How Does The Threat Scan Work?

The Mimecast Email Security Cloud Integrated Threat Scan processes 30 days of mail already delivered by Microsoft. The mail is processed using the same inspection engines when Mimecast protects live mail, giving you and your organization a window into the types of threats lying dormant in your inboxes. Mimecast will use the Microsoft Graph API within M365 and will not affect mail flow or modify settings in "Threat Scan Only" mode.

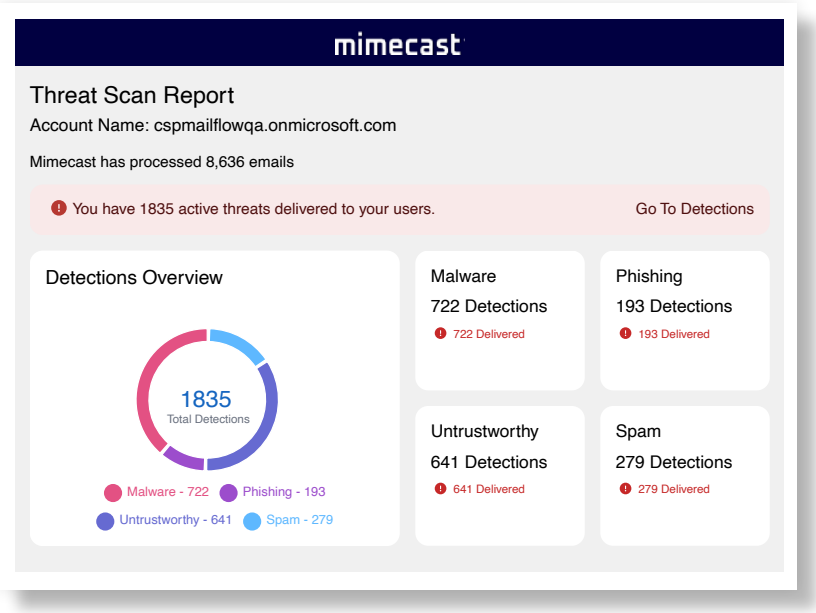
What Privileges Are Required?

Mimecast requires M365 Global Admin privileges to allow access to mail and optionally remediate any discovered threats. For more information on the required privileges, review the Connecting to Microsoft 365 article on Mimecaster Central.

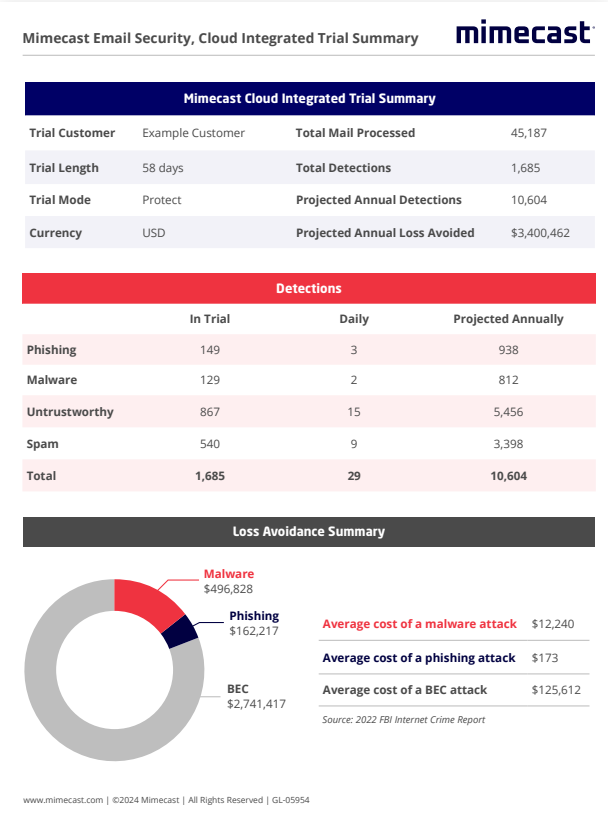
What Threat Information Is Provided?

Threats and unwanted mail are shown in 4 categories: Malware, Phishing, Untrustworthy and Spam.

Upon completion of the Threat Scan, a notification email will be sent with a summary report attached. A Mimecast representative can also provide a Loss Avoidance report based on the Threat Scan detections.



Threat Scan Complete Report



Loss Avoidance Report

Mimecast Is With You Every Step Of The Way

For a seamless, risk-free integration with your live mail environment, make sure to select the "Threat Scan Only" option when completing the initial setup. Integrating with live mail flow can come with some risk, and we recommend working closely with a Mimecast expert before moving to Monitor or Protect mode. Thanks for starting your journey to better Email and Collaboration Security with Mimecast. We are here to assist you every step of the way!