

TotalAI AI-EASM Report

AI Service Detection via Qualys Scan

Generated for
ACME CORP

Powered by



Date: October 2026

Scope: AI Services Only

Confidential and Proprietary Information: Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2026, Qualys, Inc.

- 01 Executive Summary
- 02 AI – Related Subdomains
- 03 Cloud Infrastructure Fingerprint
- 04 Shodan Banner Intelligence
- 05 Risky Exposed Ports
- 06 AI Services Exposed
- 07 Related Domains & Subsidiaries
- 08 Recommendations

1 Executive Summary

Passive intelligence gathered from DNS, certificate transparency, Shodan banners, and WHOIS — zero live probes to target infrastructure.

**184**

SUBDOMAINS

**123**

UNIQUE IPS

**30**

AI SUBDOMAINS

**18**

CLOUD ASSETS

**1**

RISKY PORTS

Risk Level: LOW

Passive Risk Score: 23

- 2 risky port(s) exposed (databases, remote access)

equitablebank.ca

Registrant: · Registrar: · ASNs: 0 · IP Ranges: 0

2

AI – Related Subdomains

Subdomains matching AI/ML patterns discovered via DNS enumeration. These indicate AI infrastructure that may be externally accessible.

SUBDOMAIN	CATEGORY	IP ADDRESS
agent.support.acmecorp.com	AGENT	204.74.99.100
llm.support.acmecorp.com	LLM	204.74.99.100
mcp.support.acmecorp.com	MCP	204.74.99.100
ml.support.acmecorp.com	ML	204.74.99.100

3

Cloud Infrastructure Fingerprint

Cloud provider detection via DNS CNAME analysis. Dangling CNAMEs indicate subdomain takeover risk

AWS
30 Subdomains

Fastly
7 Subdomains

Zendesk
1 Subdomains

SUBDOMAIN	CNAME	PROVIDER	SERVICE
ai.saptech.acmecorp.com	ingress-pro-dev-alb-1387058221.us-east-1.elb.amazonaws.com	AWS	AWS (generic)
api.acmecorp.com	h3.nfl.map.fastly.net	Fastly	Fastly CDN
staging-id.acmecorp.com	h3.nfl.map.fastly.net	Fastly	Fastly CDN
mi.acmecorp.com	dwotipmw6p2h0.cloudfront.net	AWS	AWS CloudFront
americas-tms.fulfillment.acmecorp.com	ingress-api-dev-alb-1826702583.us-west-2.elb.amazonaws.com	AWS	AWS (generic)

SUBDOMAIN	CNAME	PROVIDER	SERVICE
bi.ocf.fulfillment.acmecorp.com	ingress-pro-stg-alb-2111150449.us-west-2.elb.amazonaws.com	AWS	AWS (generic)
biext.ocf.fulfillment.acmecorp.com	ingress-ngs-prd-alb-261887294.us-west-2.elb.amazonaws.com	AWS	AWS (generic)
bizaudit.fulfillment.acmecorp.com	ingress-ngs-dev-alb-1604415976.us-east-1.elb.amazonaws.com	AWS	AWS (generic)
bwapp.akamai.acmecorp.com	ingress-pro-prd-alb-1285892917.us-west-2.elb.amazonaws.com	AWS	AWS (generic)
cdt-api.fulfillment.acmecorp.com	d269qe0b3dp163.cloudfront.net	AWS	AWS CloudFront
cdt-api.ocf.fulfillment.acmecorp.com	ingress-pro-stg-alb-1524379868.us-east-1.elb.amazonaws.com	AWS	AWS (generic)
cdt-bizaudit.fulfillment.acmecorp.com	ingress-api-stg-alb-1063984385.us-east-1.elb.amazonaws.com	AWS	AWS (generic)

SUBDOMAIN	CNAME	PROVIDER	SERVICE
cdt-customerportal.scale. fulfillment.acmecorp.com	ingress-ngs-dev-alb-1521150885.us-west-2.elb.amazonaws.com	AWS	AWS (generic)
cdt-fulfillment.fbm.acmecorp.com	d1a99sadpkf162.cloudfront.net	AWS	AWS CloudFront
cdt-intranet. fulfillment.acmecorp.com	nfl-help.zendesk.com	Zendesk	Zendesk
cdt-leaf. fulfillment.acmecorp.com	ingress-ngs-prd-alb-290935267.us-east-1.elb.amazonaws.com	AWS	AWS (generic)
cdt-midapi.scale. fulfillment.acmecorp.com	ingress-ngs-prd-alb-261887294.us-west-2.elb.amazonaws.com	AWS	AWS (generic)

4

Shodan Banner Intelligence

AI services identified from Shodan's pre-scanned banner data for this domain's IP addresses. No live probes made.

IP	PORT	SERVICE	CATEGORY	CONFIDENCE
18.160.18.72	443	n8n	Workflow AI	MEDIUM

5 Risky Exposed Ports

Internet-exposed ports commonly associated with databases, remote access, and other high-risk services.

IP	PORT	SERVICE
24.221.135.132	25	SMTP
24.221.135.142	25	SMTP

6

AI Services Exposed

AI services verified via active probing against this domain's infrastructure

IP	SERVICE	PORT	AUTH	MODELS
45.60.121.220	triton NVIDIA Triton	8000	NO	--
45.60.121.220	minio MinIO	9000	NO	--
45.60.121.220	triton NVIDIA Triton	8001	NO	--
45.60.121.220	triton NVIDIA Triton	8002	NO	--

7

Related Domains & Subsidiaries

Domains linked to acmecorp.com via WHOIS, certificate transparency, and shared infrastructure analysis.

DOMAIN	SOURCE	CONFIDENCE	RELATIONSHIP	REGISTRANT
acmecorp.com	SPF_INCLUDE	LOW	shared_infra	

8 Recommendations

CRITICAL

- Close risky ports exposed to the internet (databases, remote access).
- Conduct active probing scan for deeper AI service validation.

HIGH PRIORITY

- Review cloud infrastructure for overly permissive configurations.
- Validate related/subsidiary domains are under organizational control.
- Implement DNS monitoring for new AI-related subdomains.

Powered By



The leading provider of information security and compliance cloud solutions. More than 10,000 subscription customers worldwide in more than 130 countries trust Qualys to underpin digital transformation for greater agility, better business outcomes, and substantial cost savings. The Enterprise TruRisk Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Copyright © 2026, Qualys and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Qualys is registered trademarks of Qualys and/or its affiliates. Other names may be trademarks of their respective owners.