TITAN ORACLE Portal + Vendor Risk Evidence Pack

Report ID: **OPP-20260424-205558**

Customer: **Regional Health Plan (Blue-class Demo)**

Generated: **2026-04-24T20:55:58.758833+00:00**

Summary

Total findings	20
Critical	18
High	2
Medium	0
Low	0

Detectors

Detector	Findings
file_transfer_cve	7
portal_tracker	6
phi_in_url	2
insider_email_exfil	2
vendor_breach_intel	2
vendor_missing_baa	1

HIPAA Controls Evidenced

Control	Findings
164.502	10
164.308(a)(1)	7
164.308(a)(5)	7
164.312(e)	7
164.504	4
164.508	4
164.308(b)	3
164.502(e)	3
164.514	2
164.308(a)(4)	2
164.312(b)	2
164.530(c)	2

164.314(a)	2

Recommended Package

ENTERPRISE — $300K / year (floor, scales with user count and records)

Findings span all five Blue-class leak patterns with double digit criticals. Enterprise tier includes unlimited users, all five detectors fully enabled, daily threat-feed updates, 24x7 on-call, quarterly red-team of the portal, and an SLA-backed breach response retainer.

ROI: Anchored against the $16M OCR Anthem fine and $115M Anthem class action, a single prevented incident returns 50x to 400x the subscription cost.

All Findings

[CRITICAL] Progress MOVEit Transfer exposed to CVE-2023-34362

FID: f6bfaaedcfe1054b · Detector: file_transfer_cve · Policy: ORACLE-FILE-TRANSFER-CVE-CRITICAL

HIPAA: 164.308(a)(1), 164.308(a)(5), 164.312(e)

PRODUCT: Progress MOVEit Transfer

VENDOR: Progress Software

HOST: mft01.regional-health.example

INSTALLED VERSION: 2022.0.2

CVE: CVE-2023-34362

CVSS: 9.8

AFFECTED BEFORE: 2022.1.5 / 2022.0.4 / 2021.1.4 / 2021.0.6

DESCRIPTION: SQL injection leading to RCE actively exploited by Clop ransomware group, source of the Blue Shield CA May 2023 breach

DETECTED AT: 2026-04-24T20:55:58.756047+00:00

Recommendation: Patch the file transfer appliance within 24 hours, rotate credentials, and review egress logs for the backfill window of the CVE disclosure. Put the appliance behind a WAF with CVE specific virtual patches.

[CRITICAL] Progress MOVEit Transfer exposed to CVE-2023-35036

FID: 4f444e7b8001388b · Detector: file_transfer_cve · Policy: ORACLE-FILE-TRANSFER-CVE-CRITICAL

HIPAA: 164.308(a)(1), 164.308(a)(5), 164.312(e)

PRODUCT: Progress MOVEit Transfer

VENDOR: Progress Software

HOST: mft01.regional-health.example

INSTALLED VERSION: 2022.0.2

CVE: CVE-2023-35036

CVSS: 9.1

AFFECTED BEFORE: None

DESCRIPTION: Additional SQLi in MOVEit Transfer

DETECTED AT: 2026-04-24T20:55:58.756059+00:00

Recommendation: Patch the file transfer appliance within 24 hours, rotate credentials, and review egress logs for the backfill window of the CVE disclosure. Put the appliance behind a WAF with CVE specific virtual patches.

[CRITICAL] Progress MOVEit Transfer exposed to CVE-2023-36934

FID: d71661f12300db8a · Detector: file_transfer_cve · Policy: ORACLE-FILE-TRANSFER-CVE-CRITICAL

HIPAA: 164.308(a)(1), 164.308(a)(5), 164.312(e)

PRODUCT: Progress MOVEit Transfer

VENDOR: Progress Software

HOST: mft01.regional-health.example

INSTALLED VERSION: 2022.0.2

CVE: CVE-2023-36934

CVSS: 9.1

AFFECTED BEFORE: None

DESCRIPTION: Third SQLi vector patched July 2023

DETECTED AT: 2026-04-24T20:55:58.756068+00:00

Recommendation: Patch the file transfer appliance within 24 hours, rotate credentials, and review egress logs for the backfill window of the CVE disclosure. Put the appliance behind a WAF with CVE specific virtual patches.

[CRITICAL] Cleo VLTrader / Harmony / LexiCom exposed to CVE-2024-50623

FID: 9bf360d936c152fa · Detector: file_transfer_cve · Policy: ORACLE-FILE-TRANSFER-CVE-CRITICAL

HIPAA: 164.308(a)(1), 164.308(a)(5), 164.312(e)

PRODUCT: Cleo VLTrader / Harmony / LexiCom

VENDOR: Cleo Communications

HOST: edi.regional-health.example

INSTALLED VERSION: 5.8.0.17

CVE: CVE-2024-50623

CVSS: 9.8

AFFECTED BEFORE: 5.8.0.21

DESCRIPTION: Unrestricted file upload leading to RCE, source of the BCBS Massachusetts Cierant breach December 2024

DETECTED AT: 2026-04-24T20:55:58.756086+00:00

Recommendation: Patch the file transfer appliance within 24 hours, rotate credentials, and review egress logs for the backfill window of the CVE disclosure. Put the appliance behind a WAF with CVE specific virtual patches.

[CRITICAL] Cleo VLTrader / Harmony / LexiCom exposed to CVE-2024-55956

FID: d46df391ec693b0b · Detector: file_transfer_cve · Policy: ORACLE-FILE-TRANSFER-CVE-CRITICAL

HIPAA: 164.308(a)(1), 164.308(a)(5), 164.312(e)

PRODUCT: Cleo VLTrader / Harmony / LexiCom

VENDOR: Cleo Communications

HOST: edi.regional-health.example

INSTALLED VERSION: 5.8.0.17

CVE: CVE-2024-55956

CVSS: 9.8

AFFECTED BEFORE: 5.8.0.24

DESCRIPTION: Patch-bypass of CVE-2024-50623, actively exploited

DETECTED AT: 2026-04-24T20:55:58.756095+00:00

Recommendation: Patch the file transfer appliance within 24 hours, rotate credentials, and review egress logs for the backfill window of the CVE disclosure. Put the appliance behind a WAF with CVE specific virtual patches.

[CRITICAL] Fortra GoAnywhere MFT exposed to CVE-2024-0204

FID: aa232b7e5f82813a · Detector: file_transfer_cve · Policy: ORACLE-FILE-TRANSFER-CVE-CRITICAL

HIPAA: 164.308(a)(1), 164.308(a)(5), 164.312(e)

PRODUCT: Fortra GoAnywhere MFT

VENDOR: Fortra

HOST: ga.regional-health.example

INSTALLED VERSION: 7.1.1

CVE: CVE-2024-0204

CVSS: 9.8

AFFECTED BEFORE: None

DESCRIPTION: Authentication bypass to admin

DETECTED AT: 2026-04-24T20:55:58.756114+00:00

Recommendation: Patch the file transfer appliance within 24 hours, rotate credentials, and review egress logs for the backfill window of the CVE disclosure. Put the appliance behind a WAF with CVE specific virtual patches.

[CRITICAL] Outbound email to personal webmail (gmail.com)

FID: 100a8edb801b3bf5 · Detector: insider_email_exfil · Policy: ORACLE-INSIDER-EXFIL-BLOCK

HIPAA: 164.308(a)(4), 164.312(b), 164.502, 164.530(c)

FROM: k.santos@regional-health.example

TO: k.santos@gmail.com

TO DOMAIN: gmail.com

SUBJECT: member roster backup

ATTACHMENTS: member-roster-Q2.xlsx

SIZE (BYTES): 4194304

PHI SIGNATURES:

RISK FACTORS: has_attachment, attachment_over_1mb, bulk_data_file_type, self_send_to_personal_account

DETECTED AT: 2026-04-24T20:55:58.755948+00:00

Recommendation: Quarantine the message, notify the privacy officer, and open a HIPAA sanctions case under 164.530(e). Block personal webmail domains at the secure email gateway for employees with PHI access.

[CRITICAL] Outbound email to personal webmail (yahoo.com)

FID: 204a4af4a53eae60 · Detector: insider_email_exfil · Policy: ORACLE-INSIDER-EXFIL-BLOCK

HIPAA: 164.308(a)(4), 164.312(b), 164.502, 164.530(c)

FROM: r.kim@regional-health.example

TO: r.kim.personal@yahoo.com

TO DOMAIN: yahoo.com

SUBJECT: claims overflow

ATTACHMENTS: claims-export.csv

SIZE (BYTES): 812000

PHI SIGNATURES: ssn, mrn, dob

RISK FACTORS: has_attachment, bulk_data_file_type, phi_signatures_present, self_send_to_personal_account

DETECTED AT: 2026-04-24T20:55:58.756012+00:00

Recommendation: Quarantine the message, notify the privacy officer, and open a HIPAA sanctions case under 164.530(e). Block personal webmail domains at the secure email gateway for employees with PHI access.

[CRITICAL] PHI identifier exposed in URL

FID: 5811d80cbb52cb50 · Detector: phi_in_url · Policy: ORACLE-PORTAL-URL-PHI-BLOCK

HIPAA: 164.502, 164.514

URL: https://portal.regional-health.example/claim?mrn=MRN-884412&dob=04/17/1974

MATCHED PARAMS: mrn, dob

PHI IN PATH:

PHI IN QUERY: dob, mrn

DETECTED AT: 2026-04-24T20:55:58.755817+00:00

Recommendation: Stop passing identifiers through URL query strings. Move identifiers into POST bodies or server side session lookups. URLs land in browser history, server logs, referrer headers, and analytics pipelines.

[CRITICAL] PHI identifier exposed in URL

FID: dfab2d36879a2546 · Detector: phi_in_url · Policy: ORACLE-PORTAL-URL-PHI-BLOCK

HIPAA: 164.502, 164.514

URL: https://portal.regional-health.example/auth?member_id=SUB-221199&ssn=123-45-6789

MATCHED PARAMS: member_id, ssn

PHI IN PATH:

PHI IN QUERY: ssn

DETECTED AT: 2026-04-24T20:55:58.755873+00:00

Recommendation: Stop passing identifiers through URL query strings. Move identifiers into POST bodies or server side session lookups. URLs land in browser history, server logs, referrer headers, and analytics pipelines.

[CRITICAL] Tracker google_analytics present on analytics surface

FID: 3e0451a902399e93 · Detector: portal_tracker · Policy: ORACLE-PORTAL-TRACKER-BLOCK

HIPAA: 164.502, 164.504, 164.508

URL: https://portal.regional-health.example/login

TRACKER: google_analytics

CATEGORY: analytics

MATCH TOKEN: googletagmanager.com

PHI PAGE CONTEXT: True

DETECTED AT: 2026-04-24T20:55:58.755509+00:00

Recommendation: Remove tracker from every page that renders or receives PHI. If retention is required, route through a HIPAA compliant analytics pipeline with BAA in place.

[CRITICAL] Tracker meta_pixel present on advertising surface

FID: 4454be9075f7b2bd · Detector: portal_tracker · Policy: ORACLE-PORTAL-TRACKER-BLOCK

HIPAA: 164.502, 164.508

URL: https://portal.regional-health.example/login

TRACKER: meta_pixel

CATEGORY: advertising

MATCH TOKEN: connect.facebook.net

PHI PAGE CONTEXT: True

DETECTED AT: 2026-04-24T20:55:58.755540+00:00

Recommendation: Remove tracker from every page that renders or receives PHI. If retention is required, route through a HIPAA compliant analytics pipeline with BAA in place.

[CRITICAL] Tracker hotjar present on session_replay surface

FID: 224f695a69cfb1d7 · Detector: portal_tracker · Policy: ORACLE-PORTAL-TRACKER-BLOCK

HIPAA: 164.502, 164.504

URL: https://portal.regional-health.example/login

TRACKER: hotjar

CATEGORY: session_replay

MATCH TOKEN: static.hotjar.com

PHI PAGE CONTEXT: True

DETECTED AT: 2026-04-24T20:55:58.755568+00:00

Recommendation: Remove tracker from every page that renders or receives PHI. If retention is required, route through a HIPAA compliant analytics pipeline with BAA in place.

[CRITICAL] Tracker google_analytics present on analytics surface

FID: fb75969f1dd05faa · Detector: portal_tracker · Policy: ORACLE-PORTAL-TRACKER-BLOCK

HIPAA: 164.502, 164.504, 164.508

URL: https://portal.regional-health.example/account

TRACKER: google_analytics

CATEGORY: analytics

MATCH TOKEN: googletagmanager.com

PHI PAGE CONTEXT: True

DETECTED AT: 2026-04-24T20:55:58.755616+00:00

Recommendation: Remove tracker from every page that renders or receives PHI. If retention is required, route through a HIPAA compliant analytics pipeline with BAA in place.

[CRITICAL] Tracker meta_pixel present on advertising surface

FID: 8e1324f03cb566af · Detector: portal_tracker · Policy: ORACLE-PORTAL-TRACKER-BLOCK

HIPAA: 164.502, 164.508

URL: https://portal.regional-health.example/account

TRACKER: meta_pixel

CATEGORY: advertising

MATCH TOKEN: connect.facebook.net

PHI PAGE CONTEXT: True

DETECTED AT: 2026-04-24T20:55:58.755636+00:00

Recommendation: Remove tracker from every page that renders or receives PHI. If retention is required, route through a HIPAA compliant analytics pipeline with BAA in place.

[CRITICAL] Tracker hotjar present on session_replay surface

FID: 73295ed85da83294 · Detector: portal_tracker · Policy: ORACLE-PORTAL-TRACKER-BLOCK

HIPAA: 164.502, 164.504

URL: https://portal.regional-health.example/account

TRACKER: hotjar

CATEGORY: session_replay

MATCH TOKEN: static.hotjar.com

PHI PAGE CONTEXT: True

DETECTED AT: 2026-04-24T20:55:58.755661+00:00

Recommendation: Remove tracker from every page that renders or receives PHI. If retention is required, route through a HIPAA compliant analytics pipeline with BAA in place.

[CRITICAL] Vendor match against recent breach intel: Conduent Business Services

FID: 18ca2ea4b6edd206 · Detector: vendor_breach_intel · Policy: ORACLE-VENDOR-BREACH-INTEL-MATCH

HIPAA: 164.308(b), 164.314(a), 164.502(e)

VENDOR: Conduent Business Services

BREACH WINDOW: 2024-10-21 to 2025-01-13

RANSOMWARE GROUP: None

US REACH: 25000000

BAA ON FILE: True

SERVICES: print, mail, PHI

DETECTED AT: 2026-04-24T20:55:58.756128+00:00

Recommendation: Treat this vendor as compromised until they produce a clean forensic report. Rotate any shared secrets, pull recent exchange logs, and issue member notifications if PHI transited the vendor in the breach window.

[CRITICAL] Vendor match against recent breach intel: Young Consulting / Connexure

FID: e7fd012c788cc09a · Detector: vendor_breach_intel · Policy: ORACLE-VENDOR-BREACH-INTEL-MATCH

HIPAA: 164.308(b), 164.314(a), 164.502(e)

VENDOR: Young Consulting / Connexure

BREACH WINDOW: 2024-04-10 to 2024-04-13

RANSOMWARE GROUP: BlackSuit

US REACH: 954177

BAA ON FILE: True

SERVICES: stop loss software

DETECTED AT: 2026-04-24T20:55:58.756140+00:00

Recommendation: Treat this vendor as compromised until they produce a clean forensic report. Rotate any shared secrets, pull recent exchange logs, and issue member notifications if PHI transited the vendor in the breach window.

[HIGH] Fortra GoAnywhere MFT exposed to CVE-2023-0669

FID: e67e261b63ee660c · Detector: file_transfer_cve · Policy: ORACLE-FILE-TRANSFER-CVE-HIGH

HIPAA: 164.308(a)(1), 164.308(a)(5), 164.312(e)

PRODUCT: Fortra GoAnywhere MFT

VENDOR: Fortra

HOST: ga.regional-health.example

INSTALLED VERSION: 7.1.1

CVE: CVE-2023-0669

CVSS: 7.2

AFFECTED BEFORE: None

DESCRIPTION: Pre-auth RCE exploited by Clop for mass data theft

DETECTED AT: 2026-04-24T20:55:58.756106+00:00

Recommendation: Patch the file transfer appliance within 24 hours, rotate credentials, and review egress logs for the backfill window of the CVE disclosure. Put the appliance behind a WAF with CVE specific virtual patches.

[HIGH] Vendor missing BAA: New Analytics Startup

FID: 066b59644bf8958e · Detector: vendor_missing_baa · Policy: ORACLE-VENDOR-MISSING-BAA

HIPAA: 164.308(b), 164.502(e)

VENDOR: New Analytics Startup

SERVICES: claims, PHI

DETECTED AT: 2026-04-24T20:55:58.756152+00:00

Recommendation: Execute a Business Associate Agreement before any further PHI exchange. If the vendor refuses, stop the data flow within 30 days.