

Sophos Email Security for M365

Mar 2023

SOPHOS

Optimized for Microsoft 365



Setup Faster

Utilize Mailflow rules to enforce in/outbound
Sophos protection

Tap directly into the flow of messages for
faster processing time on all email



Protect Sooner

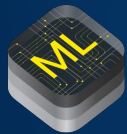
Mailflow rules connection is completed in
minutes all from Sophos Central

No delays on protection or need for MX
record redirections

Smarter Email Security

Sophos Email

- Optimized for organization who value simplicity, without compromising security
- Protect sensitive data while staying safe from spam, phishing attacks and malware, including the latest ransomware



Predictive email security
with AI

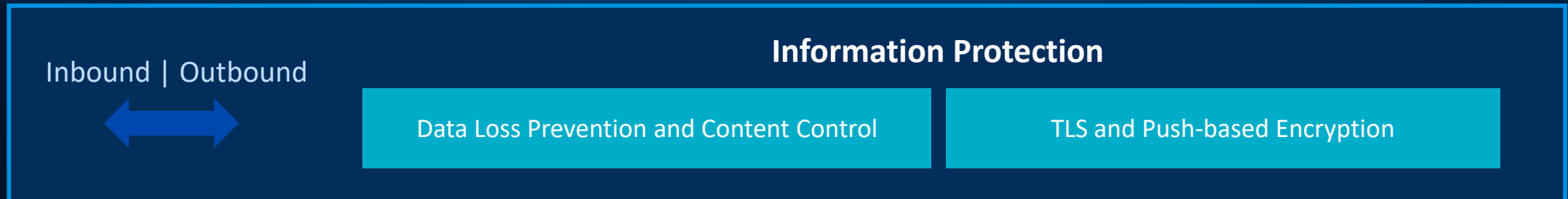
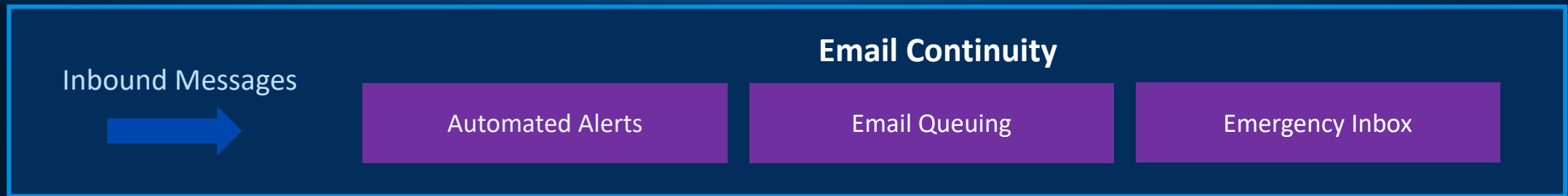
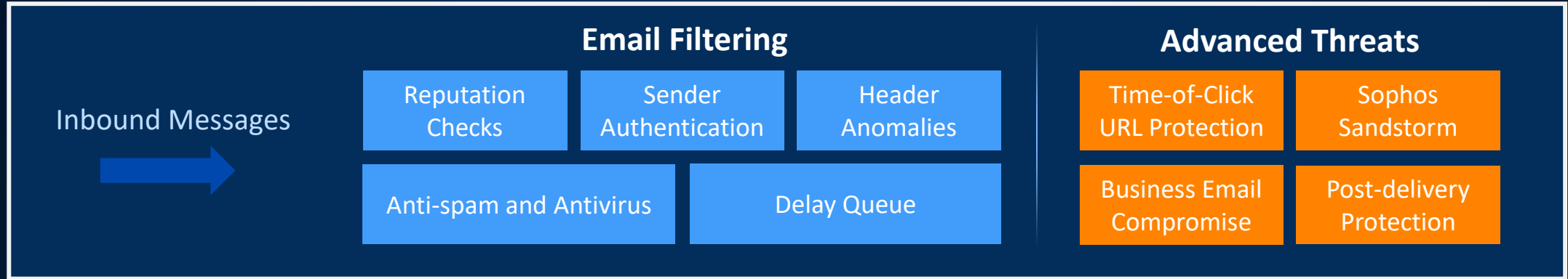


Protect Sensitive Data



Protection from
phishing fraud

Sophos Email – All in One Protection






Pre-Delivery

Smarter Sandboxing for Improved Performance

SophosLabs Intelix accurately pre-filters files to ensure high performance, with detonation focused on unknown, suspicious files



Example criteria for unknown files detonations

-  Windows EXE, 32-bit and 64-bit
-  Documents with macros
-  PDFs with scripts

Stopping Advanced Threats

Enhanced Behavioral Detection + Deep Learning

Ransomware

Stopped

10% More

EXE Malware Stopped

File Submission



- Detect suspicious files
- Pick execution environment

Attack Replay



- Event logging
- Payload extraction
- Anti-evasion

Behavior Analysis



- CryptoGuard and WipeGuard
- Rules and Patterns
- Event correlations

Deep Learning Analysis

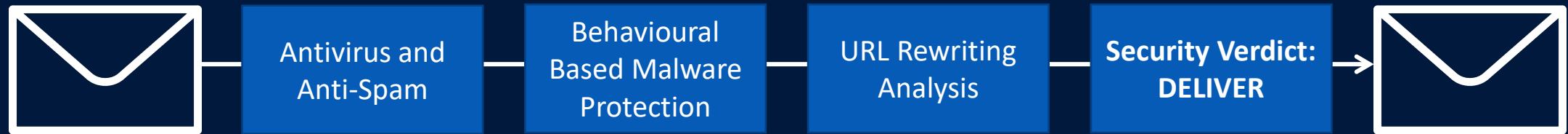


- Detect unknown executable threats
- Continuously adaptive learning model

SophosLabs Intelix

Advanced Threats Bypassing SEGs

Phishing Protection



These Attacks Are...

- Low volume, unique, non-spam
No bulk signatures or rate limits
- Sent from reputable IP addresses
No IP reputation block
- Containing zero (or clean) attachments
Nothing for a sandbox, or have evaded sandbox
- Containing zero (or clean) URLs
Nothing to rewrite or block, or have evaded analysis

Vulnerable to Identity Deception

Phishing Protection

50%

Display name Deception (Brand)

From: Chase Support <chase@gmail.com>
To: Tom Frost <ffrost@amazon.com>
Subject: Account Disabled

17%

Look-alike Domain

From: LinkedIn <noreply@liinkedin.com>
To: Jan Bird <jan.bird@gs.com>
Subject: Diana has endorsed you!

Advanced Attacks

By Imposter Type

13%

Display Name Deception (Individual)

From: Ravi Khatod <Ravi Khatod [hackjoe@gmail.com]>
To: Cong Ho <cong@Sophos.com>
Subject: Follow up on Invoice Payment

20%

Compromised Account

From: Raymond Lim <rlim@contoso.com>
To: Cong Ho <Cho@contoso.com>
Subject: PO 382313

Phishing Protection: Business Email Compromise

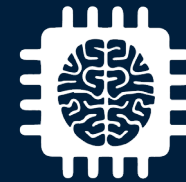


Impersonation Protection

VIP and brand - display name analysis

Policy wizards identify VIPs from AD roles

Smart banners alert email recipients



AI-Powered Content Analysis

Identifies conversations with suspicious tone and wording

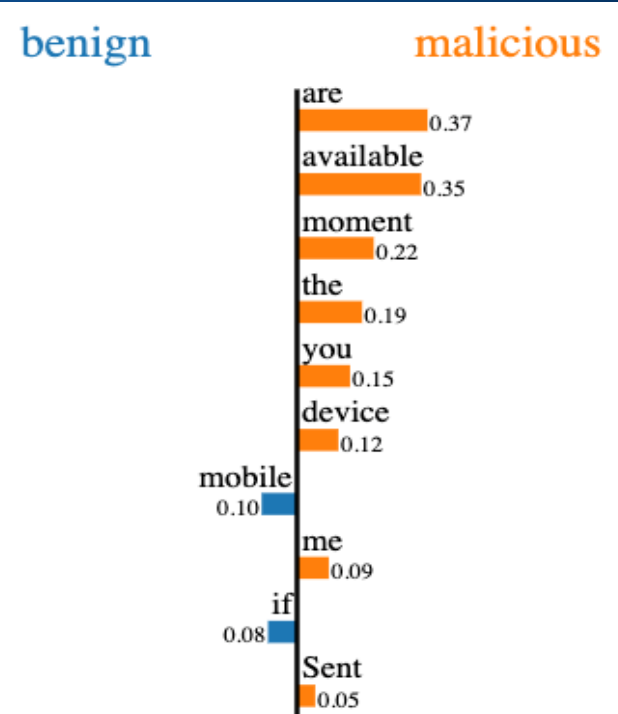
Scans body content and subject lines

How SophosAI models stops BEC scams

- State-of-the-art Natural Language Processing (NLP) models
- Understand words *in context* rather than individually
- Extract notions like “urgency” and “asking for something”
- Combine with email attributes including domain and recipient list
- **April 2021, non-English language enhancements**

Text with highlighted words

Let me know if you are available at the moment?
Sent from my mobile device



Post-Delivery

Post-Delivery Protection



Endpoint Integration

Identifies Compromised Mailboxes

Automated mailbox isolation

Cleans all known associated devices

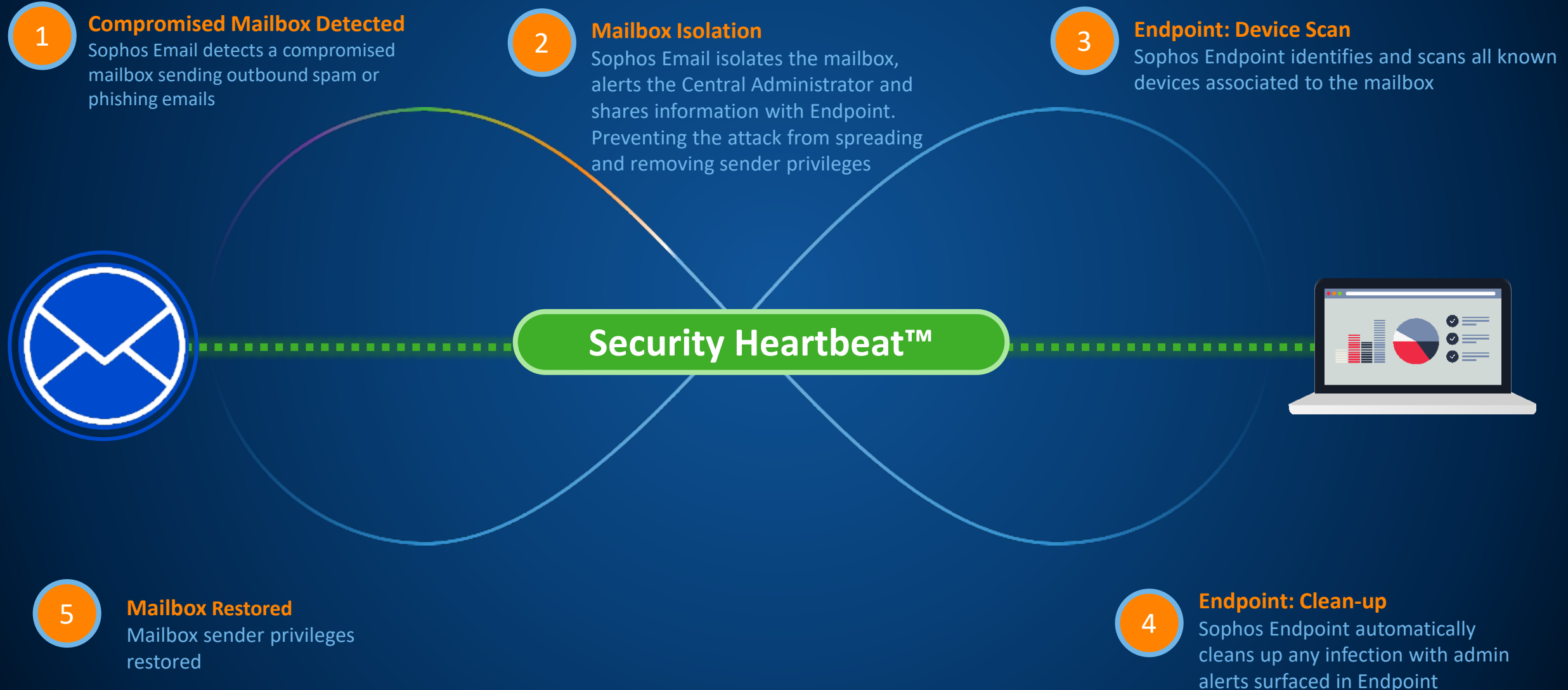


Post-delivery Protection

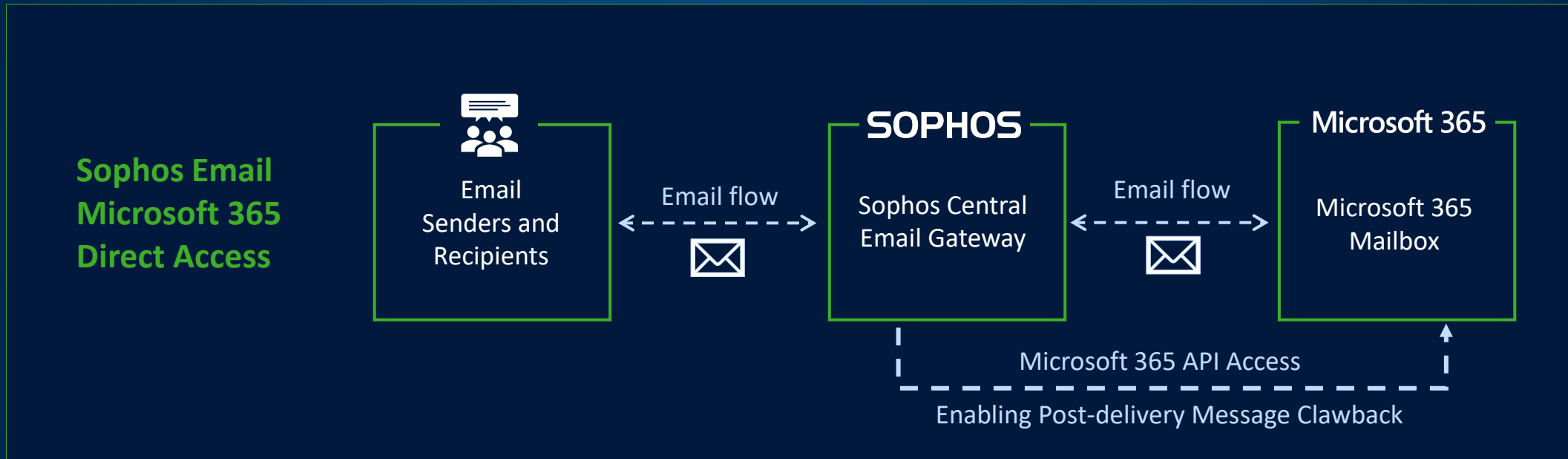
Uses Microsoft 365 APIs to
directly access mailboxes

Identify and automatically remove
malicious messages

Compromised Mailbox Detection



Microsoft 365 Direct Access



Data Protection

SOPHOS

Information Protection: Email Encryption and DLP



DLP Optimized for Simplicity

Detects PII, financial, confidential, health information

Out of the box or custom CCLs

Policy wizards define up to 50 rules



Analyze Email Content

Analyze subject, body and attachments

Stop hidden malware

Encrypt based on DLP rules



Policy Driven Encryption

Pushed-based encryption for entire email or attachments only

Full portal-based pull encryption

TLS and S/MIME

Single Console, Simplified Management

Encryption Overview



TLS Encryption

Prevent eavesdropping and tampering with the messages in transit.



Push-based Encryption

Send encrypted emails and attachments as password protected documents direct to the user's inbox. Includes Secure Messaging Portal for secure replies.



Full Portal-based pull Encryption

Manage encrypted messages entirely from the Secure Message portal. Enabling recipients to send, read, reply and add attachments securely.



S/MIME Email-Signing & Encryption

Encrypt email messages and add a digital signature to safeguard against email spoofing by verifying the sender's identity.

Managed Detection and Response (MDR)

A fully-managed, 24/7 service delivered by experts who specialize in detecting and responding to cyberattacks that technology solutions alone cannot prevent

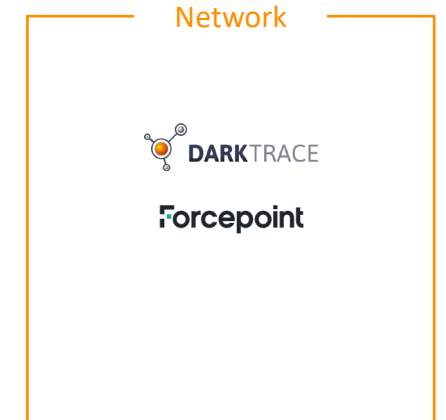
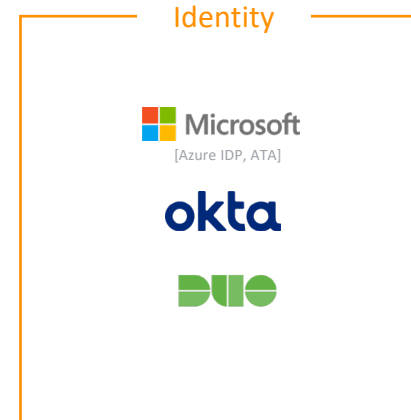
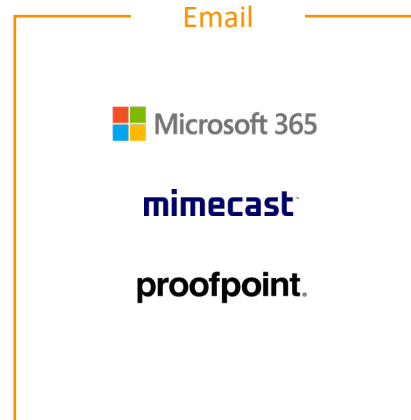
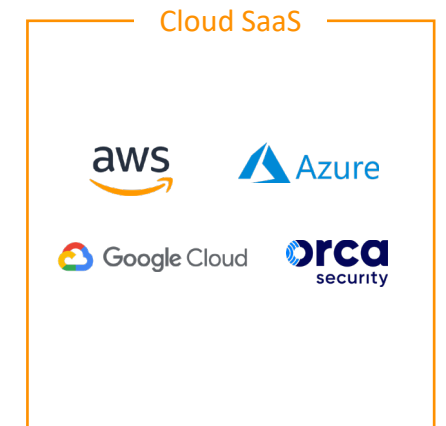


Sophos MDR

Managed Detection and Response for Any Environment

Delivered using **natively integrated XDR...**

...or through highly compatible **hybrid XDR**



Sophos MDR Included Integrations



Sophos XDR

The only XDR platform that combines native endpoint, server, firewall, cloud, email, mobile, and Microsoft integrations

Included in Sophos MDR and Sophos MDR Complete Pricing



Sophos Firewall

Monitor and filter incoming and outgoing network traffic to stop advanced threats before they have a chance to cause harm

Product sold separately; integrated at no additional charge



Microsoft Graph Security

- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Identity
- Identity Protection (Azure AD)
- Microsoft Azure Sentinel
- Office 365 Security and Compliance Center
- Azure Information Protection



Sophos Endpoint Protection

Block advanced threats and detect malicious behaviors—including attackers mimicking legitimate users

Included in Sophos MDR and Sophos MDR Complete Pricing



Sophos Email

Protect your inbox from malware and benefit from advanced AI that stops targeted impersonation and phishing attacks

Product sold separately; integrated at no additional charge



Office 365 Management Activity

Provides information on user, admin, system, and policy actions and events from Office 365 and Azure Active Directory activity logs



Sophos Cloud

Stop cloud breaches and gain visibility across your critical cloud services, including AWS, Azure, and Google Cloud Platform

Product sold separately; integrated at no additional charge



90-Days Data Retention

Retains data from all Sophos products and any third-party (non-Sophos) products in the Sophos Data Lake



Third-Party Endpoint Protection

Compatible with...

- Microsoft
- CrowdStrike
- SentinelOne
- Trend Micro
- Trellix
- BlackBerry (Cylance)
- Symantec (Broadcom)
- Malwarebytes

SOPHOS
Cybersecurity evolved.