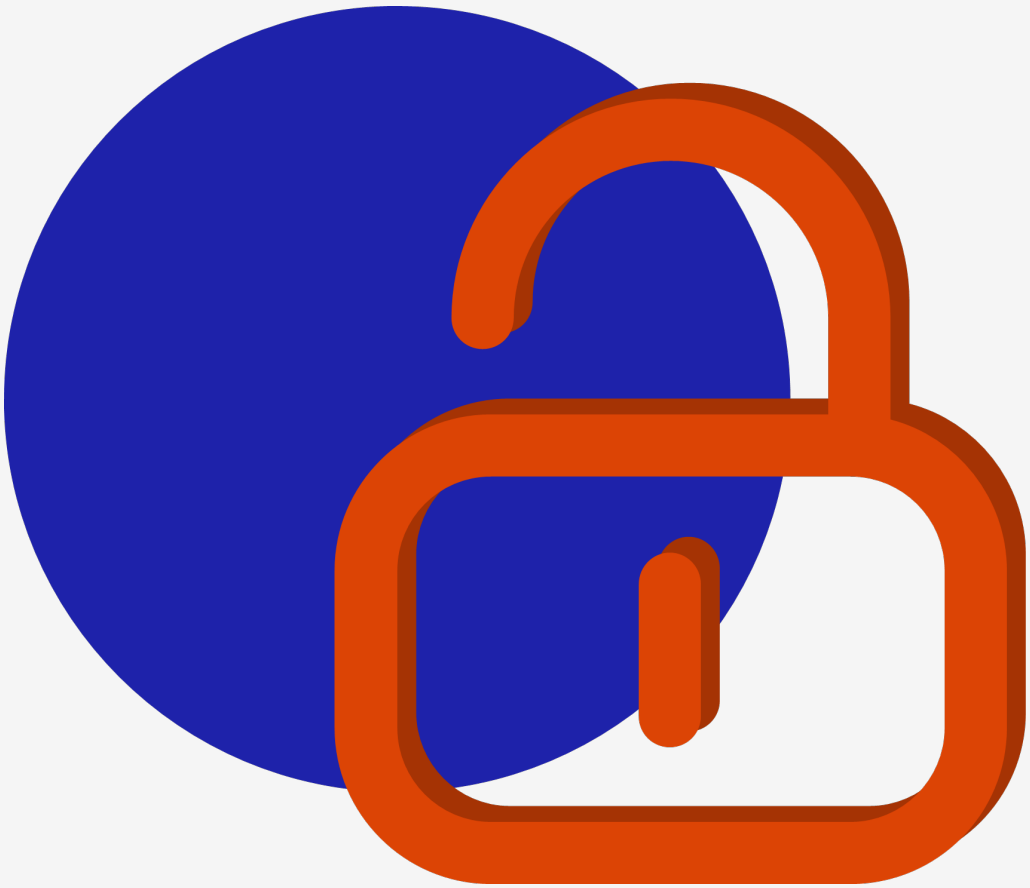
++

Sophos Central DNS Protection Security Review

Sophos

30 January 2024



Document Control

Date	Change By	Change	Issue
2024–01–26	Justin Moorcroft	Document created	0.1
2024–01–30	Logan Kroeger	Document QA	0.2
2024–01–30	Justin Moorcroft	Document published	1.0

Document Distribution

Date	Name	Company
2024–01–30	Steven Hedworth	Sophos
2024–01–30	Sam Caise	Sophos

Contents

1 Overview . . . 3
2 Approach . . . 3
2.1 DNS Protection Web Application Security Assessment . . . 3
2.2 AWS and Kubernetes Security Review . . . 3
2.3 Goal-driven Security Assessment . . . 4
3 Results . . . 5
3.1 DNS Protection Web Application Security Assessment . . . 5
3.2 AWS and Kubernetes Security Review . . . 5
3.3 Goal-driven Security Assessment . . . 5
3.4 Vulnerabilities Summary . . . 5
Appendix I Disclaimer and Non-Disclosure Agreement . . . 7
Appendix II Project Team . . . 8

1. Overview

MWR CyberSec (MWR) was commissioned by Sophos to conduct an in-depth security assessment of their DNS Filtering service.The functionality provided DNS filtering services to Sophos clients, and consisted of a UI component embedded in Sophos Central with a backend DNS service hosted in AWS. The assessment was performed remotely from the 7th of December 2023 to the 26th of January 2024.

The assessment comprised of multiple separate testing components, namely:

- A Web Application Security Assessment
- An AWS and Kubernetes Security Review
- A Goal-driven Security Assessment

MWR's consultancy team has built a strong reputation as a research-driven IT security consultancy firm. The team has a proven track record of collaborating with organisations that are industry leaders in information security. This is evident in the number of advisories and security-related publications available on MWR's Intel web page[1] and corporate insight webpages[2].

Beyond the technical competency of consultants, MWR prides itself in providing a unique set of client engagement services that put security management at the core of clients' business processes. Consultants are experienced in analysing the security architecture of solutions and providing catered security design recommendations.

2. Approach

The primary objective for the assessment was to determine whether or not any of the deployed resources were exposed in a way that could be exploited from the public internet. Additionally, testing aimed to determine whether or not any potential security-related enhancements could be made to improve the overall security posture of the DNS Filtering Service and the environment it resided in.

2.1. DNS Protection Web Application Security Assessment

The testing approach involved navigating to the DNS Protection functionality within Sophos' Central UI web application. The functionality presented by that endpoint was then assessed for any vulnerabilities or misconfigurations that could pose a security risk to Sophos. Testing was conducted using MWR's web application security assessment methodology, which is in line with the CREST application testing methodology, covering aspects pertaining to information gathering, content discovery, injection attacks, and authentication and authorisation bypass attacks. The full testing methodology is available on request.

2.2. AWS and Kubernetes Security Review

The Sophos DNS Filtering service was hosted in two AWS environments. MWR assessed the resources within the AWS environments pertaining to the DNS Filtering service to identify any security misconfigurations and possible hardening controls that could be enforced within the environment to ensure that the associated configurations deployed within Sophos' environments were secure.

[1] https://www.mwrcybersec.com/technical-research

[2] https://www.mwrcybersec.com/corporate-insights

MWR's methodology for assessing such environments combines best practice guidance issued by AWS and other industry organisations (such as NIST, NCSC and CIS) with MWR's own experience performing offensive security assessments of cloud environments.

MWR's methodology focuses on the following areas:

- Administration and patch management
- Network/Boundary Security Controls (VPCs, Subnet Layouts, Security Groups, etc):
  - This includes a port scan of any externally exposed assets, and basic vulnerability scanning for vulnerabilities in any of the exposed services.
- Data Security and Encryption:
  - Encryption at rest
  - Encryption in transit (TLS)
- Identify Management and Access Controls:
  - IAM policies, roles, groups, and users
  - Any federated access control mechanisms
  - Resource-specific access policies
- Certificate, key and secrets management
- Detection controls, such as CloudTrail and CloudWatch
- Incident readiness
- The deployed AWS Organisations' SCPs and other access controls

The assessment also included an in-depth security review of the Kubernetes clusters within the in-scope AWS environments.

2.3. Goal-driven Security Assessment

This component aimed to identify any additional malicious activities that an attacker may try to perform, which was not covered by the other components. This was determined by approaching the service from an attacker's perspective, and included a range of different actions:

- DNS Amplification Attacks
- IP Address Spoofing
- Obtaining access to other customer's data

3. Results

3.1. DNS Protection Web Application Security Assessment

The DNS Protection Web Application Security Assessment identified three low-risk vulnerabilities and three informational-risk vulnerabilities which presented minimal risk to Sophos. These vulnerabilities related to defence-in-depth measures and misconfigurations that could be patched to further improve the overall security posture of the Sophos DNS Protection functionality.

3.2. AWS and Kubernetes Security Review

The results of the AWS and Kubernetes Configuration review identified two medium-risk, six low-risk and two informational-risk vulnerabilities within the configuration of resources in the Sophos AWS environment. These vulnerabilities were not exploitable from an external perspective, and related to security hardening controls which should be implemented.

3.3. Goal-driven Security Assessment

The DNS Filtering Service was resilient towards all of the attack techniques attempted and consistently incorporated security best practices and effective security controls. As such, no vulnerabilities were identified in this portion of the assessment.

3.4. Vulnerabilities Summary

The assessments identified two medium-risk, nine low-risk and five informational-risk vulnerabilities. In total, 16 vulnerabilities were found; the table below shows a count breakdown of these vulnerabilities per component and risk rating.

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
AWS Security Assessment	0	2	6	2
Web Application Assessment	0	0	3	3
Total	0	2	9	5

The vulnerabilities identified were a result of defense-in-depth measures and inconsistencies with the implementation of security best practices. Although the overall security of each component was already of a high standard, by remediating these vulnerabilities the security posture of Sophos' DNS Filtering service would be improved.

The following risk profiles were used as guidelines to classify the vulnerabilities:

HIGH	A vulnerability will be assessed as representing a high risk if it holds the potential for an attacker to control, alter or delete Sophos's electronic assets. For example, a vulnerability which could allow an attacker to gain unauthorised access to a system or to sensitive data would be assessed as a high risk. Such issues could ultimately result in the defacement of a web site, the alteration of data held within a database or the capture of sensitive information such as account credentials or credit card information.
MEDIUM	A vulnerability will be assessed to represent a medium risk if it holds, when combined with other factors or issues, the potential for an attacker to control, alter or delete Sophos's electronic assets. For example, a vulnerability that could enable unauthorised access to be gained if a specific condition was met, or an unexpected change in configuration was to occur, would be rated as a medium risk.
LOW	A vulnerability will be assessed to represent a low risk if the likelihood or impact of exploitation is extremely low. For example, this could be an HTTPS configuration that allows weak ciphers or outdated protocols, or a CAPTCHA that can be solved programmatically.
INFORMATIONAL	A vulnerability will be assigned the informational classification when it cannot be exploited directly but is not in line with security best practice. Such a vulnerability could provide information that would facilitate research into an attack against the target system. For example, disclosure of the server type in an HTTP response.

APPENDIX I – Disclaimer and Non-Disclosure Agreement

Non-Disclosure Statement

This report is the sole property of Sophos. All information obtained during the testing process is deemed privileged information and not for public dissemination. MWR CyberSec pledges its commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of Sophos. MWR CyberSec strives to maintain the highest level of ethical standards in its business practice.

Non-Disclosure Agreement

MWR CyberSec and Sophos have signed an NDA.

Disclaimer

This report is not meant as an exhaustive analysis of the level of security now present on the tested hosts, and the data shown here should not be used alone to judge security of any computer system. Some scans were performed automatically and may not reveal all the possible security holes present in the system. Some vulnerabilities that were found may be 'false positives', although reasonable attempts have been made to minimise that possibility. In accordance with the terms and conditions of the original quotation, in no event shall MWR CyberSec or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss or other damages.

APPENDIX II – Project Team

Assessment Team

Lead Consultant	Justin Moorcroft
Additional Consultant	Jonathon Everatt

Quality Assurance

QA Consultant	Logan Kroeger

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postiglioni

MWR CYBERSEC