Web API Test – Service Description

This Service Description describes Web API Test Service ("**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

The test can be conducted on web APIs and/or web services, and includes analyzing the state of Customer's web API resources to identify vulnerabilities. To conduct the test, Sophos will use its methodology that is based on industry frameworks for application tests, which includes the Open Web Application Security Project ("OWASP") Testing Guide, Open-Source Security Testing Methodology Manual ("OSSTMM"), vendor-specific security documents, and the experience of Sophos team members.

1.2 Customer Obligations

Customer will perform the standard 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.
- This service is delivered remotely, but exceptions can be requested. Sophos will evaluate these requests, and if approved for on-site activities, Customer will provide a suitable workspace for Sophos personnel, and necessary access to systems, network, and devices. Sophos reserves the right to deny any and all on-site travel requests.
- 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.

The following Customer obligations are specific to the Web API Test:

- Upon commencement of the engagement, Customer will ensure that in-scope applications remain available and stable, and will not modify the applications in any way during the course of the

engagement. Should any modifications occur during the engagement, Sophos will not consider any changes during testing and reporting, and may require a change order and additional fees if modifications result in the need for testing be restarted.

- Customer will ensure that testing the in-scope application, in its configured state, is allowed through any third-party Terms of Service (e.g., AWS and Azure cloud services), especially cloud load-balancing services.

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.

If an exception for on-site work is approved, and 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

- Remote work will occur Monday – Friday, 8 a.m. – 6 p.m. US Eastern time.
- Approved on-site work will be performed Monday – Friday, 8 a.m. – 6 p.m. Customer's local time or similar daytime working hours.
- To simulate real-world threat actors, goal-based testing, such as Penetration Tests and Red Team Tests, can occur at any time, within the testing dates, at Sophos' discretion.
- 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

The rules of engagement for the assessment are established during scheduling and kickoff sessions. Topics to be covered include the following:

- Goals and objectives for the assessment
- Definition of scope and validation of targets
- Rules of engagement, levels of effort, and risk acceptance
- Testing timelines and schedules
- Reporting requirements, timelines and milestones
- Key personnel, roles and responsibilities, and emergency planning
- Sophos source Internet Protocol ("IP") address ranges, and tools and techniques

After completion of all staging tasks and the introductory meeting, Sophos will send a confirmation email to ensure agreement on these items.

A member of the Sophos' team will be involved between the kickoff call and the start of testing to aid the Customer in completing any pre-testing tasks. These tasks include collecting IP addresses / targets / scope, configuring any remote testing connectivity, and other mandatory pre-testing tasks.

2.2 Service Scope

The Web API Test is available in the following scopes:

- Small Web API Test: up to ten (15) methods for SOAP or up to fifteen (40) methods for REST
- Medium Web API Test: up to twenty (25) methods for SOAP or up to forty (60) methods for REST
- Large Web API Test: up to thirty (40) methods for SOAP or up to sixty (80) methods for REST

Total number of methods must be provider for each individual API to be assessed. The total number of methods can be calculated by first calculating the total number of endpoints (ex: /accounts/{accountId}) and then totaling the number of actions (i.e. HTTP Verbs) allowed on each endpoint (ex: GET, POST, PUT, DELETE). When providing the total number of methods, additionally providing the inclusive number of GET (i.e. read-only) methods may allow Sophos to increase the number of methods tested per Web API test since these methods typically require less effort in testing.

Sophos will conduct a web service test for the number of web application programming interfaces ("APIs") and/or web services defined in Customer's Agreement.

Sophos will conduct one (1) remediation validation ("RV") for only the high- and critical-severity findings listed in the final report.

After primary test completion, Customer has ninety (90) days in which to remediate issues, schedule the RV, and have Sophos perform the RV. Customer must submit the RV request through email to the Sophos point of contact for the assessment within thirty (30) days of delivery of the final report or the RV is forfeited.

Note: Sophos only conducts RVs remotely, regardless of whether the assessment was conducted on-site.

2.3 Service Methodology

Sophos will perform the following tasks during the Service.

Test User Accounts

Multiple user accounts are required to test what authorized users may accomplish, usually two authenticated user roles.

- Unauthenticated (anonymous) user
  - Access restricted resources that usually require authentication
  - Gain access to authenticated privileges or a user account
  - View other user/account data
- Authorized user
  - Elevate privileges to access internal or sensitive content
  - View other user/account data
  - Add/modify/delete other account data
  - Existing access is appropriate based upon role

Web API Test

Web API or Service Testing focuses on the following areas:

- Simple Object Access Protocol (“SOAP”)/XML structure tests
- Representational State Transfer (“REST”) / JavaScript Object Notation (“JSON”) parameter manipulation
- Input validation attacks
- Cross-site scripting attacks
- Cookie theft
- Web server insecurity
- Authentication method attacks
- Horizontal and vertical privilege escalation
- Third-party software vulnerabilities
- Database vulnerabilities

The subsections below explain the stages within the process that Sophos will use to test Customer’s web APIs and/or web services.

Dynamic Application Security Testing

Sophos will use Dynamic Application Security Testing (“DAST”), which helps detect security vulnerabilities in an application in Customer’s operational environment. DAST is generally used to refer to the testing of web applications, but the concept applies to the security testing of software in general.

DAST involves a comprehensive review of the target application's functionality, followed by probing of specific features using carefully manipulated input to identify security vulnerabilities. The security logic of the application is tested for insecure conditions and assumptions that have been built into the application that lead to vulnerabilities.

Reconnaissance

Reconnaissance allows the tester to understand the application and its normal use. This stage does not actively exploit any issues that may be apparent in the target application. Tasks and activities can include the following:

- Spidering
- Site mapping
- API documentation review
- Web Services Description Language (“WSDL”) analysis
- Swagger file analysis
- REST JavaScript API review

Automated Testing

Sophos will use automated testing to execute multiple tests in a minimal amount of time. Automated web application scanners are limited in their scope, but are effective for identifying the most common issues while saving significant amount of time during testing. Scanners can be configured to execute with or without valid credentials on the target API, and that choice has a major effect on the depth of testing. During automated testing, a network-level vulnerability scan of the web server will also be executed that aims to find exploitable weaknesses in the operating system of the server. Tasks and activities may include the following:

- Unauthenticated scan

- Authenticated scan
- Server vulnerability scan
- Content discovery scan

Results may include the following:

- Common vulnerabilities
- Injection points
- Misconfigurations
- Unlinked content

Manual Testing

Sophos will review any findings and perform manual testing as needed. Manual testing reduces the occurrence of 'false positives', improving the accuracy of testing results. Listed in the table below are tasks and activities that will be conducted as applicable.

Manual Testing Areas	Tasks and Activities
Verification and Automated Results	All automated scan results are manually verified to improve the accuracy of the findings.
Server Assessment	Application security is heavily dependent on the server itself. A weakness in the web or application server hosting the web service or API can compromise an otherwise secure application. This phase performs automated and manual attempts to discover known weaknesses or configuration issues in the web or application server software.
Injection Attacks	Injection attacks are generally regarded as the most critical of issues that web applications face and yet are very common. They include attack groups such as database (SQL) injection, Cross-Site Scripting (XSS), and command injection attacks. Should any of these flaws be discovered, a process of evaluating the real technical risk that they pose to the application, data, and users will be conducted.
Multi-stage Process Testing	Automated scanners are unsuitable for testing multi-stage processes such as account **registration** and payment processing. This check focuses the tester on the multi-stage processes, and aims to identify persistent XSS flaws, downstream database injection flaws, etc.
Authentication Testing	Web APIs generally require an authentication process to separate authorized users from others. This testing process includes logon routine weaknesses, authentication token manipulation, and password attacks.
Manual Testing Areas	**Tasks and Activities**
Privilege Escalation	User separation is critical for securing the potentially sensitive data that a user can access. Escalation attacks attempt to break from one user to another of the same peer level and is referred to as horizontal escalation. Escalation also attempts to elevate privileges by breaking from a user to a higher-level account, such as an administrator account. This is referred to as vertical escalation.

Web Services Information Gathering	This phase of testing is focused on identifying in-scope services through various methods of gathering the web service entry points and communication schemas. Web Service Discovery (DISCO) and UDDI are used to discover the WSDL descriptors and other XML documents.
XML Structure Testing	Sophos validates that the XML structure is well-formed to ensure proper function. Structure is tested for entity injection, XML embedded tag injection, SQL injection, cross-site scripting, and XPATH injection attacks.
XML Content Testing	Sophos performs testing for XML content by executing web services functions, validating web services using higher privilege (if authenticated), and executing commands on the database. Parameters are checked for invalid content including SQL constructs, XML tags, etc.
RESTful Web Services Testing	Sophos performs testing for RESTful web services by validating the maximum and minimum string lengths, by ensuring proper validation including payload, and by validating parameter names.

Results may include the following:

- Multi-stage vulnerabilities
- Injectable inputs
- XML parser configuration issues
- Persistent injection vulnerabilities
- Cross-Site scripting flaws

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 remotely from a secure location or, if an exception has been approved then from the Customer's site(s).

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.

2.4.2 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
Web API Test	Final Report	Upon completion of testing	Email

2.4.2.1 Final Report

Sophos will issue a report to your organization after completing the test. The report may include the following:

- Executive summary
- Methods, detailed findings, narratives, and recommendations if any
- Attachments as needed for relevant details and supporting data

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 expiration of the review period, the report will be deemed final. 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 Customer designated contact, within five (5) business days of such email confirmation, the Service shall be deemed complete.

During the three (3) weeks after delivering the Service, the Sophos Technical Quality Assurance ("TQA") process for reporting may require validation and investigation of issues raised in the report. This will result in a small amount of testing outside the primary testing interval that will stop prior to delivery of the report. At the end of the TQA process, Sophos will issue a formal report to the Customer-designated point of contact.

2.5 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 For Approved 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.