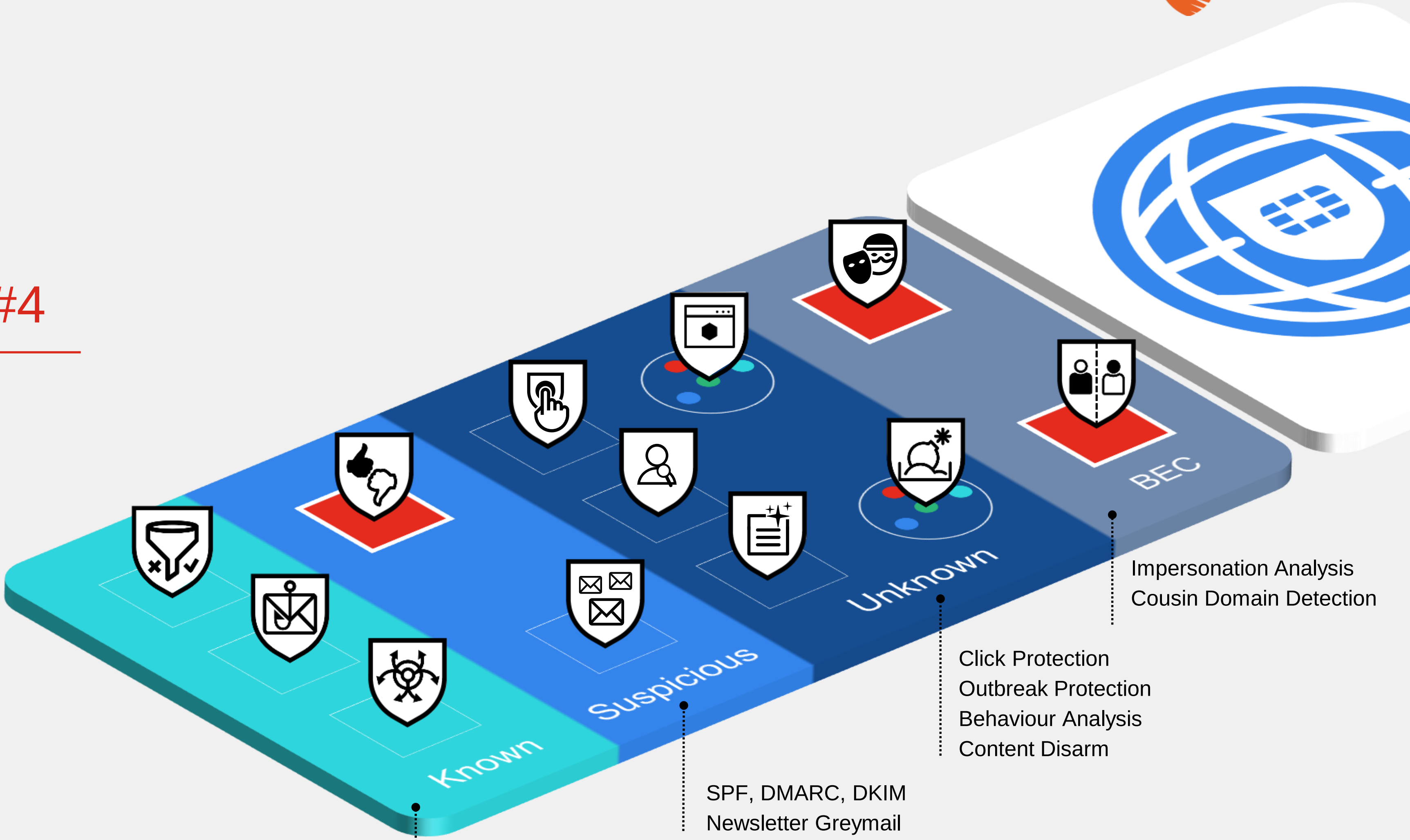
THREAT MITIGATION #4

Business Email Compromise Prevention

- Whaling & spear-phishing
- Targeted attacks

Solution:

Advanced methods to detect targeted BEC attacks.



Impersonation Analysis
Cousin Domain Detection

Click Protection
Outbreak Protection
Behaviour Analysis
Content Disarm

SPF, DMARC, DKIM
Newsletter Greymail

FortiGuard URL Filtering
FortiGuard Anti-Spam
FortiGuard Antivirus

FortiGuard Labs Statistics (Q4 2020)

15M
BOTNET C&C ATTEMPTS
Thwarted Per Minute

47M
SPAM
Blocked Per Day

462K
MALICIOUS WEBSITE ACCESSES
Blocked Per Minute

906
ZERO DAY
Threats Discovered

5.3M
NETWORK INTRUSION ATTEMPTS
Resisted per minute

136K
PHISHING
Blocked Per Minute

1.2 PB
OF THREAT SAMPLES

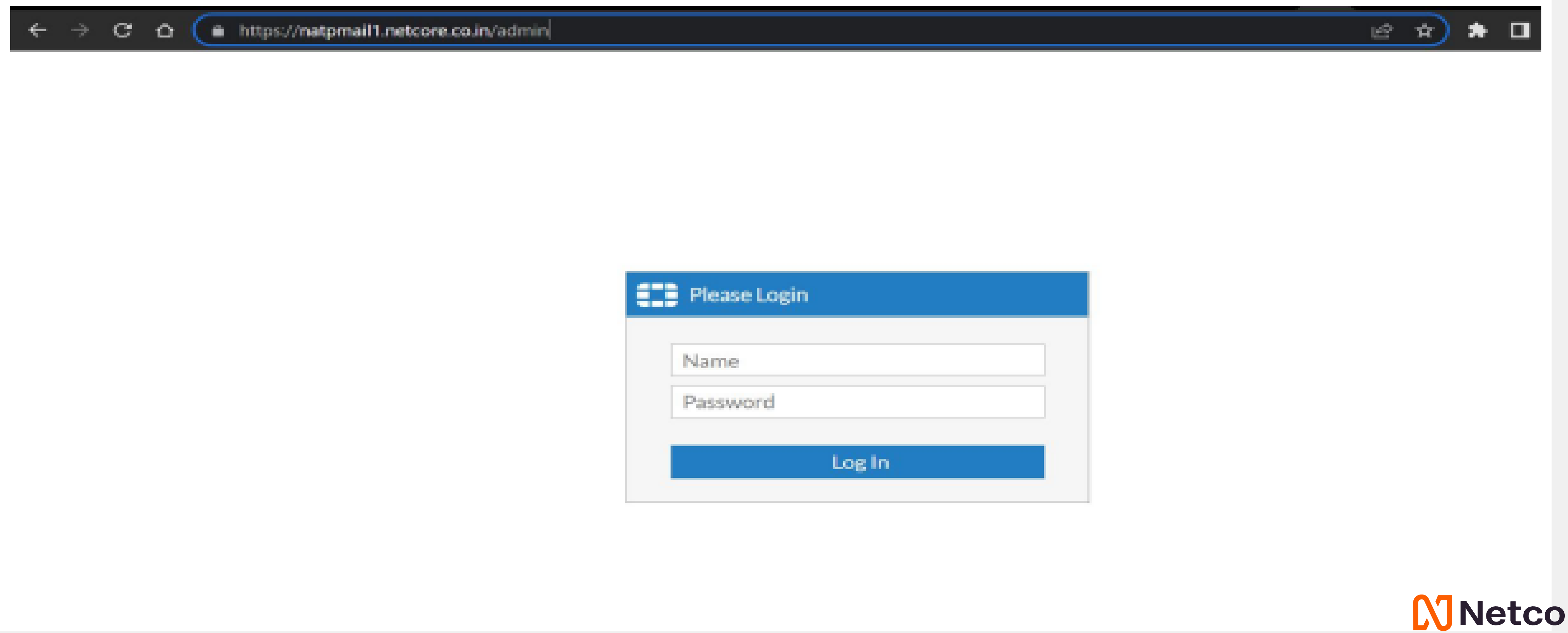
609K
HOURS
of Threat Research Globally Per Week

904K
MALWARE PROGRAMS
Neutralized Per Minute

Netcore ATP Admin Panel

Admin Login

Login with “https://Domainfqdn/admin” using your local or AD credentials



https://natpmail1.netcore.co.in/admin

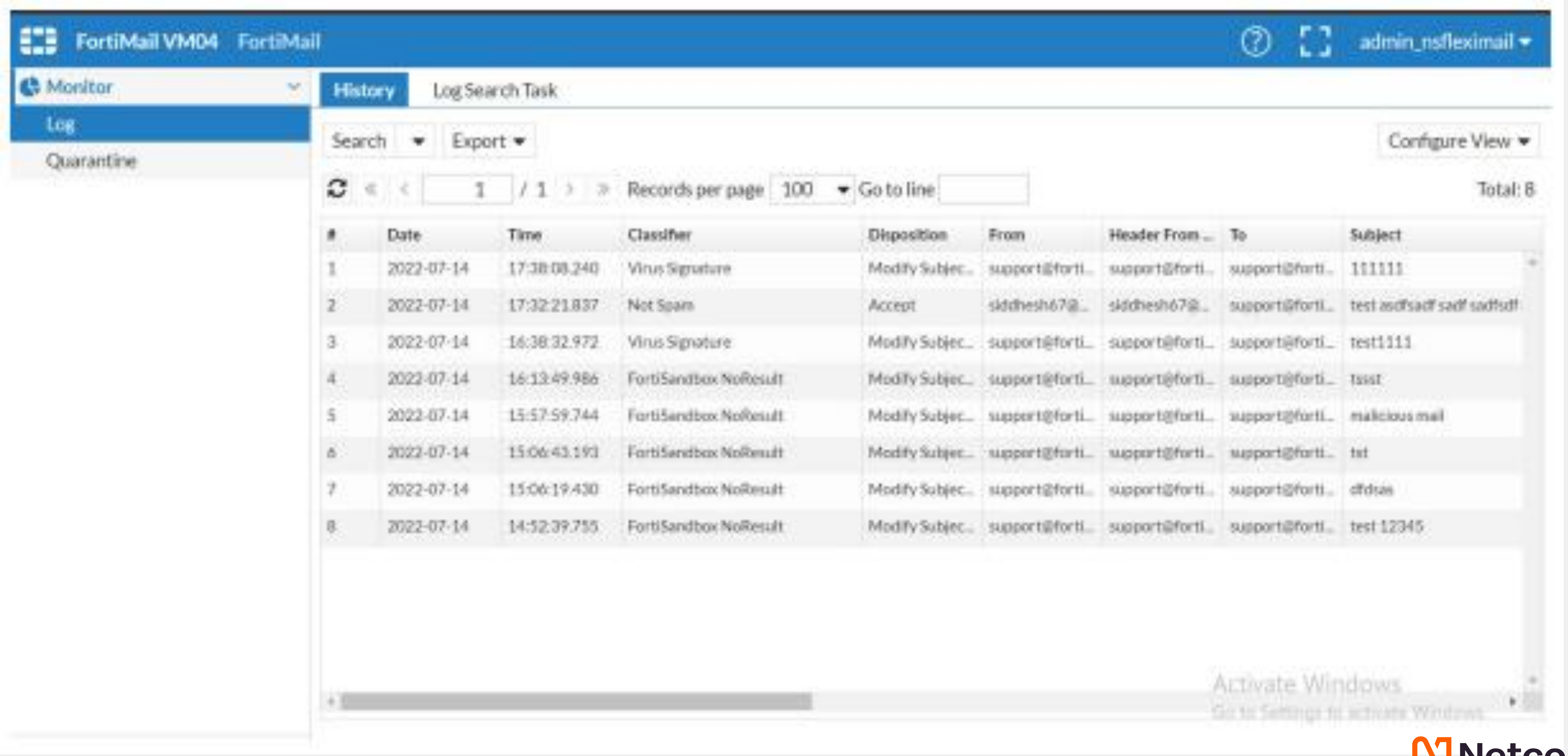
Please Login

Name

Password

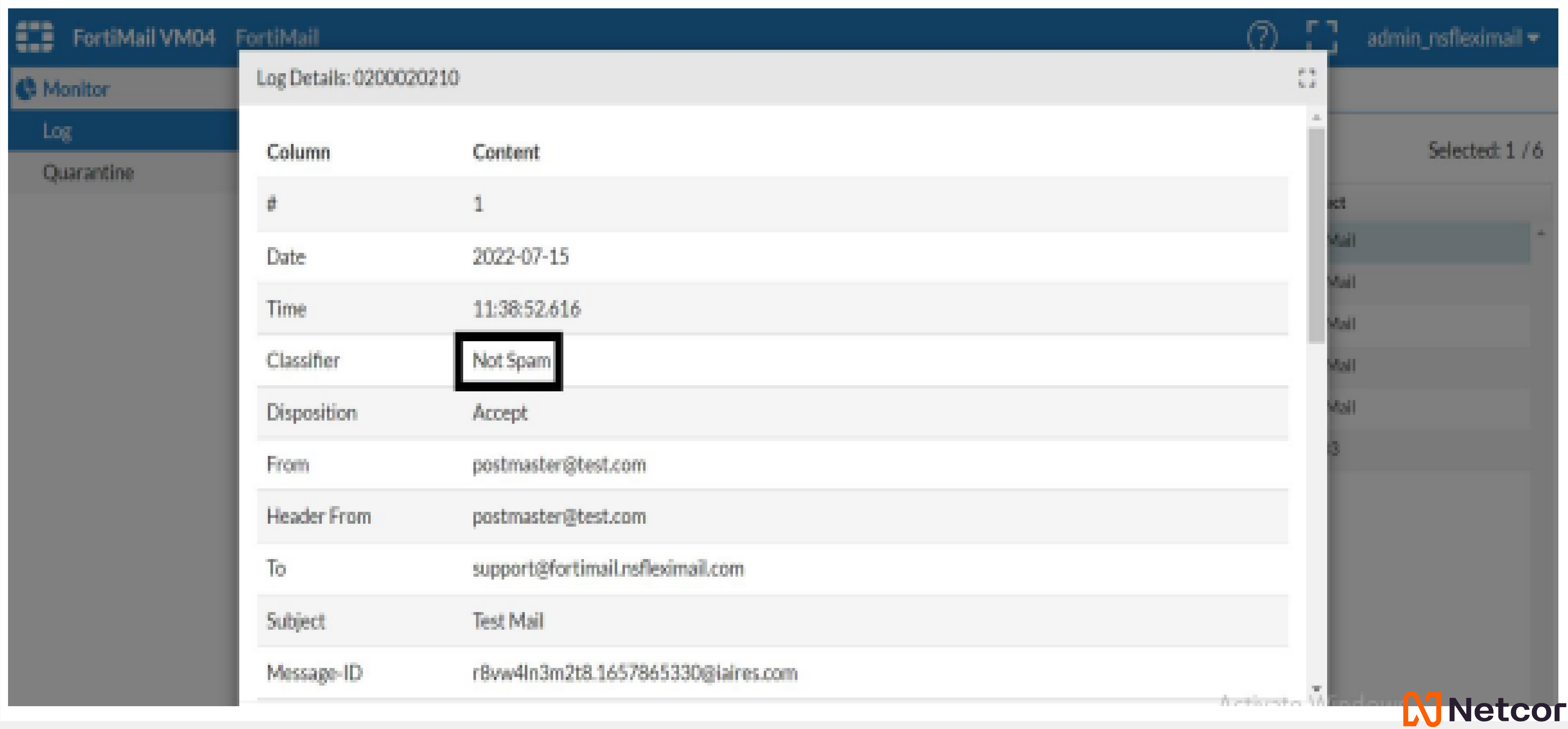
Log In

- Once login you will get to see the option to view the logs you can check a user log and status of the mail under the log history section as shown in the below snapshot



#	Date	Time	Classifier	Disposition	From	Header From ...	To	Subject
1	2022-07-14	17:38:08.240	Virus Signature	Modify Subjec...	support@forti...	support@forti...	support@forti...	111111
2	2022-07-14	17:32:21.837	Not Spam	Accept	siddhesh67@...	siddhesh67@...	support@forti...	test asdfsadf sadf sadfsdf
3	2022-07-14	16:38:32.972	Virus Signature	Modify Subjec...	support@forti...	support@forti...	support@forti...	test1111
4	2022-07-14	16:13:49.986	FortiSandbox NoResult	Modify Subjec...	support@forti...	support@forti...	support@forti...	tsst
5	2022-07-14	15:57:59.744	FortiSandbox NoResult	Modify Subjec...	support@forti...	support@forti...	support@forti...	malicious mail
6	2022-07-14	15:06:43.193	FortiSandbox NoResult	Modify Subjec...	support@forti...	support@forti...	support@forti...	tst
7	2022-07-14	15:06:19.430	FortiSandbox NoResult	Modify Subjec...	support@forti...	support@forti...	support@forti...	dfdsas
8	2022-07-14	14:52:39.755	FortiSandbox NoResult	Modify Subjec...	support@forti...	support@forti...	support@forti...	test 12345

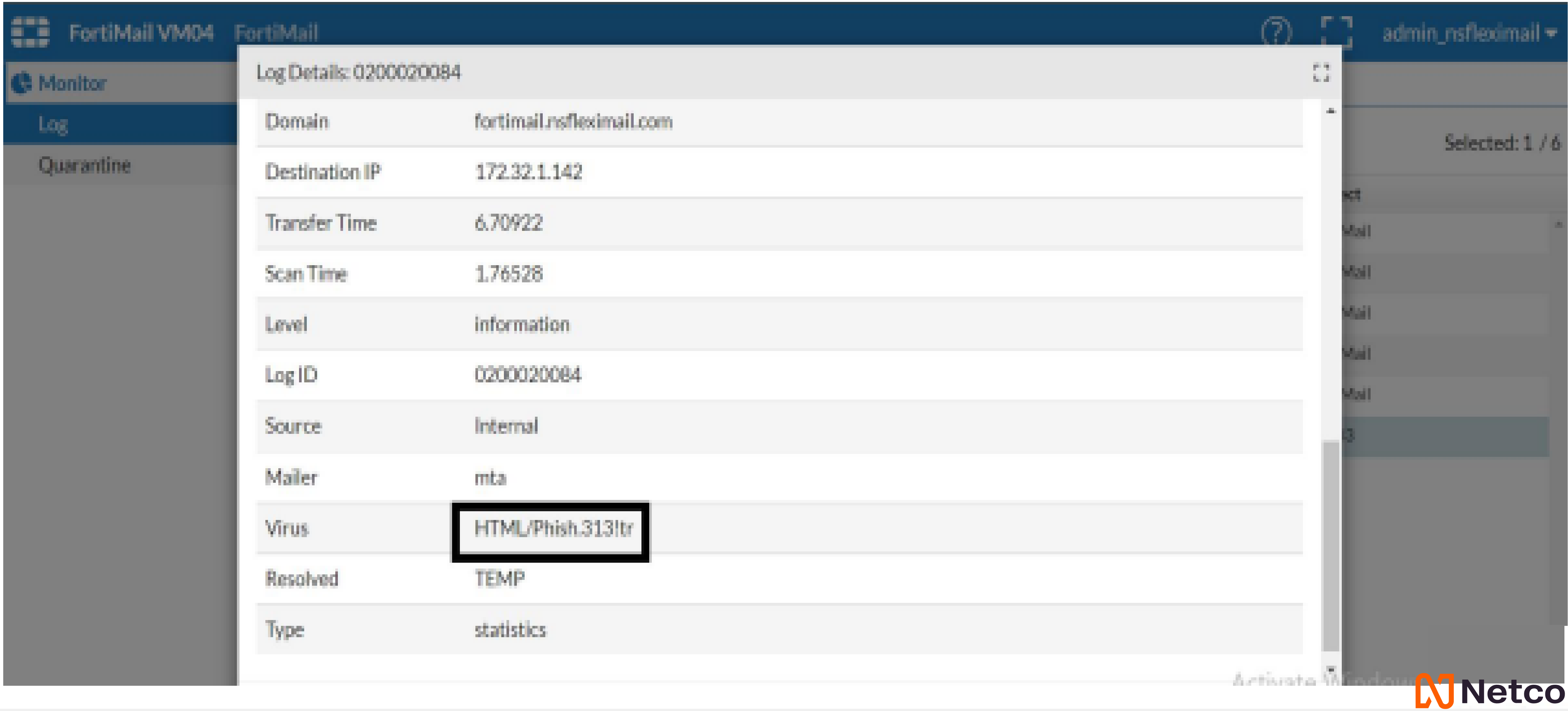
Admin can check the logs whether it’s a genuine or a malicious/phishing mail by clicking on the relevant logs for an email. in the below snapshot you can get the detail of a genuine mail in which the classifier shows the status as not spam detail which means the mail is genuine and not a spam mail.



Log Details: 0200020210

Column	Content
#	1
Date	2022-07-15
Time	11:38:52.616
Classifier	Not Spam
Disposition	Accept
From	postmaster@test.com
Header From	postmaster@test.com
To	support@fortimail.nsfleximail.com
Subject	Test Mail
Message-ID	r8vw4ln3m2t8.1657865330@laires.com

Admin can check for a mail weather it’s a malicious mail by simply clicking on the log you will get the classifier status as virus and at the bottom of the logs you will get the type of spam mail as shown in the below snapshot.



Log Details: 0200020084

Domain	fortimail.nsfleximail.com
Destination IP	172.32.1.142
Transfer Time	6.70922
Scan Time	1.76528
Level	information
Log ID	0200020084
Source	Internal
Mailer	mta
Virus	HTML/Phish.313!tr
Resolved	TEMP
Type	statistics

Quarantine Mail

You can quarantine email messages based on the message content, such as whether the email is spam or contains a prohibited word or phrase. FortiMail units have two types of quarantine:

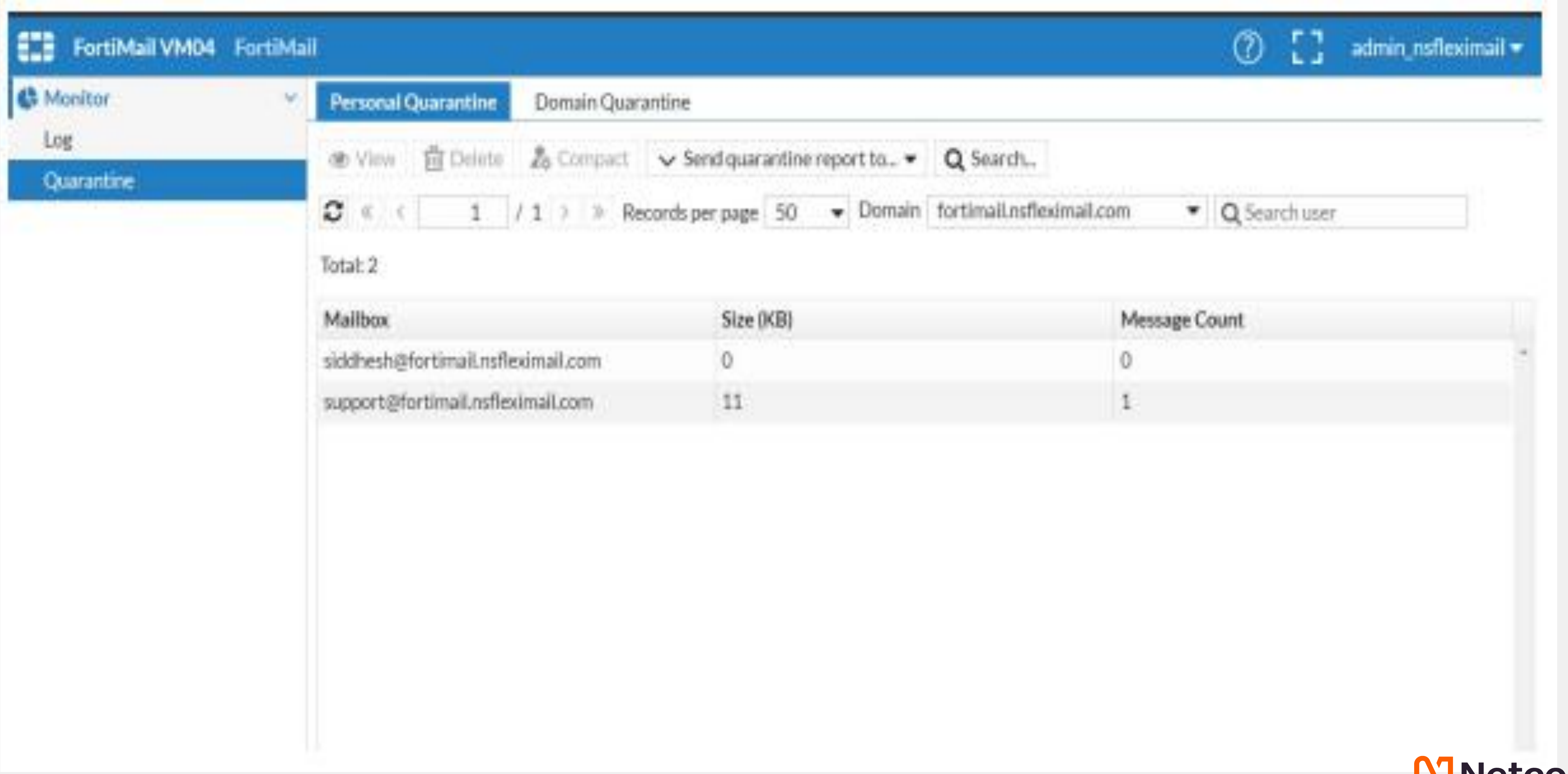
Personal Quarantine

Quarantines email messages into separate folders for each recipient address in each protected domain. The FortiMail unit periodically sends quarantine reports to notify recipients, their designated group owner, and/or another email address of the email messages that were added to the quarantine folder for that recipient.

Domain Quarantine

Quarantines email messages into separate folders for each protected domain, in the case of a multi-tenant environment. Unlike the per-recipient quarantine, the FortiMail unit does not send a quarantine report. The FortiMail administrator, assigned to their respective domain, should review the quarantined email messages to decide if they should be released or deleted.

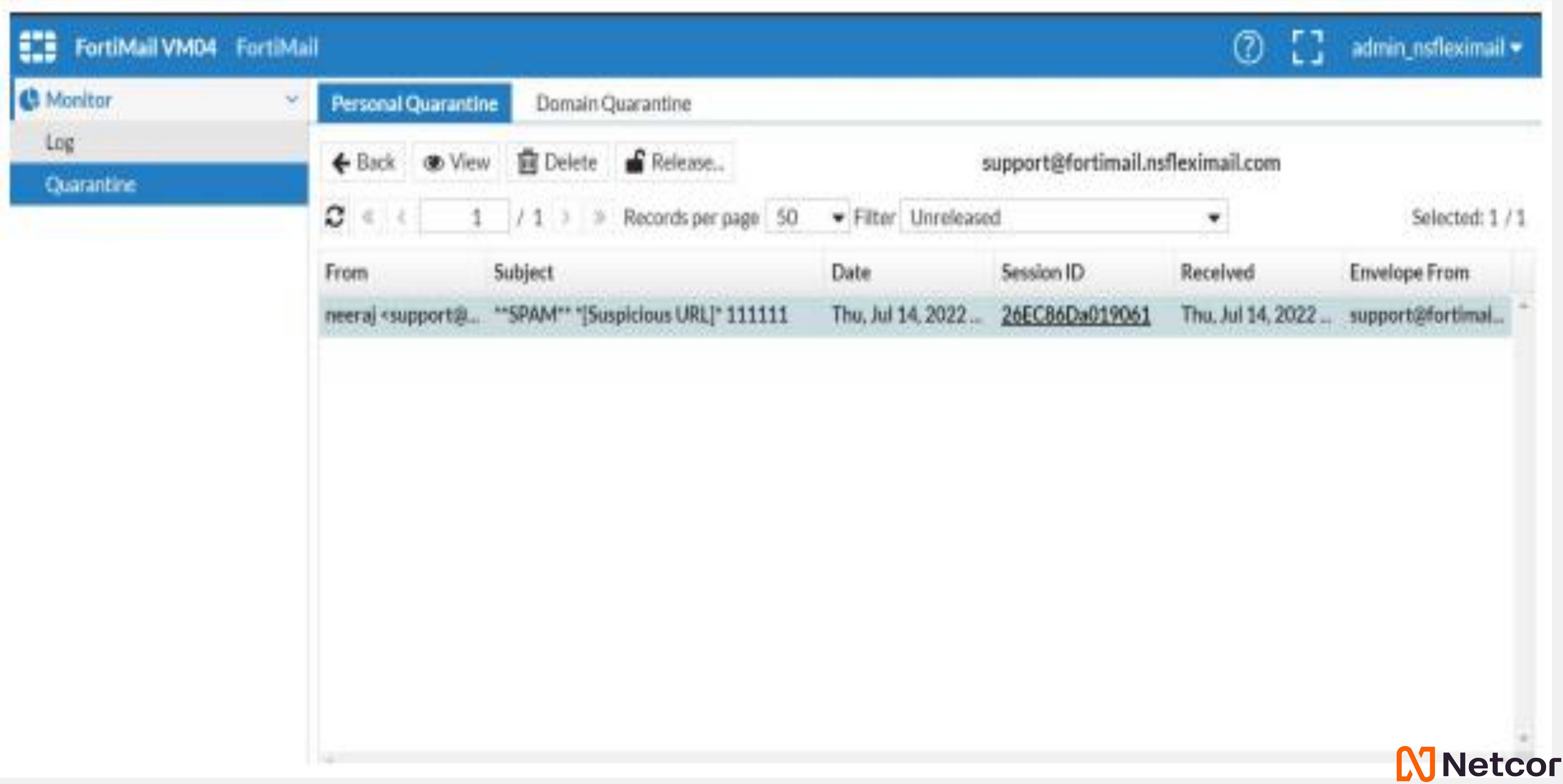
To check the mail quarantine kindly, navigate to the quarantine option and check for the quarantine mail as shown in the below snapshot.



Total: 2

Mailbox	Size (KB)	Message Count
siddhesh@fortimail.nsfleximail.com	0	0
support@fortimail.nsfleximail.com	11	1

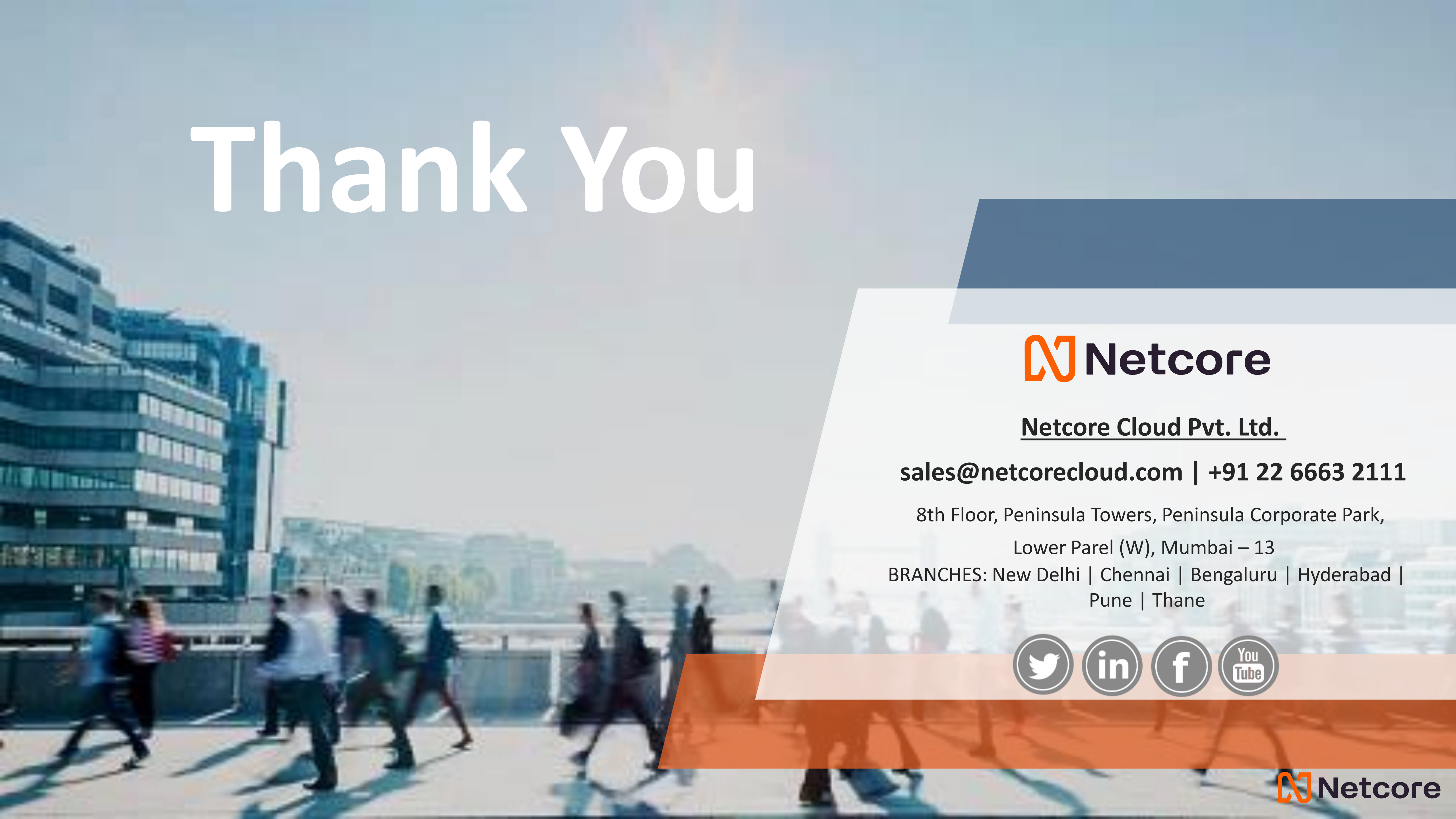
To release the quarantine mail, you can simply double click on the email and you will get an option to release that mail from the quarantine as shown in the below snapshot



support@fortimail.nsfleximail.com

1 / 1 Records per page 50 Filter Unreleased

From	Subject	Date	Session ID	Received	Envelope From
neeraj <support@...	**SPAM** *[Suspicious URL]* 111111	Thu, Jul 14, 2022 ...	26EC86Da019061	Thu, Jul 14, 2022 ...	support@fortimail...



Thank You

Netcore

Netcore Cloud Pvt. Ltd.

sales@netcorecloud.com | +91 22 6663 2111

8th Floor, Peninsula Towers, Peninsula Corporate Park,
Lower Parel (W), Mumbai – 13
BRANCHES: New Delhi | Chennai | Bengaluru | Hyderabad | Pune | Thane