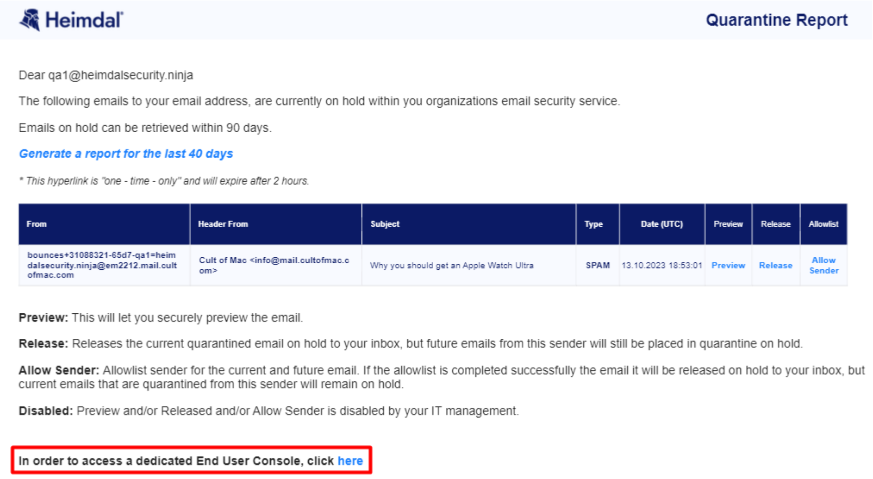
Heimdal AntiSPAM EMAIL SECURITY

The best way to release emails that have been blocked by Heimdal is to open the Email Security personal/individual console

There is a link at the bottom of the daily Quarantine Report that is emailed to you. (The link changes daily so always use todays report!)



Heimdal — Quarantine Report

Dear qa1@heimdalsecurity.ninja

The following emails to your email address, are currently on hold within you organizations email security service.

Emails on hold can be retrieved within 90 days.

Generate a report for the last 40 days

** This hyperlink is "one - time - only" and will expire after 2 hours.*

From	Header From	Subject	Type	Date (UTC)	Preview	Release	Allowlist
bounces+31088321-65d7-qa1=heimdalsecurity.ninja@em2212.mail.cultofmac.com	Cult of Mac <info@mail.cultofmac.com>	Why you should get an Apple Watch Ultra	SPAM	13.10.2023 18:53:01	Preview	Release	Allow Sender

Preview: This will let you securely preview the email.

Release: Releases the current quarantined email on hold to your inbox, but future emails from this sender will still be placed in quarantine on hold.

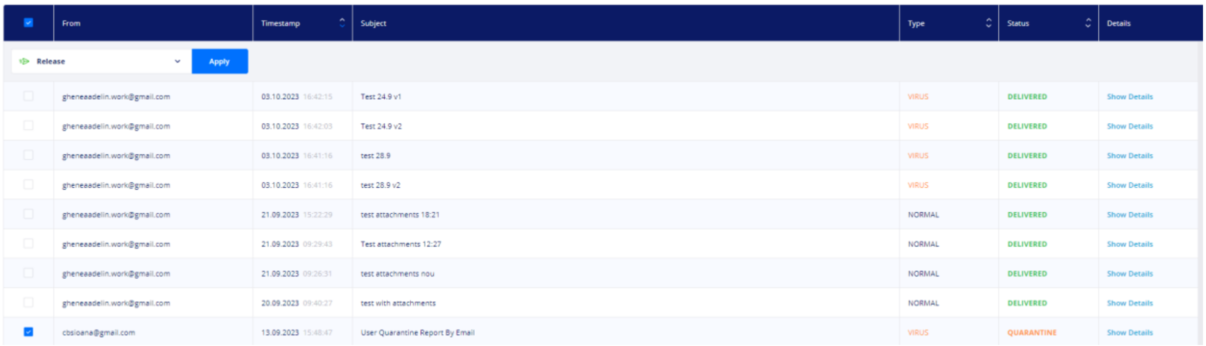
Allow Sender: Allowlist sender for the current and future email. If the allowlist is completed successfully the email it will be released on hold to your inbox, but current emails that are quarantined from this sender will remain on hold.

Disabled: Preview and/or Released and/or Allow Sender is disabled by your IT management.

In order to access a dedicated End User Console, click here

If you click on the link, the screen below will display and you can see all the email sent to your email address. Note the status column showing:
DELIVERED, QUARANTINED, QUEUED, UNDELIVERED, or REJECTED.

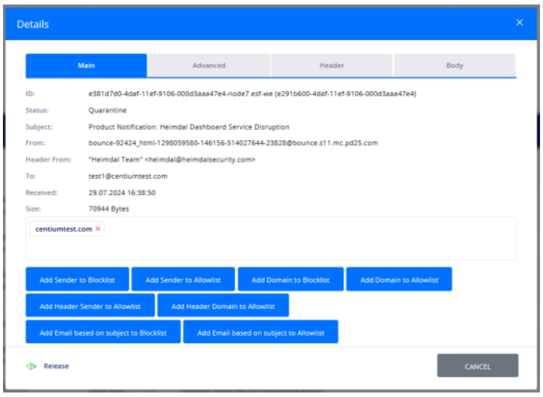
Quarantined emails can be released from the Email Security console by selecting the email and by choosing the **Release** action from the top drowndown menu.



☑	From	Timestamp	Subject	Type	Status	Details
□	gheneaadelin.work@gmail.com	03.10.2023 16:42:15	Test 24.9 v1	VIRUS	DELIVERED	Show Details
□	gheneaadelin.work@gmail.com	03.10.2023 16:42:03	Test 24.9 v2	VIRUS	DELIVERED	Show Details
□	gheneaadelin.work@gmail.com	03.10.2023 16:41:16	test 28.9	VIRUS	DELIVERED	Show Details
□	gheneaadelin.work@gmail.com	03.10.2023 16:41:16	test 28.9 v2	VIRUS	DELIVERED	Show Details
□	gheneaadelin.work@gmail.com	21.09.2023 15:22:29	test attachments 18:21	NORMAL	DELIVERED	Show Details
□	gheneaadelin.work@gmail.com	21.09.2023 09:29:43	Test attachments 12:27	NORMAL	DELIVERED	Show Details
□	gheneaadelin.work@gmail.com	21.09.2023 09:26:31	test attachments nou	NORMAL	DELIVERED	Show Details
□	gheneaadelin.work@gmail.com	20.09.2023 09:40:27	test with attachments	NORMAL	DELIVERED	Show Details
☑	cbsioana@gmail.com	13.09.2023 15:48:47	User Quarantine Report By Email	VIRUS	QUARANTINE	Show Details

Once an email is released, it isn't possible to release it again!
In this case the button will show "**This action is not allowed by your IT admin**"

Clicking on the **Details** column next to an email allows you to add items to the **Blocklist**.



ID: e381d7d0-4daf-11ef-9106-000d3aaa47e4-node7.esf-we (e291b600-4daf-11ef-9106-000d3aaa47e4)
Status: Quarantine
Subject: Product Notification: Heimdal Dashboard Service Disruption
From: bounce-92424_html-1298059580-146156-514027644-23828@bounce.s11.mc.pd25.com
Header From: "Heimdal Team" <heimdal@heimdalsecurity.com>
To: test1@centiumtest.com
Received: 29.07.2024 16:38:50
Size: 70944 Bytes

centiumtest.com ×

Add Sender to Blocklist
Add Sender to Allowlist
Add Domain to Blocklist
Add Domain to Allowlist
Add Header Sender to Allowlist
Add Header Domain to Allowlist
Add Email based on subject to Blocklist
Add Email based on subject to Allowlist
Release
CANCEL

TheType column shows the type of detection:

1. **SPAM,**
2. **SPF**
3. **DMARC.**

You are able to release SPAM emails,
SPF or DMARC are more dangerous and you would need to contact Andisa to ask for them to be released / whitelisted. If they are from a safe sender then they are detected because the sender hasn't configured their own email system correctly. That needs fixing by the sender and not yourself.

Here is a brief explanation of SPAM, SPF and DMARC:
SPAM filters are like the guard at the front door checking for suspicious visitors.
They look for things like:

- Weird subject lines (e.g., "Win $$$ Now!")
- Messages with lots of links or bad grammar
- Emails from unknown or untrusted senders

If the guard thinks an email is fishy or unwanted, it blocks it or throws it into the "spam" folder.

SPF (Sender Policy Framework) is like a "who's allowed to send emails FROM this domain" list.
Imagine someone trying to deliver a package to your house, but their name isn't on the list of trusted delivery drivers. You won't accept the package, right?
If the email's sender isn't on the "allowed list," it gets blocked. However it is the sender that sets up their own SPF.

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is like a "house rule" that tells you what to do if the SPF record isn't right.

- "If the sender isn't on our SPF list or can't prove they're legitimate, delete the email."

It's an extra layer of protection to stop people from pretending to be someone else, like fake bank emails trying to scam you.