proofpoint.

DATA SHEET

Internal Mail Defense

Protect Your People From Advanced Threats In Internal Email

KEY BENEFITS

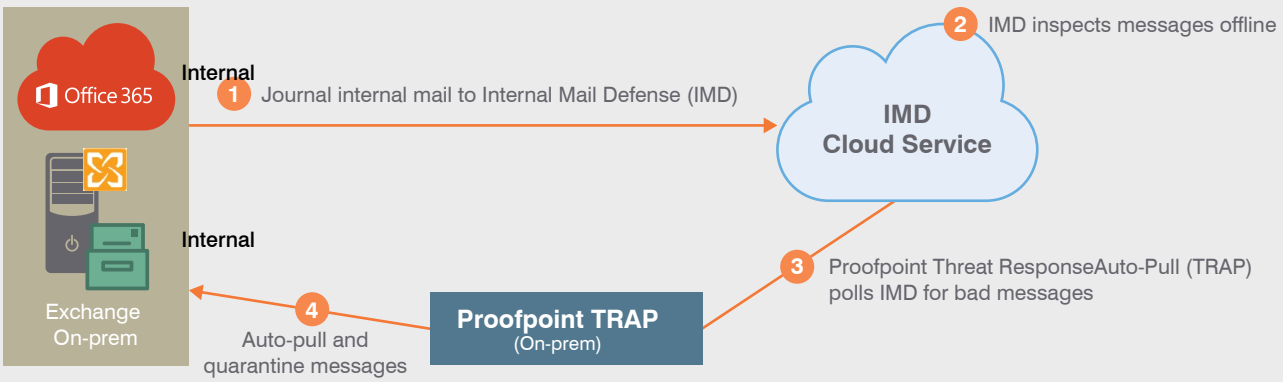
- Increase protection with robust anti-spam and multilayered malware scanning
- Protect against malicious URLs and attachments, including attachment sandboxing
- Quickly identify compromised accounts and take necessary action
- Reduce the time to contain and quarantine email threats
- Reduce exposure time to malicious emails
- Quarantine messages forwarded to individuals or distribution lists
- Robust reporting to quickly receive details in regards to compromise accounts and automatic alerting for incident changes or quarantine confirmation

Proofpoint Internal Mail Defense provides you with a robust, multilayered approach to protecting your organization's internal email. It also gives you the ability to help detect compromised accounts.

Proofpoint Internal Mail Defense provides you with a robust, multilayered approach to protecting your organization's internal email. It also gives you the ability to help detect compromised accounts.

With today's advanced threats, it's more important than ever to fully protect your organization's email communications. Because of its importance, email is the primary way cyber criminals try to attack an organization. A lot of time and effort has been spent over the years trying to protect email coming into an organization. But this often leaves security for internal email overlooked.

More than ever, internal email traffic must be treated the same way as email coming from external sources. It's important to have a multilayered security approach to scan internal emails. And you need to have the capability to scan these emails for malicious content in the form of URLs and attachments. And when a malicious internal email has been detected, you need an easy way to automatically pull and quarantine the offending messages. It's also important to have robust reporting for your internal email that gives your security team visibility into accounts that have potentially been compromised.



Internal Mail Defense High-Level Architecture

This multilayered approach is important because we have seen many problems related to credential phishing that can result in compromised accounts. These are accounts that attackers have taken over by various means and then use to look as though they are legitimate users within an organization. With the rise of cloud-based email services, these compromised accounts can appear as 'trusted' users. This can happen even when sending emails to other organizations using the same cloud email platform. These compromised accounts can be used to do anything from sending out spam attacks to malicious emails to leaking sensitive data.

Proofpoint MLX Machine Learning Technology

Powered by our MLX machine learning technology, Internal Mail Defense provides spam and phishing detection to give you maximum protection against email threats. It examines hundreds of thousands of attributes in every email. And it accurately detects text, image and attachment-based spam or phishing emails. At the same time, it automatically adapts to new threats as they appear. MLX technology uses the latest advances in reputation and content-based analysis. And it delivers the industry's highest level of effectiveness at 99%. This protects your people and your organization against all types of spam email.

Multilayered Malware Scanning

Internal Mail Defense uses several techniques to protect against both known and emerging threats. Signature-based detection prevents known threats while dynamic reputation analysis continually assesses local and global IP addresses to determine whether to accept, reject or throttle email connections. Together, these features help protect you at the first signs of malicious activity.

Protection from Malware-free Threats

Internal Mail Defense detects threats that don't involve malware, such as credential phishing and impostor email. It assesses the reputation of the sender by analyzing hundreds of thousands of email attributes, including the sender/recipient relationship, headers, and content. Impostor email—also known as business email compromise or CEO fraud—is a fast-growing threat that can cause huge losses.

Threat Protection Technology

Internal Mail Defense provides you with advanced threat protection. It leverages the power of Proofpoint Targeted Attack Protection (TAP), our industry-leading email analysis solution. Internal Mail Defense has robust reporting that allows your security team to quickly get reporting that indicates exactly which accounts may have been compromised. This enables them to quickly take action on those accounts.

Threat Remediation and Reporting

Using Proofpoint Threat Response Auto-Pull (TRAP), Internal Mail Defense can automatically pull bad messages out of your organization's message flow. This helps you rapidly lock down any threats that might be posed by internally compromised email accounts. It also allows your security team to get reporting that indicates exactly which accounts may have been compromised. And it enables them to quickly take action on those accounts.

LEARN MORE

For more information, visit **proofpoint.com**.