Security Dashboard

In this article

Overview

The Security & Compliance Center enables your organization to manage data protection and compliance. Assuming you have the necessary permissions, the Security Dashboard enables you to review your Threat Protection Status, as well as view and act on security alerts.

Depending on what your organization's Office 365 subscription includes, the Security Dashboard includes several widgets, such as Threat Management Summary, Threat Protection Status, Global Weekly Threat Detections, Malware, and more, as described in the following sections.

To view the Security Dashboard, in the Office 365 Security & Compliance Center, go to **Threat management** > **Dashboard**.

Note

You must be an Office 365 global administrator, a security administrator, or a security reader to view the Security Dashboard. Some widgets require additional permissions to view. To learn more, see Permissions in the Office 365 Security & Compliance Center.

Threat Management Summary

The Threat Management Summary widget tells you at a glance how your organization was protected from threats over the past seven (7) days.

The information you'll see in the Threat Management Summary depends on what you subscription includes. The following table describes what information is included for Office 365 E3 and Office 365 E5. ||| |---|---| |**Office 365 E3**|**Office 365 E5**| |Malware messages blocked
Phishing messages blocked
Messages reported by users

|Malware messages blocked
Phishing messages blocked
Messages reported by users
Zero-day malware blocked

Advanced phishing messages detected
Malicious URLs blocked| |

To view or access the Threat Management Summary widget, you must have permissions to view Advanced Threat Protection reports. To learn more, see What permissions are needed to view the ATP reports?.

Threat Protection Status

The Threat Protection Status widget shows threat protection effectiveness with a trending and detailed view of phish and malware.

The details depend on whether your Office 365 subscription includes Exchange Online Protection (EOP) with or without Office 365 Advanced Threat Protection (ATP).

Table 1

If your subscription includes...	**You'll see these details**
EOP but not Office 365 ATP	Malicious email that was detected and blocked by EOP. See Threat Protection Status report (EOP).
Office 365 ATP	Malicious content and malicious email detected and blocked by

Table 1

EOP and Office 365 ATP

Aggregated count of unique email messages with malicious content blocked by the anti-malware engine, zero-hour auto purge, and ATP features (including Safe Links, Safe Attachments, and ATP anti-phishing).

See Threat Protection Status report (ATP).

To view or access the Threat Protection Status widget, you must have permissions to view Advanced Threat Protection reports. To learn more, see What permissions are needed to view the ATP reports?.

Global Weekly Threat Detections

The Global Weekly Threat Detections widget shows how many threats were detected in email messages over the past seven (7) days.

The metrics are calculated as described in the following table:

Table 2

Metric	How it's calculated
Messages scanned	Number of email messages scanned multiplied by the number of recipients
Threats stopped	Number of email messages identified as containing malware multiplied by the number of recipients
Blocked by ATP	Number of email messages blocked by ATP multiplied by the number of recipients
Removed after delivery	Number of messages removed by zero-hour auto purge multiplied by the number of recipients

Malware

Malware widgets show details about malware trends and malware family types over the past seven (7) days.

Insights

Insights not only surface key issues you should review, they also include recommendations and actions to consider.

For example, you might see that phishing email messages are being delivered because some users have disabled their junk mail options. To learn more about how insights work, see Reports and insights in the Office 365 Security & Compliance Center.

Threat investigation and response

If your organization's subscription includes Office 365 Advanced Threat Protection Plan 2, your Security Dashboard has a section that includes advanced threat investigation and response tools. Your organization's security team can use the information in this section to understand emerging campaigns, investigate threats and manage incidents.

Trends

Near the bottom of the Security Dashboard is a **Trends** section, which summarizes email flow trends for your organization. Reports provide information about email categorized as spam, malware, phishing attempts, and good email. Click a tile to view more detailed information in the report.

And, if your organization's Office 365 subscription includes Office 365 Advanced Threat Protection Plan 2, you will also have a **Recent threat management alerts** report in this section that enables your security team to view and take action on high-priority security alerts.

To view or access the Sent and Received Email widget, you must have permissions to view Advanced Threat Protection reports. To learn more, see What permissions are needed to view the ATP reports?.

To view or access the Recent Threat Management Alerts widget, you must have permissions to view alerts. To learn more, see RBAC permissions required to view alerts.