**Cloudflare Zero Trust Pilot Testing Document**

**Author(s): Theo Bautista**

**1. Introduction**

This document outlines the testing conducted for the Cloudflare Zero Trust (ZTA) pilot implementation at Premier Technology Solutions. The objective of this pilot was to demonstrate the effectiveness of Cloudflare's Zero Trust platform in addressing key security challenges, including reactive Shadow IT management, endpoint vulnerabilities, and the need for enhanced Third-Party Risk Management.

The pilot focused on key functionalities of Cloudflare Zero Trust, including DNS filtering, device posture checks, and the secure access portal WARP client and WARP Access capabilities. The following sections detail the evidence gathered through screenshots and observations during the testing phase.

**2. Key Evidence from Pilot Testing**

**2.1. DNS Filtering Blocking Unauthorized Applications (e.g., drive.google.com)**

**Purpose:** To demonstrate Cloudflare Gateway's ability to prevent access to unsanctioned applications and personal cloud storage, thereby mitigating Shadow IT risks and preventing data leakage.

**Test Scenario:** An attempt was made to access drive.google.com from a device protected by the Cloudflare WARP client and configured with a DNS filtering policy to block personal cloud storage.

**Expected Outcome:** Access to facebook.com or drive.google.com should be blocked, and a custom block page or a clear indication of the block should be displayed and redirected it to SSO portal page before going to Approved Tool Portal.

**Evidence:**

A screen shot of a computer

AI-generated content may be incorrect.

*Figure 1: Blocked Page*

A screenshot of a login form

AI-generated content may be incorrect.

*Figure 2: SSO Portal via Auth0 Apps*

**2.2. SSO Portal with Approved Applications**

**Purpose:** To demonstrate the functionality of the Single Sign-On (SSO) portal in providing secure and streamlined access to company-approved applications, promoting the use of sanctioned tools over Shadow IT alternatives.

**Test Scenario:** A user attempted to access an unapproved application and redirected via the Premier Technology Solutions' SSO portal, configured auth0.

**Expected Outcome:** The user should be successfully authenticated through the SSO process and presented with a portal displaying a list of accessible, company-approved applications (e.g., Microsoft OneDrive, Microsoft Teams, SharePoint Online).

**Evidence:**

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 3: Approved Portal Page*

**2.3. Device Posture Check Failing for Outdated O.S**

**Purpose:** To verify that Cloudflare Zero Trust can enforce device compliance policies by detecting and blocking non-compliant devices, such as those lacking full disk encryption.

**Test Scenario:** An attempt was made to access a protected application or resource from a device that was intentionally configured with outdated operating system. A device posture policy was set in Cloudflare Zero Trust to require updated O.S not older than 10.0.19045.

**2.4. Real-time Access Logs Showing Policy Enforcement**

**Purpose:** To illustrate the visibility and auditing capabilities of Cloudflare Zero Trust, showing how policy enforcement actions are logged in real-time.

**Test Scenario:** Various access attempts were made (e.g., trying to access a blocked site, a compliant device accessing a resource, a non-compliant device attempting access). The Cloudflare Zero Trust dashboard's real-time logs were monitored.

**Expected Outcome:** The access logs should clearly record details of each attempt, including the user, device, attempted resource, and the policy action taken. This provides auditable evidence of ZTA policies in action.

**Evidence:**

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 4: Blocked Outdated Devices*

**2.5. WARP Client Connectivity and Security**

**Purpose:** To verify the successful deployment and active operation of the Cloudflare WARP client on endpoint devices, ensuring that all internet traffic is routed through the Cloudflare Zero Trust network for inspection and policy enforcement.

**Test Scenario:** A device with the Cloudflare WARP client installed was connected to the internet. The WARP client's status and connection details were observed.

**Expected Outcome:** The WARP client should show a "Connected" status, indicating that the device's internet traffic is being protected and routed through the Cloudflare Zero Trust platform.

**Evidence:**

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 5: Warp Connectivity Status*

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 6: Warp Login Page*