

UNCLASSIFIED



# **ARCTIC WOLF CYLANCEON-PREM SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW**

**Version 1, Release 1**

**27 May 2025**

**Developed by Arctic Wolf and DISA for the DOD**

UNCLASSIFIED

### **Trademark Information**

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

**TABLE OF CONTENTS**

	<b>Page</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Executive Summary.....	1
1.2 Authority.....	1
1.3 Vulnerability Severity Category Code Definitions.....	1
1.4 STIG Distribution.....	2
1.5 SRG Compliance Reporting.....	2
1.6 Document Revisions.....	2
1.7 Other Considerations.....	2
1.8 Product Approval Disclaimer.....	2
<b>2. ASSESSMENT CONSIDERATIONS.....</b>	<b>4</b>
2.1 Security Assessment Information – External Identity and Access Management.....	4
2.2 Security Assessment Information – Central Log Server.....	4
<b>3. CONCEPTS AND TERMINOLOGY CONVENTIONS.....</b>	<b>5</b>
3.1 Architecture.....	5
<b>4. GENERAL SECURITY REQUIREMENTS.....</b>	<b>6</b>
4.1 Summary.....	6

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions .....	1

## LIST OF FIGURES

	<b>Page</b>
Figure 3-1: Architecture .....	5

## 1. INTRODUCTION

### 1.1 Executive Summary

The Arctic Wolf CylanceON-PREM Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This document is meant for use in conjunction with other STIGs, including the appropriate operating system STIGs.

### 1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

### 1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

**Table 1-1: Vulnerability Severity Category Code Definitions**

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will <b>directly and immediately</b> result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which <b>has a potential</b> to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which <b>degrades measures</b> to protect against loss of Confidentiality, Availability, or Integrity.

## 1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from <https://public.cyber.mil/>.

## 1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil).

## 1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil). DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

## 1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil). This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW federal/DOD mandated standards.



## **2. ASSESSMENT CONSIDERATIONS**

This STIG is not intended to provide technical guidance for all portions of CylanceON-PREM. This STIG is applicable to only a subset of the potential set of components available for use in and with CylanceON-PREM. All applicable components are part of the default installation per the installation instructions provided with the platform.

### **2.1 Security Assessment Information – External Identity and Access Management**

This STIG delegates certain security controls to an external Identity and Access Management system; delegated controls are out of scope for this STIG. Security controls in this STIG ensure the correct integration of the external system but thereafter rely on the security capabilities of the external system.

CylanceON-PREM allows the use of several supported providers including Active Directory, Lightweight Directory Access Protocol (LDAP), and others. This STIG was tested and validated using LDAP.

### **2.2 Security Assessment Information – Central Log Server**

This STIG requires integrating a Central Log Server for managing audit records within CylanceON-PREM. By providing centralized logging, real-time analysis, and automated alerting, a Central Log Server allows CylanceON-PREM to maintain a robust security posture and effectively respond to potential threats, ultimately contributing to the organization's overall security strategy.

### 3. CONCEPTS AND TERMINOLOGY CONVENTIONS

#### 3.1 Architecture

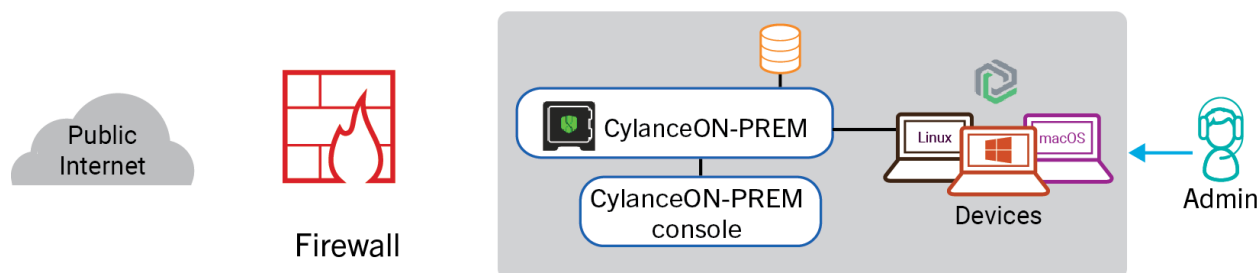
**CylanceON-PREM** – A virtual server that acts like a management console and provides secure communications between CylanceON-PREM and local infrastructure (endpoints) without exposing the local network to the internet.

**Console** – The console allows users to view and manage threats, scripts, and memory events that might be found on the devices in an environment. It also allows users to manage device and application events, view and manage quarantined events, and manage users and devices that communicate with CylanceON-PREM.

**Desktop Agent** – Desktop agent must be installed on a device (endpoint) to protect the device. CylancePROTECT Desktop supports Windows, macOS, and Linux operating systems.

**Database** – An internal database can be used (included with CylanceON-PREM), or users can configure an external database. The database is a relational database that contains the endpoint information and must be DOD approved.

Figure 3-1: Architecture



## 4. GENERAL SECURITY REQUIREMENTS

### 4.1 Summary

CylanceON-PREM requires robust security measures, including certificate-based authentication for secure communication, role-based access control (RBAC), and strong password policies with multifactor authentication (MFA). All files must be evaluated by the artificial intelligence model to detect threats, and a “break glass” account must be maintained for emergency access.

Regular maintenance is critical, such as restarting the server every 30 days to invoke health checks, refresh certificates, and clear resource issues, along with applying software updates and patches.

Network security must include TLS encryption, firewalls, and segmentation, while sensitive data must be encrypted at rest and in transit. Comprehensive logging, monitoring, and periodic backups ensure system integrity, aligning with industry standards such as ISO 27001 and NIST for compliance and proactive risk management.