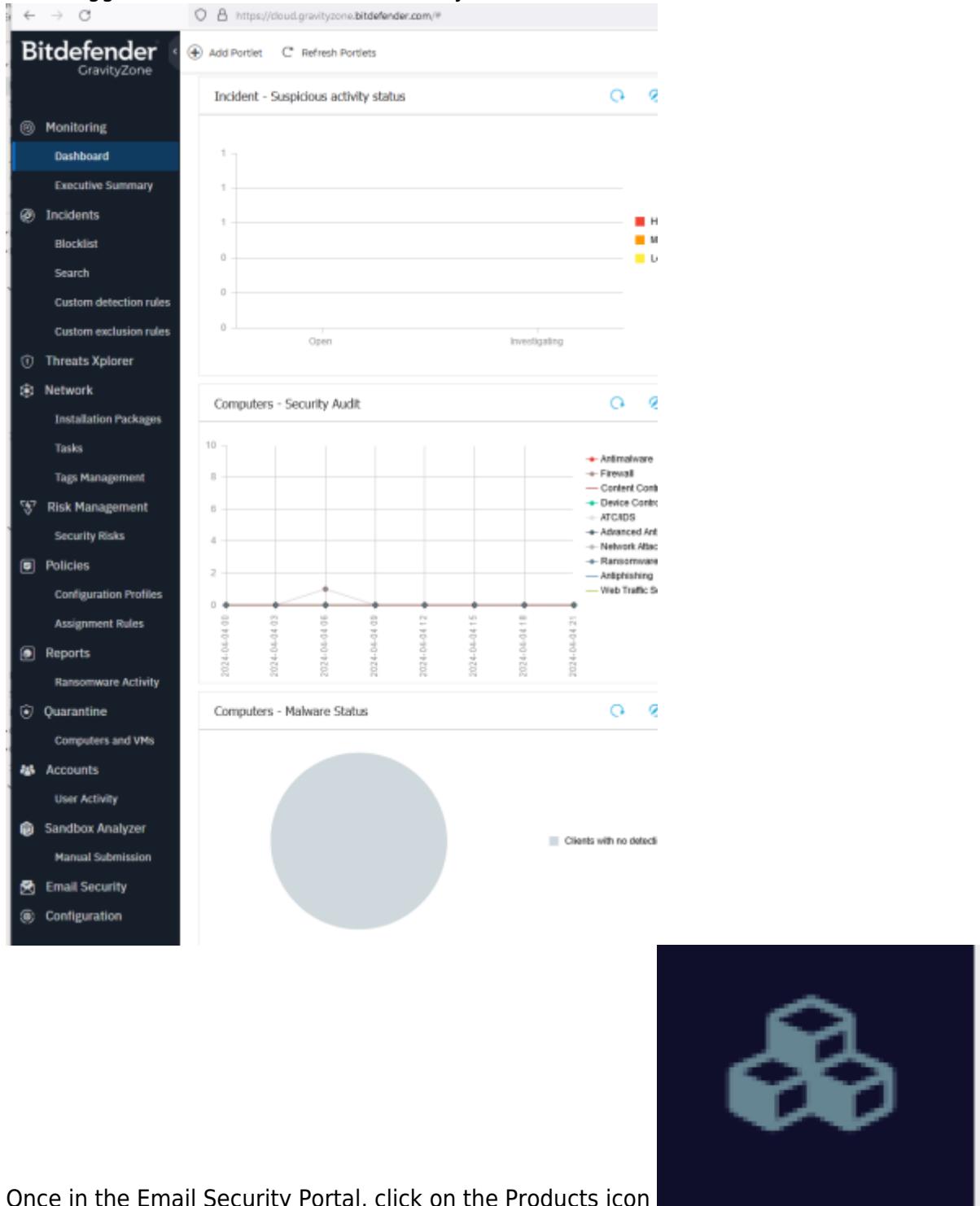


Log into the Bitdefender portal with your company username and password -

<https://cloud.gravityzone.bitdefender.com/>

Once logged in, click on the Email Security link on the left hand side:



The screenshot shows the Bitdefender GravityZone portal interface. The left sidebar is titled 'Bitdefender GravityZone' and contains a navigation menu with the following items:

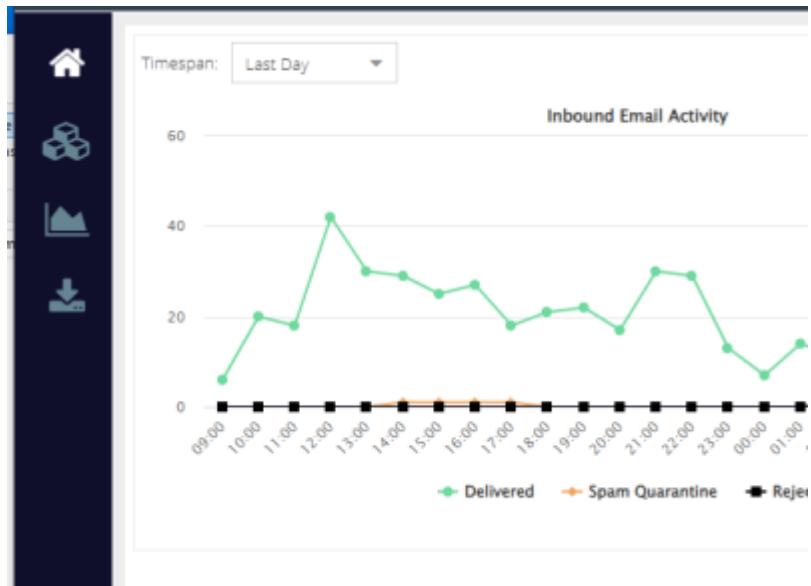
- Monitoring: Dashboard, Executive Summary
- Incidents: Blocklist, Search, Custom detection rules, Custom exclusion rules
- Threats Xplorer
- Network: Installation Packages, Tasks, Tags Management
- Risk Management: Security Risks
- Policies: Configuration Profiles, Assignment Rules
- Reports: Ransomware Activity
- Quarantine: Computers and VMs
- Accounts: User Activity
- Sandbox Analyzer: Manual Submission
- Email Security
- Configuration

The main content area has three tabs:

- Incident - Suspicious activity status:** A line chart showing the status of incidents over time. The Y-axis ranges from 0 to 1, and the X-axis shows 'Open' and 'Investigating' status. The chart shows a single data point at 'Investigating' status with a value of 1.
- Computers - Security Audit:** A line chart showing the status of security audits over time. The Y-axis ranges from 0 to 10, and the X-axis shows dates from 2024-04-04 to 2024-04-21. The chart shows a single data point at 2024-04-06 with a value of 1. The legend includes: Antimalware, Firewall, Content Cont, Device Cont, ATCIDS, Advanced Ant, Network Attic, Ransomware, Antiphishing, and Web Traffic.
- Computers - Malware Status:** A large gray circle with the text 'Clients with no detected' below it.

On the right side of the main content area, there is a large, dark blue rectangular area containing a stylized icon of three interconnected cubes.

Once in the Email Security Portal, click on the Products icon  on the left hand side.



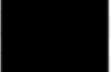
Click on the link for Global Quarantine.

The screenshot shows the Bitdefender GravityZone interface. The left sidebar has a 'Products' section with 'Email Security' selected. Under 'Email Security', the 'Global Quarantine' link is highlighted in blue. Other options include Message Rules, Connection Rules, Custom Rule Data, Spam Deny List, Spam Safe List, Mailboxes, Group Management, and Product Configuration. Below the main menu, there are 'SecureMail' and 'Settings' sections, with Administrators and Active Directory listed under Settings.

Once the form loads, you can adjust the Timespan from the top drop down menu as well as any of the other filters on the page.

The screenshot shows the 'Quarantine Messages' report. The left sidebar is the same as the previous screenshot. The main area has a 'Quarantine Messages' title and a 'Timespan' dropdown set to 'Last 24 hours'. Below it is a table with columns: Message, Quarantine, Content, and Action. The table shows a single row with the message '1234567890@domain.com' in the Content column and 'Quarantine' in the Action column. There are 'Delete' and 'Archive' buttons at the bottom of the table.

Click the Run Report button when ready to see a list of emails stuck in quarantine for the time period you selected.

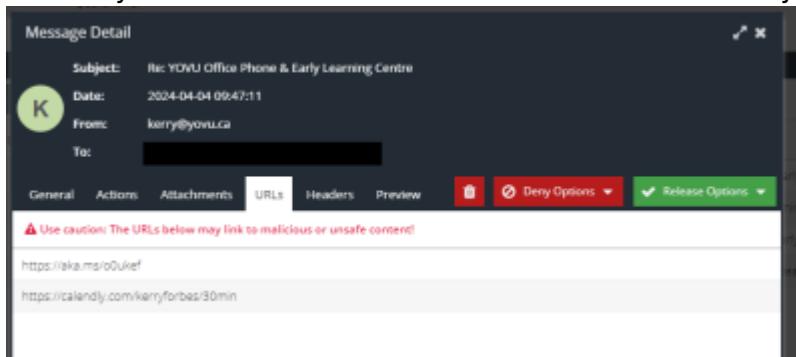
		Deny Options		Release Options	
Direction	Sender/Recipient (local)	Sender Address	Sender IP	Subject	Recipient(s)
<input type="checkbox"/>	2024-02-04 09:47:11	Henry@yovu.ca	289.83.288.45	Re: YOVU Office Phone &...	
<input type="checkbox"/>	2024-02-04 09:47:48	louisville41452093-2008	149.11.233.244	Dear Bill from Alaska Conn...	
<input type="checkbox"/>	2024-02-04 18:31:17	louisville7738-0782	128.341.240.38	Starting (Medium) Chat...	
<input type="checkbox"/>	2024-02-04 11:28:09	AutodeskOpen@Inno...	46.92.383.87	Re: [Autodesk Academi...	

You can achieve multiple objectives with this report.

You will see the list of suspected emails, who they were from, who they were sent to and why the have been quarantined.

If you click on the Subject line for the email you want to investigate, this will open a representation of that email in a safe sandbox form to protect your from anything in that email that might be suspicious. After looking at the email, you can determine if in fact this is a legitimate email or is in fact Spam or possibly malware.

If you click on the Magnifying glass at the right, it will show you all of the details for the email as well as any attachments or links in the email. Be very careful about clicking on any of the links as this will remove you from the safe sandbox environment and take you directly to that link.



Once you determine if this is a valid email or not, after selecting the email either by click on the magnifying glass to the right, or placing a checkbox at the left for that email, you can click on the Release Options dropdown of the Deny Options dropdown if you want to release this email or the Deny Options download if you want to deny this email.

Your options for the Release Options are:

1. Release - will release this email to the user's inbox without adjusting any spam rules
2. Safe Sender - will release this email to the user's inbox AND will add the sending email ACCOUNT (i.e. rdakin@computersdotcalm.com) to the Spam Safe list.
3. Safe Domain - will release this email to the user's inbox AND will add the sending email DOMAIN (i.e. computersdotcalm.com) to the Spam Safe list.
4. IP address - will release this email to the user's inbox AND will add the IP Address of the sending email server to the Spam Safe list.

Your options for the Deny Options are:

1. Deny Sender - this will add the sending email ACCOUNT to the Spam Deny list.
2. Deny Domain - this will add the sending email DOMAIN to the Spam Deny list. Be very careful with this option as you may inadvertently block say all Gmail account.
3. IP address - this will add the IP Address of the sending email server to the Spam Deny list. Once again, be very careful with this option.

Once you are done, if there are any emails left in the report, you can delete all of them or individual ones by placing a check mark on the left and then clicking the Delete icon at the top of the column to

delete those emails.

When you are done, you can click the Red close icon in the top right hand corner.

From:
<http://wiki.computersdotcalm.com/> - **ComputersDOTCalm Wiki**

Permanent link:
<http://wiki.computersdotcalm.com/doku.php?id=bitdefender:check-email-quarantine&rev=1713019364>

Last update: **2024/04/13 14:42**

