

## Microsoft Entra ID Security Assessment

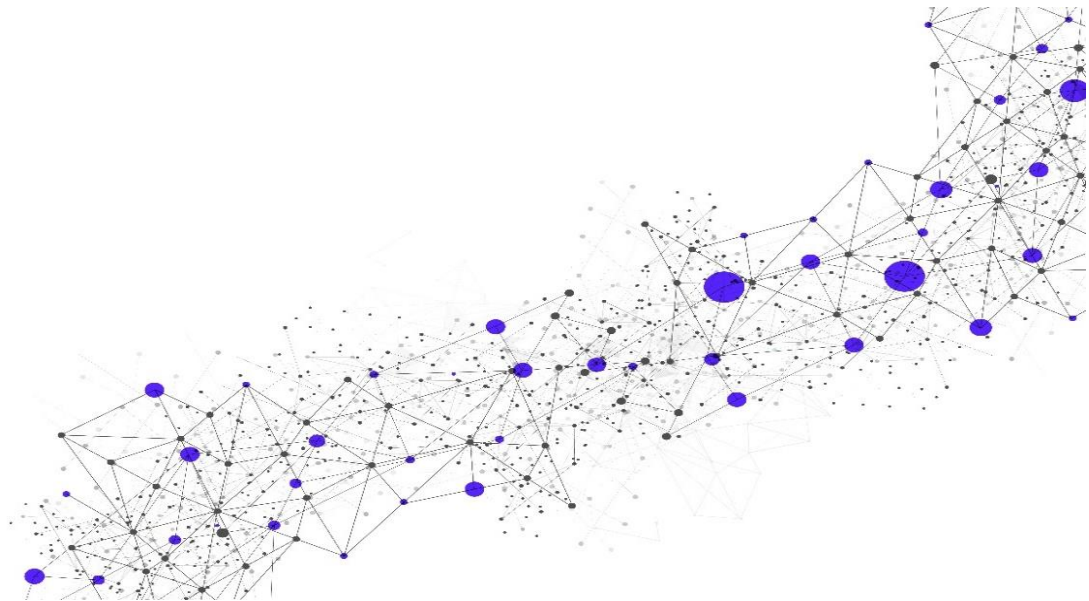
---

Release Date

**May 06, 2024**

Version

**1.0**



[www.secureworks.com](http://www.secureworks.com)

### Global Headquarters

1 Concourse Pkwy NE #500

Atlanta, GA 30328

Phone: +1 877 838 7947

Email: [info@secureworks.com](mailto:info@secureworks.com)

Additional office locations: <https://www.secureworks.com/about/offices>

---

## Table of Contents

<b>1</b>	<b>Service Introduction</b>	<b>4</b>
1.1	Overview	4
1.2	Customer Obligations	4
1.3	Scheduling	4
1.4	Timeline	5
<b>2</b>	<b>Service Details</b>	<b>5</b>
2.1	Service Initiation	5
2.2	Service Scope	5
2.3	Service Methodology	5
2.4	Service Delivery	6
2.4.1	Delivery Coordination	6
2.5	Deliverables	7
2.5.1	Microsoft Entra ID Security Assessment Report	7
2.6	Out of Scope	8
<b>3</b>	<b>Service Fees and Related Information</b>	<b>8</b>
3.1	Invoice Commencement	8
3.2	Expenses	8
3.3	Term	8
<b>4</b>	<b>Additional Terms</b>	<b>9</b>
4.1	For Approved On-site Services	9
4.2	Security Services	9
4.3	Record Retention	9
4.4	Compliance Services	9
4.5	Post-Engagement Activities	9
4.6	Legal Proceedings	10

### Copyright

© Copyright 2007-2024. SecureWorks, Inc. or its affiliates. All Rights Reserved.

This publication contains information that is confidential and proprietary to Secureworks® and is subject to your confidentiality obligations set forth in your contract with Secureworks or its affiliates. This publication and related hardware and software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Copying and/or reverse engineering of any Secureworks hardware, software, documentation, or training materials is strictly prohibited.

This publication and related Secureworks software remain the exclusive property of Secureworks. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronic or mechanical, photocopying, recording, or otherwise without the prior written permission from Secureworks.

Due to continued service development, the information in this publication and related software may change without notice. Please refer to your contract with Secureworks for any provided warranty information.

Secureworks® is a trademark or registered trademark of SecureWorks, Inc. or its affiliates. All other trademarks not owned by Secureworks that appear on this publication are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Secureworks.

---

## 1 Service Introduction

This Service Description (“SD”) describes the Microsoft Entra ID Security Assessment Service (“Service”). All capitalized words and phrases shall have the meanings set forth herein, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement for direct or indirect purchases (individually referenced herein as “CRA”), that is incorporated herein by reference. For avoidance of doubt, the CRA available at [www.secureworks.com/eula](http://www.secureworks.com/eula) (or at [www.secureworks.jp/eula-jp](http://www.secureworks.jp/eula-jp) for Customers located in Japan) applies to Customer’s purchases through an authorized Secureworks’ reseller.

### 1.1 Overview

Secureworks will offer a Microsoft Entra ID Security Assessment (ESA), focusing on cloud-based Microsoft Entra ID, (formerly Azure Active Directory) enabling customers to leverage the experience and insights of the Secureworks Incident Response team to understand how attackers can exploit Microsoft Entra ID misconfigurations and security control gaps to achieve their objectives. The customer can use the concise and actionable report created from the assessment to implement a best-practice Microsoft Entra ID 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 Secureworks 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 Secureworks, to permit Secureworks 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. Secureworks will evaluate these requests, and if approved for on-site activities
  - The customer will provide a suitable workspace for Secureworks personnel, and necessary access to systems, network, and devices.
  - Secureworks 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 Secureworks to perform the Service.
- Customer will provide Secureworks all required information (key personnel contact information, credentials, and related information) at least two (2) weeks before initiating the Service.

### 1.3 Scheduling

Secureworks will contact a customer-designated representative within five (5) business days after the execution of a Transaction Document to begin the Service Initiation activities described herein. These activities will ensure effective and efficient use of the Service.

Secureworks 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 Secureworks.

## 1.4 Timeline

Remote work will occur Monday – Friday, within the standard daytime working hours aligning with customer's local time zone

Approved on-site work will be performed Monday – Friday, 8 a.m. – 6 p.m. Customer's local time or similar daytime working hours.

Work performed outside of the hours listed above, as requested, or required by the 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, Secureworks 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 scope:

Secureworks will conduct an in-depth evaluation of one (1) of your organization's Microsoft Entra ID tenant to identify potential vulnerabilities and ensure optimal security configurations are addressed. For complex environments, additional costs may apply, which will be communicated transparently before engagement commencement.

The Secureworks team will execute the scope per requirements as outlined in a Transaction Document.

### 2.3 Service Methodology

During the Service, Secureworks will provide step-by-step instructions for you to provision a read-only account in your Entra ID environment to be used for this service and some read-only application permission to facilitate data collection. Secureworks uses this account to collect the Entra ID configuration data required to perform the technical assessment.

Secureworks will examine the following:

- **Access Control Mechanisms:** Review and governance of users, groups, service principals, and role assignments.
- **Identity Management:** Evaluation of internal/external user permissions, collaboration settings, and identity integrations.

- **Authentication Methods:** Assessment of authentication methods and Conditional Access policies.
- **Application Security and Compliance:** Governance of Enterprise Applications, application consent settings, and compliance with best practices.
- **Compliance with Best Practices:** Ensuring alignment with the latest industry best practices and regulatory standards.
- **Identifying and Mitigating Attack Paths:** Strategies to strengthen connections and reduce risks between platforms like Entra ID and Active Directory.

The Service is delivered in the following phases: initial meeting and data collection phase, the assessment phase, and a debrief. Additionally, a final report will be delivered to your point of contact.

### Initial Meeting

The initial meeting involves gathering key stakeholders, conveying the scope of the assessment and presenting the clear objectives. The assessor and customer will discuss critical areas to be examined such as Microsoft Entra ID configuration, policies, and controls, examining key areas such as user provisioning, password management, authentication methods, role-based access controls, and security monitoring. By leveraging industry-standard frameworks and methodologies, the assessment will provide actionable insights to help you strengthen your Microsoft Entra ID security.

### Assessment Phase

The assessment process involves a detailed examination of the Entra ID environment using industry-standard frameworks, methodologies, and Microsoft's best practices. This phase includes data collection, analysis, and evaluation of the security posture. The assessment team utilizes various tools and techniques to gather information about the Entra ID configuration, policies, and controls. This data is then analyzed to identify vulnerabilities, misconfigurations, and areas for improvement.

### Debrief

The debrief is a critical phase where the assessment team presents their findings, recommendations, and actionable insights to the customer. This session provides an opportunity for the customer to ask questions, seek clarification, and understand the necessary steps for remediation. The debrief includes a comprehensive review of the findings, discussion of identified vulnerabilities, and recommendations for enhancing the security posture of the Entra ID environment.

## 2.4 Service Delivery

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

### 2.4.1 Delivery Coordination

Secureworks will provide coordination for the Service(s) with appropriate communication and updates to the stakeholder community. The coordinator will oversee logistics coordination 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 Secureworks 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).

Secureworks solely reserves the right to refuse to travel to locations deemed unsafe by Secureworks or locations that would require a forced intellectual property transfer by Secureworks. Secureworks solely reserves the right to require a physical security escort at additional Customer expense to locations that are deemed unsafe by Secureworks. Customer will be notified at the time that services are requested if Secureworks refuses to travel or if additional physical security is required, and Customer must approve the additional expense before Secureworks travel is arranged. In the event any quarantines, restrictions, or measures imposed by governmental authority or Secureworks restrict travel to any location, Secureworks 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, Secureworks 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. Secureworks will work with Customer to determine appropriate specific deliverables, delivery method, and cadence.

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Microsoft Entra ID Security Assessment	Debrief Session	Mutually agreed upon	Conference call
Microsoft Entra ID Security Assessment	Final Report	Mutually agreed upon	Mutually agreed upon

**2.5.1 Microsoft Entra ID Security Assessment Report**

Once the technical assessment is complete, Secureworks 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 Microsoft Entra ID security, based on Secureworks and industry-accepted practices for securing Microsoft Entra ID.
- 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 the customer before the expiration of the review period, the report will be deemed final.

Secureworks 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 Secureworks. 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 [0](#) comprises the Secureworks standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate Transaction Document. Secureworks reserves the right to decline requests that:

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

---

## 3 Service Fees and Related Information

See Secureworks applicable CRA and Transaction Document 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.secureworks.com/legal/product-terms>, as updated from time to time (the “Product Terms Page”) or Transaction Document 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 Secureworks’ reseller but instead shall be subject to Customer’s agreement with its reseller.

### 3.2 Expenses

Customer agrees to reimburse Secureworks, directly or indirectly (in the 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 Secureworks agree that usage is necessary to complete Service delivery.

### 3.3 Term

The term of the Service is defined in the Transaction Document. Service will expire according to the Transaction Document 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 an extended term (if applicable), the terms and conditions of the CRA shall be in full force and effect.



---

## 4 Additional Terms

### 4.1 For Approved On-site Services

Notwithstanding Secureworks' employees' placement at Customer's location(s), Secureworks 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 Secureworks to provide any or all 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 Secureworks completes testing.

### 4.3 Record Retention

Secureworks will retain a copy of the Customer Reports in accordance with Secureworks' record retention policy. Unless Customer gives Secureworks written notice to the contrary prior thereto and subject to the provisions of the applicable CRA and DPA, all Customer Data collected during the Services and stored by Secureworks will be deleted within 30 days from issuance of the final Customer Report. If Customer or its authorized agent requests that Secureworks retain Customer Data for longer than its standard retention policy, Customer shall pay Secureworks' costs and expenses associated with the extended retention and storage of such Customer Data. Notwithstanding the foregoing, Secureworks 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 Secureworks' Services may discuss or relate to legal issues, Secureworks 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 Secureworks 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, Secureworks will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by Secureworks in the performance of the Services hereunder (the "**Engagement Media**"), unless prior to such commencement, Customer has specified in writing to Secureworks any special requirements for Secureworks to return such Engagement Media (at Customer's sole expense). Upon the customer's request, Secureworks will provide options for the transfer to Customer of Engagement Media and the related costs thereto. If so requested, Secureworks will provide a confirmation letter to the customer addressing the completion and scope of these post-engagement activities, in Secureworks' standard form. Unless agreed to otherwise by the parties, and subject to any applicable legal or regulatory requirements, Secureworks 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 Secureworks 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 Secureworks or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify Secureworks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Secureworks 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 Secureworks as to the Service.