OVERVIEW

Professional Services for Sophos Central Products

SOPHOS

Table of contents

Sophos Services Subscription

Sophos Professional Services can be purchased via the Sophos Services Subscription. The subscription is a flexible, value-driven offering designed to meet customers' evolving needs for Sophos Professional Services. Powered by Sophos Service Units (SSUs), it allows you to redeem units for the services you need when you need them. Whether you need to solve urgent issues, deliver complex projects, or receive strategic advice, the subscription helps you move faster, stay secure, and adapt as your business evolves.

For a full list of the Sophos Professional Services redeemable with SSUs, download the catalog of services.

Sophos Endpoint /Sophos XDR/ Sophos MDR implementation (1-250 users)

This Central CIXA/XDR/MDR Implementation service is intended for organizations with a single location and basic requirements for Sophos Endpoint protection. The Professional Services engineer will assist with the deployment of the Sophos Central client software and provide basic guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Endpoint/Server security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Endpoint /Sophos XDR/Sophos MDR implementation engagement.

Activities

Activation of Sophos Central License(s)

Sophos Endpoint deployment planning
- Competitor removal review/testing
  - 1 product version
- Devise installation process
  - GPO, 3rd party tools (e.g., SCCM, PDQ, etc.)
- Review installation logs
- Deployment testing (up to 5 devices)

Sophos Endpoint Agent GUI
- Tamper Protection
- Events/Logging
- Self-Help

Knowledge transfer and configuration of Endpoint/Server Base Policies
- Threat Protection
  - Defining Exclusions
- Peripheral Control
- Web Control

Logs and Reports
- Events
- Custom Reports
- Scheduling
- Audit Logs

Review/Implement Active Directory Synchronization

Communicating with Sophos Technical Support
- Gathering Diagnose logs

Q&A (as time permits)

Product code:
PCBZTCCAA

SKU:
PRPCBA00ZZPCAA

SSU value:
1

Implementation process

We begin with a 1-hour planning/kick-off meeting to review the technical requirements and pre-requisites to prepare for the implementation.

Sophos Endpoint /Sophos XDR/ Sophos MDR implementation (251-1000 users)

This implementation service is intended for organizations with diverse operational requirements including but not limited to integration with a SIEM solution and configuring Update Cache/Message relays. The Professional Services engineer will assist with the deployment of Sophos Central client software and provide guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Endpoint/Server security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Endpoint /Sophos XDR/Sophos MDR implementation engagement.

Activities

Activation of Sophos Central License(s)

Sophos Endpoint deployment planning
- Competitor removal review/testing
  - Up to 4 products/versions
- Devise installation process
  - GPO, 3rd party tools (e.g., SCCM, PDQ, etc.)
- Review installation logs
- Deployment testing (up to 10 devices)

Sophos Endpoint Agent GUI
- Tamper Protection
- Events/Logging
- Self-Help

Review and configuration of up to 2 each of the following policies
- Threat Protection
  - Defining Exclusions
- Peripheral Control
- Application Control
- Web Control
- Update Management
- Windows Firewall

Overview of Server Lockdown and File Integrity Monitoring Concepts

Logs and Reports
- Events
- Custom Reports
- Scheduling
- Audit Logs

Threat Cases
- Live Discover

Review/Implement Active Directory Synchronization

Installation of up to 2 Update Cache/Message Relay

Sophos Central Alerting
- Configuration of Email Alerting

API Token Management for SEIM Integration

Communicating with Sophos Technical Support
- Gathering Diagnose logs

Continued deployment assistance to Endpoints/Servers during the engagement

The number of devices deployed is wholly dependent on the customer

Q&A (as time permits)

Product code:
PCDZTCCAA

SKU:
PRPCDZ00ZZPCAA

SSU value:
2

Implementation process

We begin with a 1-hour planning/kick-off meeting to review the technical requirements and pre-requisites to prepare for the implementation.

SOPHOS

Sophos Endpoint /Sophos XDR/ Sophos MDR implementation (1001-5000 users)

This implementation service is intended for larger organizations with more complex network and operational requirements. The Professional Services engineer will assist with the enablement of Enterprise Dashboard and the deployment of the Sophos Central client software and provide guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Endpoint security solution in an enterprise environment.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Endpoint /Sophos XDR/Sophos MDR implementation engagement.

Activities

Activation of Sophos Central License(s)
- Activation of Enterprise Dashboard and Enablement of Master Licensing (if required)

Enterprise Dashboard Configuration/Review
- Enterprise Installer vs. Sub-estate Installer
- Enterprise Administration Roles
- Global Templates Concepts

Sophos Endpoint deployment planning
- Competitor removal review/testing (up to 5 products/versions)
- Devise installation process
- Review installation logs
- Deployment testing (up to 20 devices)
- Disk Imaging for VDI

Review and configuration of up to 2 each of the following policies
- Threat Protection
  - Defining Exclusions
- Peripheral Control
- Application Control
- Web Control
- Windows Firewall

Policy Assignment - Device vs. User

Logs and Reports
- Events
- Custom Reports
- Scheduling
- Audit Logs

Threat Cases
- Live Discover

Endpoint/Server Agent GUI
- Tamper Protection
- Events/Logging
- Self-Help

Review/Implement Active Directory Synchronization

Installation of up to 2 Update Cache/Message Relay

Sophos Central Alerting
- Configuration of Email Alerting
- API Token Management for SIEM Integration
- Scheduling
- Audit Logs

Sophos Central Alerting
- Configuration of Email Alerting
- API Token Management for SEIM Integration

Communicating with Sophos Technical Support

Continued deployment assistance to Endpoints/Servers during the engagement
- The number of devices deployed is wholly dependent on the customer

Q&A (as time permits)

Product code:
PDXZTCCAA

SKU:
PRPDXA00ZZPCAA

SSU value:
4

Implementation process

We begin with a 1-hour kick-off meeting to review the technical requirements and pre-requisites to prepare for the implementation. Our engineer will coordinate scheduling follow-up meetings for the configuration and implementation during the kick-off call.

SOPHOS

Sophos Email implementation

This service is intended for organizations with 1 (one) email tenant and up to 5 (five) email domains. Additional email tenants and/or domains may require the purchase of supplementary services time.

The Professional Services engineer will assist with the configuration, knowledge transfer, guidance, and assistance with the cutover from your current solution. This will ensure a successful cutover to Sophos Central Email and enable your IT staff to become familiar with the key concepts in the configuration and management of the Sophos solution.

The following outlines the tasks and knowledge transfer that will be completed during the Sophos Email implementation.

Activities

Activation of Sophos Central License(s)

Sophos Email Gateway deployment planning

- Review current email rules
  - Block/Allow lists
  - Approved URLs
  - VIP management

Review/implement Active Directory/ Azure AD synchronizations/versions)

- Or import users/distribution lists from other sources

Configuration

- Sophos Email Security Policies
  - SPAM
  - Banners
  - Quarantine/ User Self-Help
  - Sender checks
  - Malware Scanning
  - Time-of-click
  - VIP Management
- Data Loss Prevention Policies
  - Attachment/Keyword handling
  - Email Encryption
  - Built-in templates

Cutover

- DNS changes (up to 5 domains/zones)
  - MX/SPF/DKIM records
- O365 modifications
  - Mail flow changes for inbound and outbound mail
- On-Premises Exchange
  - Connectors for inbound and outbound mail
- Other mail providers compatible with Sophos Email Gateway

Review Logs and Reporting

Communicating with Sophos Technical Support

Cutover Assistance

- Verify DNS records
- Verify mail flow and policies
- Verify Block/Allow lists
- Verify mail logs and quarantine items

Scheduled post-cutover assistance

- Next business day after cutover

Q&A (as time permits)

Product code:
PGBZTCCAA

SKU:
PRPGBA00ZZPCAA

SSU value:
2

Implementation process

We begin with a 1-hour planning/kick-off meeting to review the technical requirements and pre-requisites to prepare for the implementation.

The engineer will coordinate follow-up meetings during the initial call for the configuration, cutover and a post-cutover call.

NOTE: If you have more than 5 email domains/zones, additional services hours may be required to complete your implementation.

Sophos Mobile implementation

The Professional Services engineer will assist with the deployment of Sophos Mobile client software and provide guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts and advanced features in the configuration and management of the Sophos Mobile security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Mobile Implementation engagement.

Activities

Activation of Sophos Central License(s)

Device Configuration
- Apple iOS
- Apple OSX
- Android
- Chrome
- Windows

Policy Creation and Assignments/version(s)
- User
- Device
- Compliance

Configure Sophos Mobile Email access

Configure EAS Proxy

Application Deployment
- App Groups

Sophos Mobile Threat Defense
- 3rd party integrations (e.g. InTune, Airwatch, etc.)

Logs and Reports
- Events
- Custom Reports
- Scheduling
- Audit Logs

Deployment testing
- Up to 10 devices

Sophos Mobile Control Agent GUI

Review/Implement Active Directory Synchronization

Sophos Central Alerting
- Configuration of Email Alerting

Communicating with Sophos Technical Support
- Gathering Diagnose logs

Q&A (as time permits)

Product code:
PD2ZTCCAA

SKU:
PRPD2A00ZZPCAA

SSU value:
2

Implementation process

We begin with a 1-hour kick-off meeting to review the technical requirements and pre-requisites to prepare for the implementation. Our engineer will coordinate scheduling follow-up meetings for the configuration and implementation during the kick-off call.

Sophos Device Encryption implementation

The Professional Services engineer will assist with the deployment of the Sophos Central Device Encryption client software and provide guidance and knowledge transfer. This enables your IT staff to become familiar with the key concepts in the configuration and management of the Sophos Central Device Encryption security solution.

The following is an outline of the tasks and knowledge transfer that may be completed during a Sophos Central Device Encryption Implementation engagement.

Activities

Activation of Sophos Central License(s)

Review and configuration of up to 2 Sophos Device Encryption policies

Policy Assignments/versions)

Sophos Endpoint deployment planning

- Review process for migration from current product
- Review Bitlocker requirements on Endpoints
- Review Group Policy Objects for Bitlocker
- Devise installation process
  - Review setup of software deployment via GPO or 3rd party tools
  - Provide installation script
- Review installation logs
- Deployment testing
  - Up to 5 devices

Sophos Endpoint Recovery Procedures

- Retrieve Recovery Key
- Change Bitlocker Authentication Passcode

Sophos Endpoint Agent GUI

- Tamper Protection
- Events/Logging
- Self-Help

Logs and Reports

- Events
- Custom Reports
- Scheduling
- Audit Logs

Communicating with Sophos Technical Support

- Gathering Diagnose logs

Q&A (as time permits)

Product code:

PD2ZTCCAA

SKU:

PRPD2A00ZZPCAA

SSU value:

1

Implementation process

We begin with a 1-hour kick-off meeting to review the technical requirements and pre-requisites to prepare for the implementation. Our engineer will coordinate scheduling follow-up meetings for the configuration and implementation during the kick-off call.

Sophos Endpoint solution review

The purpose of the Sophos Endpoint Solution Review is to assess the current Sophos Endpoint policies and provide recommendations to help improve your organization's security posture using Sophos Central. The delivery time consists of a remote teleconference meeting of approximately 2 hours. After the meeting, the engineer will compile the results and provide documentation within 2 business days.

The goal is to understand, document, and advise on your current configuration. It is not intended to perform troubleshooting or impact any immediate changes to the environment or resolve open issues.

Global Settings

- General
  - Role Management
  - API Credentials
  - Tamper Protection
  - Website Management
  - Global Exclusions
  - Allowed Applications
  - Manage Update Caches and Message Relays
  - HTTPS Updating
  - Configure email alerts
- Sophos Endpoint Protection
  - Controlled Updates
  - SSL/TLS decryption of HTTPS websites
  - Data Lake uploads (Sophos XDR only)
- Server Protection
  - Controlled Updates
  - Data Lake uploads (Sophos XDR only)

Sophos Endpoint Policies (up to 2 of each policy type)

- Sophos Endpoint Threat Protection
  - Exclusions
- Peripheral Control
- Web Control
- Update Management

Server Policies (up to 2 of each policy type)

- Server Threat Protection
  - Exclusions
- Peripheral Control
- Web Control
- Update Management
- File Integrity Monitoring

Product code:

PH4ZTCCEP

SKU:

PRPH4E00ZZPCAA

SSU value:

1

Security posture assessment

Product code:
PCAZ3CCAA

SKU:
PCAZ3C00ZZPCAA

SSU value:
2

The goal is to understand and advise on your current security posture and is not intended to perform troubleshooting or impact any immediate changes to the environment or resolve open issues. The Security Posture Assessment begins with a conference call and remote screen sharing session which may last up to 4 hours. The following will be performed during the meeting and documentation will be provided within 10 business days.

Activities

Sophos Central Health Check

Our Health Check of your Central environment is designed to make sure you follow our best practices, ensuring you get the most out of our endpoint solution. The engineer will review and provide guidance on the following:

Global Settings

- General
  - Tamper Protection
  - Global Exclusions
  - HTTPS Updating
  - Multi-factor Authentication (MFA)
- Sophos Endpoint Protection
  - Controlled Updates
- Server Protection
  - Manage Update Caches and Message Relays
  - Controlled Updates

Sophos Endpoint Policies (up to 2 of each policy type)

- Sophos Endpoint Threat Protection
- Peripheral Control
- Web Control

Server Policies (up to 2 of each policy type)

- Server Threat Protection
- Peripheral Control
- Web Control
- File Integrity Monitoring

NIST assessment

The NIST Cyber Security Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. Completing the assessment will provide you with a report giving insight into your organization's current maturity. You will have actionable recommendations to improve your security posture.

EASM and dark web scanning

The final task we will perform is an external device discovery scan, locating systems that are available on the public internet. We will complete vulnerability scans on these devices to assess if they are susceptible to attack. Finally, we will look to see if any of your corporate information can be found on the Dark Web.

SOPHOS

To learn more please contact your Sophos representative or visit: sophos.com/professional-services

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Updated November 2025