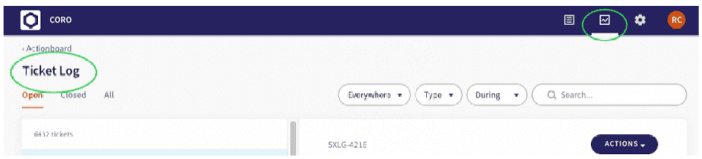
v1.5

Version 1.5 constitutes a major release, with multiple additions, extensions and improvements.

Terminology

We've aligned terminology, and now all issues that require attention are referred to as tickets.

Additionally, the Detection log is now called the **Ticket Log**.



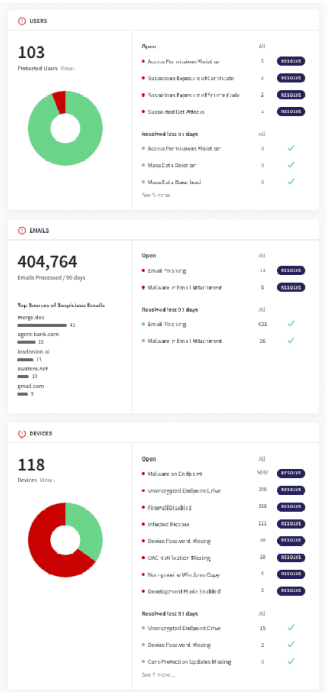
We've also renamed access for **Cloud Apps** in the **Control Panel**, and it's now called **Access Permissions**.

Actionboard

The **Actionboard** has been updated and enriched to give a more accurate snapshot of your network security posture, including:

- Resolution statistics are now in the ticket overview at the top of the board.

- Enriched widgets appear similar to the following:



Improvements include:

- The graphical layout of widgets has been improved to more plainly differentiate between their different parts
- Open and resolved ticket details for the last 90 days are clearly displayed on the right part of the widget
- All tickets are now linked to their complete details in the **Ticket Log**, enabling operators to take action faster, with fewer clicks and less navigation
- Entity details and statistics are displayed on the left side of each widget to help operators visualize security posture details at a glance
- The information on the left side of each widget is linked to its relevant "entity" space (for example, **Users**, **Devices**)

Tickets

The **Ticket Log** now includes all tickets from all areas of the system. We've also improved the way we handle and display tickets for you, as follows:

- Automatic ticket resolution has been updated to resolve more tickets, reducing the amount of manual work for operators
- Enriched details have been added to tickets to provide further context around events
- Advanced filtering has been added to enable sorting and searching for specific tickets and groups of tickets

Automatic ticket resolution

Previously, most tickets created in the system needed to be reviewed and then manually closed by the operator, regardless of severity and regardless of any actions or remediation taken for the related issues.

We've now improved ticket handling by automatically closing all tickets related to issues that don't need to be reviewed by an operator, making it more intuitive and easier to manage the number of open tickets in the system at any given time.

Protected and unprotected user tickets

In general, all tickets created in relation to users:

- For protected users, tickets are logged and referenced for audit after being closed; this logging activity is communicated to the operators in the ticket view.
- For unprotected users, Coro continues to generate tickets related to unprotected users, and these tickets are only accessible via the **Ticket Log** view. Additionally, these tickets are now:
  - Automatically closed by Coro and cannot be re-open
  - Not logged nor referenced for audit
    Note: Coro has no obligation for keeping these tickets accessible over time.

Ticket classifications

Tickets are identified and handled by Coro according to the following classifications:

- Require operator's review (G1) - tickets remain open until the operator explicitly closes them
- Suggested for operator's review (G2) - tickets remain open for a limited period of time and are automatically closed by the system when the respective time window for review is over, whether the operator reviewed them or not
- Immediately auto-closed by the system (G3) - tickets are closed immediately by Coro, either following their resolution or because the related issues only need to be monitored and logged for compliance audits

How it works

1. After created in the system, tickets are sorted and assigned to their relevant area: email, data, devices, users, cloud apps.
2. Tickets are classified according to the unique logic for that area.
3. If a closed ticket is explicitly re-opened by the operator, it is automatically re-classified independent of its initial classification by the system.

Email ticket logic

Email security issues are handled as follows:

Tickets associated with user phishing/safe feedback provided via Coro add-ins, spoofing of important domains (including customer's domains), and impersonation of specific users of the customer - these tickets are classified as G2, suggested for review, and are automatically closed after the review period of two weeks.

All other flagged incoming emails are deleted or removed from the Inbox and moved to the Suspected folder, and are classified as G3, and are immediately closed by the system.

Data ticket logic

Ticket logic for data violations attempts to find the balance between the need to:

- Detect and log everything for audit that might constitute a privacy/compliance breach
- Primarily focus on particularly problematic private information exposures.

Accordingly, data governance tickets are classified as follows:

- Detections that, according to the best practices of data governance regulations (GDPR, HIPAA, SOC2, etc.), require attention of the data compliance officers - tickets are classified as suggested for review (G2), with a review time window of two weeks
- All other tickets are classified as G3, and are automatically closed by the system

Device ticket logic

Coro detects files and processes on the endpoint devices suspected as malicious, as well as various vulnerabilities in the security posture of the devices.

- All files detected as malicious are automatically quarantined and all processes detected as suspicious are automatically terminated; no further remediation actions on the side of the operator are required. At the same time, after examining the ticket, the operator may decide to approve the respective file or even to exclude the folder in which the flagged file resided from malware scans by Coro. Therefore, all tickets on malware files/processes are classified as suggested for review (G2), with a review time window of two weeks.
- The classification of the device vulnerability tickets depends on the Device Posture settings for each environment and it depends on the vulnerabilty that is introduced, and can be one of the following:
  - *Ignore*. No auto-remediation is performed, and the ticket is classified as G3, being auto-closed and logged immediately.
  - *Review*. No auto-remediation is performed, and the ticket is classified as requiring review (G1). The ticket remains open until either the operator closes it manually or the vulnerability is observed by the Coro endpoint agent as being resolved.
  - *Enforce*. Auto-remediation is performed, recorded in the ticket, and the ticket is classified as G3, and thus auto-closed.

User ticket logic

- Access Permission violations for which an operator has already explicitly specified an auto-remediaton action are immediately closed
- All other user tickets are classified as suggested for review (G2), with time windows of 1-2 weeks, depending on the possible lasting effect of the respective detection
- At this time, Suspected Bot Attack and Abnormally Massive Dowload tickets are currently classified as G3 and are automatically closed, however Coro is currently evaluating this logic and considering aligning them with the other tickets in the Users category.

Cloud app ticket logic

- All files detected as malicious are automatically moved to a dedicated quarantined folder; no further remediation action on the part of the operator is required. At the same time, after examining the ticket, the operator may decide to approve the respective file, or to permanently delete it. Therefore, all cloud app malware tickets are classified as suggested for review (G2), with a review time window of two weeks.
- Suspected Identity Compromise and Abnormal Admin Activity tickets are classified as suggested for review (G2), and are automatically closed after the review period of two and four weeks, respectively.
- Suspected Bot Attack tickets are classified as G3, being automatically closed and logged immediately.

Enriched details

All details related to each ticket are now embedded within each ticket, enabling operators to quickly access tickets, understand their context, and resolve any open tickets, without having to navigate anywhere else.

In the **Ticket Log**, tickets look similar to the following:

From the **Ticket Log** these details have been added within each ticket:

- a complete list of all related events and their details, enabling the operator to understand why the ticket was created and where the issue is within the network; this set of details is uniquely organized depending on the origin of the ticket
  For example, PII policy violations can appear similar to the following:

- a snapshot of the most recent related activity that is recorded in the **Activity Log** is now embedded within each ticket, with a link to the entire list of related activity:

Filtering

You can filter to find specific tickets easily:

Filters include:

- **Module** - filter to see tickets for only devices, cloud apps, email, users, data or for all modules together
- **Type** - view tickets related to one or more specified policy violations (for example, device password missing or development mode enabled)
- **Time period** - view tickets for a specified period of time
- **Free text** - enter free text to find tickets by additional parameters

Malware in cloud drives: remediation and allowlisting

Automatic remediation is now implemented when malicious malware/ransomware files are detected in drives associated with Microsoft 365, Google Workspace, Salesforce, Dropbox and Box. Additionally, operators can also allowlist specific files.

When a problematic file is detected in one of your connected cloud drives, the file is immediately quarantined using a "trash" folder. If the operator approves the file described in the ticket, the file is restored to its original location within the drive.

Alternatively, the operator can choose to permanently delete the file in question.

Settings and permissions

The following settings have been improved:

- Device posture settings
- Data governance access
- Access management

Device posture settings

The new **Device Posture** settings allows the operators to specify what device vulnerabilities are of interest, for which environments (Windows PC, Windows Servers, and macOS), and to what extent.

The default settings are configured according to the most common practices, but operators can adapt them to the specifics of their operations.

For each pair of environment+vulnerability, an operator can specify whether this vulnerability should be Ignored, Reviewed, or Enforced, as follows:

- **Ignore -** tickets are generated, but they will be immediately logged, automatically closed by the system and automatically remediated
- **Review -** no auto-remediation is performed; tickets remain open until either closed by an operator or the vulnerability is observed by the Coro endpoint agent as already resolved.
- **Enforce -** auto-remediation is performed, and the ticket is automatically logged and closed. **Note:** This option is available only for environments/vulnerabilities for which remediation of the respective vulnerability can be done through the Coro Endpoint Protection agent.

Data governance permissions management

Data governance regulations such as GDPR, HIPAA, SOC2, PCI DSS, and CPA, require monitoring of:

- potential exposure of sensitive information to an unauthorized person within or outside of the organization
- access to such information by an unauthorized person

The permissions appear similar to the following:

Operators can now specify the authorization policy according to the unique business practices and authorizations. By default, all workspace users are defined as Allowed to Access (which means they can view, but cannot share the data) all types of sensitive information, reflecting the implicit policy that has been enforced in Coro in earlier versions.

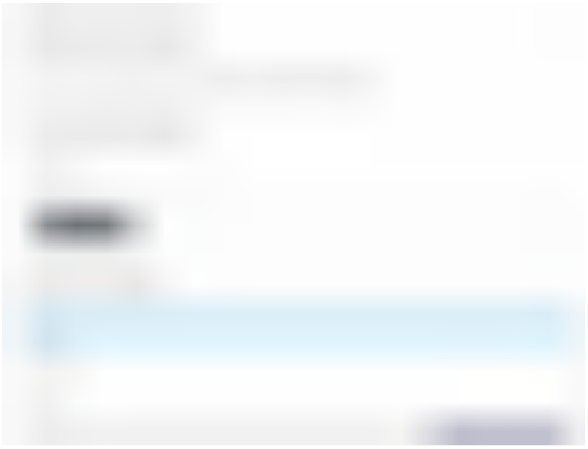
You can change the default policy of permissions by adding or removing permissions to the access and expose data objects that might contain personally identifiable information (PII), payment card information (PCI) and protected health information (PHI).

Additionally, you can also add explicit permission for a user to expose information that might contain PII and PCI (but not PHI).

The data governance tickets displayed from the Actionboard will be created only if the detected data objects have been accessed or shared in violation of the current policy settings.

Cloud apps access permissions

We've made a couple of updates to the user interface for access permissions



Note: due to the changes introduced by Microsoft and Google to their email services to comply with current and foreseen privacy regulations, the IP address of the sender is no longer part of the email headers from these providers, and thus is not accessible for Coro to monitor in the context of Access Permissions.

Activity Log

The **Activity Log** has been enriched with numerous important additions and improvements, and now appears similar to the following:

These changes include:

- activities are now logged that were previously not logged (auto-remediation actions, manual action of contacting the users associated with a ticket by email)
- activity log records are linked to their corresponding tickets
- the actor behind the specific activity log record is now logged as well
- free text search is available to find relevant activity faster

Endpoint protection for Windows

While a major version for the Endpoint Protection agents is scheduled for the end of October, we are now releasing an update to Coro Endpoint Protection for Windows. (An update for macOS will also come later on.)

This version contains:

- Multiple performance improvements
- Monitoring, and control over the remote malware scan actions, including the ability to stop the scan before it has ended
- Collecting log files from the endpoint agents, both by the user by saving the log files to the desktop, as well as remotely, by Coro technical support team
- An enhanced block mode of operation that is optimized for EDR functionality when Coro Endpoint Protection is used side-by-side with Windows Defender Antivirus. In this mode, we ensure that all the essential information is accessible to our agent despite the fact that it is not operating as the primary antivirus.
  Note: this feature is still in Beta, and thus by default is set to Off. In the next version, it is planned to become our primary mode of operation.

Contextual data for network objects

The **Users** and the **Devices** sections now also include information from the **Ticket Log** and the **Activity Log**, embedded within the card for the specific object.

For example, you can clearly see all open tickets, access their details directly from within the context of the laptop, and view the related activity from the **Activity Log** for the selected laptop device in the following screenshot: