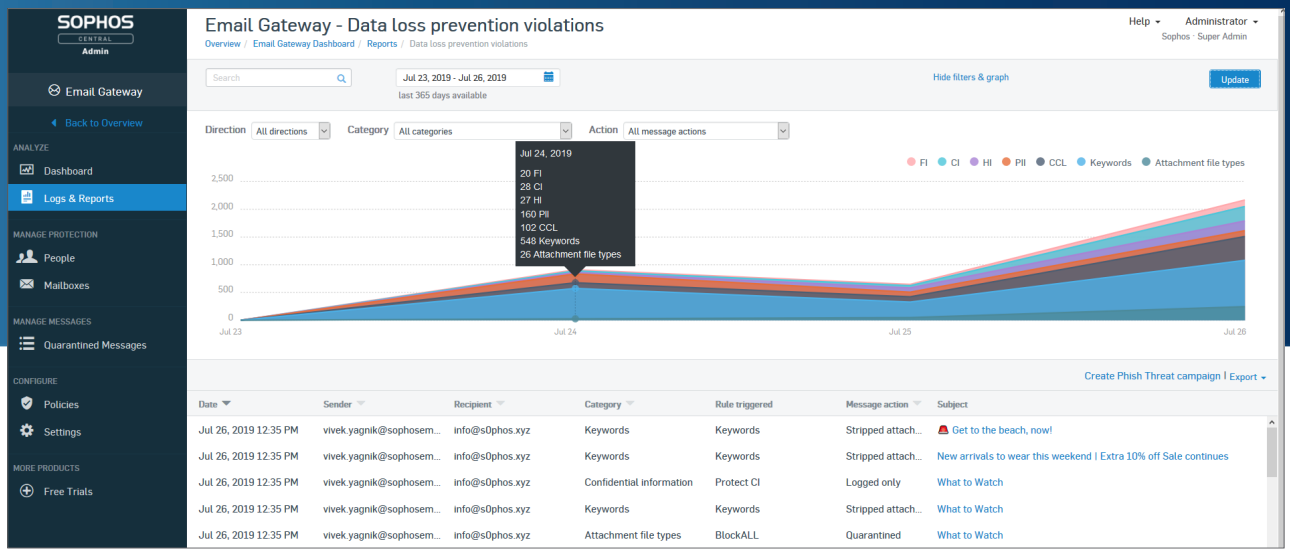
SOPHOS

What's New in Sophos Email

The latest updates available for Sophos Email



Overview

Sophos Email is email security delivered simply through Sophos Central's easy-to-use single management console, protecting your users from unwanted and malicious email threats today, and tomorrow, with the latest artificial intelligence to defend against ransomware and zero-day malware.

The latest enhancements to the Sophos Email go further, preventing outbound email data loss and inbound malware threats; synchronizing defenses with Sophos Endpoint and Phish Threat to respond to email threats inside your organization; and enhance reporting and policy control to provide greater visibility.

Phishing Email Impersonation Protection

Impersonation phishing attacks aim to deceive employees by using the name of a trusted sender or brand to encourage victims to reply, click a link, open an attachment, and so on.

Sophos Email has now made it simple to block these attacks, adding features to existing phishing protection, including SPF, DKIM, and DMARC authentication techniques, header anomaly analysis and several exciting advancements for Sophos Email Advanced phishing protection:

- Compare the display name of inbound emails to the display name of commonly abused cloud service brand names and to VIPs within the customers organization to check for matches. These could be the CEO, CFO, and HR director, and so on
- Analysis of the domain name of an email address in relation to the display name. Looking for free email services, for example Kris Hagerman <**whatever@gmail.com**>
- Analysis of look-a-like domains to identify domain names like the corporate domain – when the attacker is impersonating an internal user, such as Kris Hagerman <whatever@**sopos.co**>
- Alternatively, if an attacker is attempting to impersonate a trusted brand, Sophos Email will also identify domain names similar to well-known cloud services such as Microsoft, Amazon, and LinkedIn e.g. **Amazon Support** <anything@**amazon-email**.co>
- This new service then allows email administrators to act on potential attacks with policy controls to quarantine, tag the subject line, delete, or warn users, with a banner added to inbound emails

Data Loss Prevention and Content Control

Protect sensitive information, with discovery of financials, confidential contents, health information, and PII (Personally identifiable information) in all emails and attachments.

- Simple policy wizards provide granular control of data breach prevention measures, including multi-rule policies for groups and individual users with seamless integration of encryption (available as earlier access program)
- Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs
- Advanced malware protection blocks hidden threats that use forged file names to look safe, analyzing multiple attributes of a file to detect the true identity
- Automate phishing imposter defenses with keyword filters to block or quarantine sent emails and remove attachments displaying sensitive keywords in the file name
- Save valuable time with single saas-based console, managing data loss prevention measures for email, alongside endpoint protection

Email Encryption

Secure sensitive data and make compliance easy. Use policy-based enforced TLS encryption to prevent eavesdropping when messages are in transit, and policy-based email encryption from–converting a standard email into one with encrypted attachments, sent direct to the recipient's inbox.

- Encryption setup in minutes–with the ability to encrypt the entire email or attachments only
- Flexible policy control–allows organizations to encrypt all outbound messages sent to a set list of recipient addresses and domains
- Send secure messages fast–using the O365 add-in button, or by adding the organization's custom subject line tag to the message i.e. "Secure: ***"
- Reply securely–with Sophos Secure Messaging Portal for secure email replies, including attachments

Smart Banners

Smart Banners can now be added to any email received from outside the organization. These help recipients to identify the risk from each email and allows them to add senders to their allow and block lists with one click.

- Simple colored grading system allows the recipient to quickly identify how trustworthy a sender/email message is trustee sender (green), unknown (yellow), untrusted (orange)
- Grading based on sender checks performed by Sophos Email, including SPF, DKIM, DMARC, and header anomaly analysis
- Improves the end users experience by allowing them to update their personalized allow and block sender lists from within the email itself

Connected email security

Synchronized Security takes Sophos Email beyond the benefit of unified management in Sophos Central, creating new ways to connect email security with endpoint and Phish Threat end user security training to respond to risks inside your organization:

Compromised mailbox detection

Link Sophos Email and Sophos Endpoint to automatically detect and clean up infected computers sending outbound spam and viruses.

Watch the video

Thanks to its shared user list, Sophos Central is now able to link mailboxes protected by Sophos Email with the associated computers protected by Sophos Endpoint security. Once linked, if Sophos Email detects five or more spam or virus emails sent in 10 minutes, the mailbox is automatically blocked while an endpoint scan is carried out and the infection removed, and alerts shared via Sophos Central.

Sophos Central products required: Sophos Email Standard or Advanced and Sophos Endpoint

Identify and train at-risk users

Link Sophos Email and Phish Threat to identify risky user behavior and launch targeted security awareness training.

Watch the video

The new Sophos Email Advanced 'At Risk Users' report highlights exactly which users are clicking email links re-written by Time-of-Click URL protection. This identifies users who have either been warned or blocked from visiting a website due to its risk profile. You're then simply one click from the report to enroll users in Phish Threat simulations and security awareness training, increasing their threat awareness and reducing risk.

Sophos Central products required: Sophos Email Advanced and Sophos Phish Threat.

19-12-26 NA (PC)

SOPHOS