Active Directory Security Assessment – Service Description

This Service Description describes Active Directory Security Assessment ("**Service**"). All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined below).

This Service Description is part of and incorporated into, as applicable: (i) Customer's manually or digitally-signed agreement with Sophos covering the purchase of a Service subscription; (ii) if no such signed agreement exists, then this Service Description will be governed by the terms of the Sophos End User Terms of Use posted at https://www.sophos.com/legal (collectively referred to as the "**Agreement**"). To the extent there is a conflict between the terms and conditions of the Agreement and this Service Description, the terms and conditions of this Service Description will take precedence.

Notwithstanding anything to the contrary in the Agreement, Customer acknowledges and agrees that: (i) Sophos may modify or update the Service from time to time without materially reducing or degrading its overall functionality; and (ii) Sophos may modify or update this Service Description at any time to accurately reflect the Service being provided, and any updated Service Description will become effective upon posting to https://www.sophos.com/legal.

1.1 Overview

Sophos will provide Customer with an Active Directory Security Assessment (ADSA), which enables Customer to leverage the experience and insights of the Sophos Incident Response team to understand how attackers can exploit Active Directory misconfigurations and security control gaps to achieve their objectives. Customer can use the concise and actionable report created from the assessment to implement a best-practice Active Directory management model that helps remove current and future attack paths within the environment that attackers can exploit.

1.2 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Sophos to perform the Service is contingent upon the following:

- Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Sophos, to permit Sophos to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.
- For on-site activities, Customer will provide a suitable workspace for Sophos personnel, and necessary access to systems, network, and devices.
- Replies to all requests are prompt and in accordance with the delivery dates established between the parties.
- Customer's scheduled interruptions and maintenance intervals allow adequate time for Sophos to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Sophos testing activities as needed, to prevent disruption to Sophos business and performance of the Service (e.g., takedown requests, ISP deny list).
- Customer will provide to Sophos all required information (key personnel contact information, credentials, and related information) at least two (2) weeks before initiating the Service.

1.3 Scheduling

Sophos will contact a Customer-designated representative within five (5) business days after the execution of an Agreement to begin the Service Initiation activities described herein. These activities will ensure effective and efficient use of the Service.

Sophos will use commercially reasonable efforts to meet Customer's requests for dates and times to deliver the Service(s), taking into consideration Customer-designated downtime windows, Customer deliverable deadlines, and other Customer scheduling requests. Written confirmation of an agreed-upon schedule shall constitute formal acceptance of such schedule.

Once scheduling of any on-site work at Customer facility has been mutually agreed to, any changes by Customer to the on-site work within two (2) weeks of the on-site work to be performed will incur a $2,000 re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by Sophos.

1.4 Timeline

- On-site work will be performed Monday – Friday, 09:00 – 17:00 Customer's local time or similar daytime working hours.
- Remote work will occur Monday – Friday, 09:00 – 17:00 Customer's local time or similar daytime working hours.
- Work performed outside of the hours listed above, as requested or required by Customer, will incur additional service charges.

2 Service Details

The subsections below contain details about the Service and how it will be initiated.

2.1 Service Initiation

Prior to initiating the Service, Sophos will contact Customer's designated point of contact to gather information and understand Customer goals and expectations.

2.2 Service Scope

The Service is available in the following scopes:

- Small Active Directory Assessment: One (1) Active Directory Assessment, up to two (2) Active Directory domains
- Medium Active Directory Assessment: One (1) Active Directory Assessment, up to five (5) Active Directory domains
- Large Active Directory Assessment: One (1) Active Directory Assessment, up to ten (10) Active Directory domains

The Sophos team will execute the scope per requirements as outlined in an Agreement.

2.3 Service Methodology

During the Service, Sophos uses configuration review toolsets and interviews with Customer personnel to identify Active Directory configuration management practices and relevant cybersecurity controls. Sophos provides step-by-step instructions for Customer to collect the Active Directory configuration data required to perform the technical assessment. Sophos does not require interactive access to Customer IT environment.

Sophos may examine the following:

- Best practices
- Administrative model and delegation of administration
- Service principal names
- Management of group policies
- Attack vectors
- Shortest path to Domain Administrator
- Protected groups and overprivileged objects
- End of Life operating systems
- Domain trusts
- Kerberoastable accounts
- Unconstrained delegation

The Service is delivered in the following phases: data collection phase, the assessment phase, and a debrief.

Data Collection

The evaluation necessitates that Customer gathers from the Active Directory or Directories within the defined scope. Sophos will provide detailed instructions on how to collect the data using PowerShell. The rationale behind utilizing a virtual machine is to avoid any persistent trace of the data collection in the environment that could be later detected by Endpoint Detection and Response (EDR) systems.

While it is possible to perform data collection without a domain admin account, given the security-focused nature of this assessment, Sophos aim is to obtain the most precise data possible. With a domain admin account, Sophos can accurately associate the sessions within the domain with the respective accounts, thus ensuring the highest level of data accuracy.

Following the completion of the assessment, the virtual machine and the domain admin account should be promptly deleted to eliminate any potential evidence remnants.

Assessment

Upon receipt of the data during the data collection phase, Sophos will commence the data analysis and report generation process. Customer does not need to take any further actions during this phase of the assessment.

The timeline for analyzing Active Directory data is inherently difficult to predict due to the distinctive characteristics of each Active Directory environment. It is noteworthy that a smaller Active Directory may require more time for analysis than a considerably larger one, depending on historical configuration decisions over its lifecycle.

The analysis and report completion process spans a duration of three (3) to six (6) weeks.

Debrief

After Sophos establishes a timeframe for report completion, our consultant will initiate contact with the designated point of contact to coordinate a debriefing session. In this session, Sophos will thoroughly review each finding and offer the Customer an opportunity to seek clarification on the findings' nature and the required remediation steps.

The duration of the debriefing session lasts up to two (2) hours, contingent upon the volume of findings within the domain and the number of related questions.

2.4 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

2.4.1 Delivery Coordination

Sophos will provide coordination for the Service(s) with appropriate communication and updates to the stakeholder community. The coordinator will oversee logistics for people, processes, and tools as well as timeline and meeting facilitation.

The scope of delivery coordination includes the following:

- Develop delivery timeline with Customer and with Sophos personnel.
- Work with Customer to identify and address issues or concerns that impact service delivery.
- Periodic, high-level updates on progress.
- Confirm delivery and procure project sign-off.

Services will be delivered from Customer's site(s) and/or remotely from a secure location. Sophos and Customer will determine the location of the service(s) to be performed herein.

Sophos solely reserves the right to refuse to travel to locations deemed unsafe by Sophos or locations that would require a forced intellectual property transfer by Sophos. Sophos solely reserves the right to require a physical security escort at additional Customer expense to locations that are deemed unsafe by Sophos. Customer will be notified at the time that services are requested if Sophos refuses to travel or if additional physical security is required, and Customer must approve the additional expense before Sophos travel is arranged. In the event any quarantines, restrictions, or measures imposed by governmental authority or Sophos restrict travel to any location, Sophos may at its election (i) deliver the Services remotely or (ii) postpone the Services until travel is permitted. If neither option (i) nor (ii) in the preceding sentence is feasible, Sophos may terminate the affected Services and provide Customer with a refund of any unused, prepaid fees.

2.5 Deliverables

Listed in the tables below are the standard deliverables for the Service. Sophos will work with Customer to determine appropriate specific deliverables, delivery method, and cadence.

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Active Directory Security Assessment	Debrief Session	Mutually agreed upon	Conference call
Active Directory Security Assessment	Final Report	Mutually agreed upon	Mutually agreed upon

Once the technical assessment is complete, Sophos will deliver a final report ("Final Report") to the Customer designated point of contact. The report will include:

- Practical recommendations to rectify identified deficiencies.
- Recommendations for further strengthening Active Directory security, based on Sophos and industry-accepted practices for securing Active Directory.
- Identification of design flaws and vulnerable configuration.
- Risk-prioritized action items and remediation guidance that includes levels of effort to implement.

Customer shall have one (1) week from delivery of the report to provide comments to be included in the final report. If there are no comments received from Customer before the expiration of the review period, the report will be deemed final.

Sophos will also schedule with Customer an online conference call (“Debrief Session”) to present the findings and recommendations.

Upon completion of the Service, the Customer-designated contact will receive a secure/encrypted email confirmation from Sophos. Unless otherwise notified in writing to the contrary by the Customer designated contact, within five (5) business days of such email confirmation, Service shall be deemed complete.

2.6 Out of Scope

The information in Section 2 comprises the Sophos standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Upon request, Sophos can provide out-of-scope technical support on a time and materials basis pursuant to a separate Agreement. Sophos reserves the right to decline requests that:

- Are beyond the scope of the Service(s) described herein
- Are beyond the capability of Sophos to deliver within the contracted service levels
- Might violate legal or regulatory requirements.

3 Service Fees and Related Information

See Sophos applicable Agreement for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

3.1 Invoice Commencement

See the Service-specific Addendum incorporated herein by reference at https://www.sophos.com/legal/-terms, as updated from time to time (the “Product Terms Page”) or Agreement for information about invoice commencement. Provisions related to the term of the Service and payment terms within the Product Terms Page shall not apply to Customer’s consumption of Services in case of purchases through a Sophos’ reseller but instead shall be subject to Customer’s agreement with its reseller.

3.2 Expenses

Customer agrees to reimburse Sophos, directly or indirectly (in case of purchases through an authorized reseller), for all reasonable and actual expenses incurred in conjunction with delivery of the Service.

These expenses include but are not limited to the following:

- Travel fees related to transportation, meals, and lodging to perform the Services, including travel to Customer location(s)
- Digital media storage, specific equipment necessary for delivering the Service, or licensing necessary for tailored digital forensic analysis work.

- Monthly fees for other purchased infrastructure to support service delivery (e.g., public cloud computing services) may apply, if Customer and Sophos agree that usage is necessary to complete Service delivery.

3.3 Term

The term of the Service is defined in the Agreement. Service will expire according to the Agreement provided that, if there is currently an in-progress delivery of the Service at the time of expiration, then the term shall automatically extend and expire upon completion of such in-progress delivery of the Service. During such extended term (if applicable), the terms and conditions of the Agreement shall be in full force and effect.

4 Additional Terms

4.1 On-site Services

Notwithstanding Sophos' employees' placement at Customer's location(s), Sophos retains the right to control the work of such employees. For international travel, on-site Services may require additional documentation, such as visas, visitor invitations, and related documentation, which may affect timing of the Services and reimbursable expenses

4.2 Security Services

Customer acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding Customer's systems and accepts those risks and consequences. Customer hereby consents and authorizes Sophos to provide any or all of the Security Services with respect to Customer's systems. Customer further acknowledges that it is Customer's responsibility to restore network computer systems to a secure configuration after Sophos completes testing.

4.3 Record Retention

Sophos will retain a copy of the Customer Reports in accordance with Sophos' record retention policy. Unless Customer gives Sophos written notice to the contrary prior thereto and subject to the provisions of the applicable Agreement and DPA, all Customer Data collected during the Services and stored by Sophos will be deleted within 30 days from issuance of the final Customer Report. If Customer or its authorized agent requests that Sophos retain Customer Data for longer than its standard retention policy, Customer shall pay Sophos' costs and expenses associated with the extended retention and storage of such Customer Data. Notwithstanding the foregoing, Sophos shall be entitled to retain Customer Data as necessary to comply with its own legal, regulatory, judicial, audit, or internal compliance requirements.

4.4 Compliance Services

Customer understands that, although Sophos' Services may discuss or relate to legal issues, Sophos does not provide legal advice or services, none of such Services shall be deemed, construed as or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by Sophos in connection with any Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.

4.5 Post-Engagement Activities

Subject to any applicable legal or regulatory requirements, thirty (30) days after completing delivery of the Service, Sophos will commence with the appropriate media sanitization and/or destruction procedures of

the Customer acquired images, hard drives or other media obtained by Sophos in the performance of the Services hereunder (the "**Engagement Media**"), unless prior to such commencement, Customer has specified in writing to Sophos any special requirements for Sophos to return such Engagement Media (at Customer's sole expense). Upon Customer's request, Sophos will provide options for the transfer to Customer of Engagement Media and the related costs thereto. If so requested, Sophos will provide a confirmation letter to Customer addressing completion and scope of these post-engagement activities, in Sophos' standard form. Unless agreed to otherwise by the parties, and subject to any applicable legal or regulatory requirements, Sophos shall, in its sole discretion, dispose of the Engagement Media on or after the engagement conclusion and only maintain a copy of the completed engagement-specific deliverables.

4.6 Legal Proceedings

If Customer knows or has reason to believe that Sophos or its employees performing Services under this Service have or will become subject to any order or process of a court, administrative agency or governmental proceeding (e.g., subpoena to provide testimony or documents, search warrant, or discovery request), which will require Sophos or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify Sophos, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Sophos for (a) its employees' time spent as to such response, (b) its reasonable and actual attorneys' fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Nothing in this paragraph shall apply to any legal actions or proceedings between Customer and Sophos as to the Service.

4.7 Endpoint Assessment

Unless otherwise agreed upon in writing, if a software agent has been deployed as part of the Service, within thirty (30) days following the date of the Completed Final Report (the "**Thirty Day Period**"), Customer shall uninstall any and all copies of the software agent used for the Service. During the Thirty Day Period, (i) Customer shall not use the software agent, and (ii) the license and use restrictions that apply to the software agent remain in effect notwithstanding the expiration of termination of the Service. Customer will install Sophos' proprietary software agent if Endpoint Assessment Services are in scope. Customer (i) will use the Endpoint Assessment software agent for its internal security purposes, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the software agent; and (b) will not remove any language or designation indicating the confidential nature thereof or the proprietary rights of Sophos from the software agent. Customer will uninstall the software agent as described in this Service.