



# Sophos Email

## Product and Licensing Overview

License	Feature Description	Sophos Email Standard	Sophos Email Advanced
<b>Setup and Management</b>			
Microsoft and Google compatible	<p>Compatible with the following leading email service provider platforms to provide advanced email security:</p> <ul style="list-style-type: none"> <li>• Microsoft Exchange Online and Microsoft Office 365</li> <li>• Microsoft Exchange 2003 or later</li> <li>• G Suite from Google Cloud</li> </ul> <p>Support is not limited to these platforms - a simple MX configuration is all that's required and Sophos Email is compatible with any service where you own the domain and control the associate DNS records.</p>	✓	✓
Sophos Central cloud management and reporting	<p>Sophos Email protects and manages your email in the cloud through Sophos Central.</p> <p>Browser requirements for Sophos Central management interface:</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 11</li> <li>• Microsoft Edge</li> <li>• Google Chrome</li> <li>• Mozilla Firefox</li> <li>• Apple Safari</li> </ul>	✓	✓
Active Directory Sync and Azure Active Directory Sync	<p>Microsoft Active Directory Sync (AD Sync) and Azure AD Sync gives organizations a simple way to move on premise Active Directory or Exchange environments to the cloud.</p> <ul style="list-style-type: none"> <li>• Keep users automatically sync'd with Sophos Email using AD Sync</li> <li>• Full support of automatic updating of AD data where businesses have completely moved to the cloud</li> </ul>	✓	✓
Manually enter alias records	Administrator access to manually add email address alias records when Active Directory is unavailable	✓	✓
Self-service portal for end users	<p>Sophos Email provides your end users with access to the following tools:</p> <ul style="list-style-type: none"> <li>• Manage quarantined emails (accept/delete emails)</li> <li>• Edit allow/block list rules</li> <li>• View messages in the event of an outage using the emergency inbox</li> </ul>	✓	✓
Domain / Group / User policies	Create unique email security policies for individuals, groups or the whole domain can be done in minutes.	✓	✓
Data center locations	<p>Meet data compliance regulations and improve end user experience with a choice of global data centers:</p> <ul style="list-style-type: none"> <li>• Ireland</li> <li>• United States</li> <li>• Germany</li> </ul>	✓	✓
<b>Business Continuity</b>			
Spooling ensures no mail is ever lost	In the event of a disruption to your Microsoft or Google Cloud email service the recipient's emails are automatically queued with Sophos Email, then delivered once service is restored (5 day retry period).	✓	✓
User access to 24/7 emergency inbox	Read access to queued email is provided from a 24/7 emergency inbox inside the end user portal.	✓	✓
Administrator alerts	In the event of third party cloud email service provider outages, alerts are provided when mail can't be delivered to a server/service.	✓	✓
<b>Security</b>			
Live threat updates stop the latest attacks	Powered by SophosLabs, Sophos Email provides live updates to protect against the latest threats.	✓	✓
Anti-spam, anti-virus and anti-phishing detection	<p>Inbound and outbound email filtering to block unwanted email:</p> <ul style="list-style-type: none"> <li>• Reputation filtering blocks 90% of spam</li> <li>• Our anti-spam engine that catches the rest, including the latest phishing attacks</li> <li>• Sender Genotype, our next-generation reputation filtering technology, eliminates botnet spam at the IP-connection level by monitoring connection requests and rejecting those showing evidence of botnet connections</li> <li>• Sophos Delay Queue provides protection against snow shoe spam</li> </ul>	✓	✓
Email quarantine	<p>Sophos Email's easy to use preset controls have your message quarantine policies setup and your business protected in seconds.</p> <p>The end user portal then lets users release mails on demand, and in-message quarantine digests provide a daily summary of quarantined mail, with the option to release direct from the inbox.</p>	✓	✓
Allow/Block lists	The end user portal allows users to setup allow and block lists.	✓	✓
SPF, DKIM and DMARC authentication	<ul style="list-style-type: none"> <li>• Sender Policy Framework (SPF) - to identify IP addresses authorized to send email from the domain.</li> <li>• Domain Keys Identified Mail (DKIM) - provides cryptographic proof that a messages was sent from a specific sender and hasn't been tampered with</li> <li>• Domain Message Authentication Reporting &amp; Conformance (DMARC) - determines what to do when messages fail SPF or DKIM checks from the sender</li> </ul>	✓	✓
Header anomaly checks	Header anomaly detection identifies if the sender display name is the same as an internal user name.	✓	✓
<b>Active Threat Protection (ATP)</b>			
Time-of-Click URL Protection	URL re-writing to check the website reputation of email links before delivery and at the time you click - blocking stealthy, delayed attacks.		✓
Sophos Sandstorm	Cloud-based Sandbox able to detect both known and unknown malware and unwanted applications before it executes		✓
Sophos Sandstorm data center locations	<p>Ensure compliance with a choice of location for email scanning and sandbox analysis:</p> <ul style="list-style-type: none"> <li>• Ireland</li> <li>• United States</li> <li>• Japan</li> </ul>		✓