

Threat Discover for Email

Deployment Requirements

Deployment Form-Factor

On-premise Virtual Appliance (OVA)

Supported Hypervisors

- VMWare ESX or ESXi 5.5 and up
- VMware Workstation (Windows) 11 and up
- VMware Fusion (Mac) 7.0 and up

Minimum Virtual Machine Hardware Requirements

- 4 CPU cores
- 4 GB RAM
- 300 GB disk storage

Supported Microsoft Exchange Environments

- Exchange 2010, 2013
- Exchange Online (O365)

Permissions Required for Scanning

- Exchange: User with Application Impersonation role or Full Access permission to scan selected mailboxes
- Active Directory: read-only permissions for querying AD user and group information

Supported Browsers for Threat Discover Dashboard

- Google Chrome 47.0 and up

As the #1 threat vector, email is the preferred way for many threat actors to target and gain footholds in an organization. Security professionals therefore need a quick and easy way to gain visibility into threats within their email environment. Proofpoint Threat Discover for Email quickly and simply provides this visibility.

Proofpoint Threat Discover for Email is a complimentary threat assessment tool that identifies malicious URLs and attachments residing in Exchange on-premises or Exchange Online (O365).

With Proofpoint Threat Discover for Email, you can start seeing scan results in minutes, with tool setup taking less than an hour.

Threat Discover for Email Features

- Scans Microsoft Exchange for URL and attachment-based threats
- Provides scan filter options to target specific mailboxes for scanning (e.g. specific department mailboxes, scan time window, etc.)
- Generates automatic scan report with meaningful metrics including number of mailboxes scanned, number of malicious messages found, top threats, and more
- Offers threat research write-ups for email campaigns associated with malicious URLs and attachments identified during scans
- Exports scan results in Excel format for custom reporting needs



Figure 1. Sample Threat Discover scan results