Cloud scanning

Cloud configuration and software security

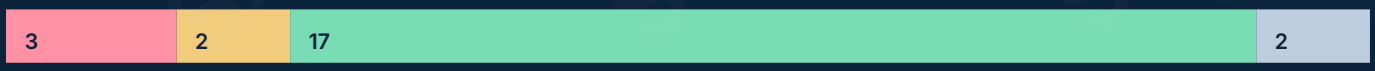
! Action required

Restrict public access and update the customer portal.

Public storage, unrestricted remote access and a vulnerable Log4j component need urgent attention.

24	3	1	1
Resources in scope	High-priority assets	Known vulnerabilities	Overdue actions

ASSET STATUS



3 Action | 2 Attention | 17 Pass | 2 Unknown

SECURITY CHECKS

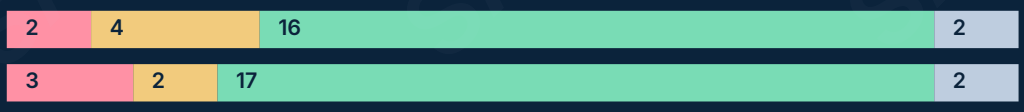
Exposure	22/24 pass
Access	23/24 pass
Logging	23/24 pass
Protection	22/24 pass
Software	23/24 pass

Assessment coverage: 118 of 120 applicable checks returned a result. Grey indicates missing or outdated evidence.

TOP THREE PRIORITIES

1	**Update Log4j Core**	Application owner / 12 Sep
2	**Restrict public storage access**	Cloud operations / 13 Sep
3	**Restrict remote administration**	Cloud operations / 13 Sep

CHANGE SINCE 06 SEPTEMBER



2 checks now pass; one new issue. Both assessments cover the same assets.

24 Azure resources | 2 subscriptions | West Europe + North Europe

Asset security overview

Security checks for each asset, ordered by priority.

01 Overview | 02 Assets | 03 Intelligence | 04 Actions

! Action ! Attention + Pass ? Unknown

ASSET / PLATFORM	Exposure	Access	Logging	Protection	Software
CLD-01 ns-store-prod	! Action	+ Pass	+ Pass	+ Pass	+ Pass
CLD-02 ns-admin-nsg	! Action	+ Pass	+ Pass	+ Pass	+ Pass
CLD-05 ns-portal-app	+ Pass	+ Pass	+ Pass	+ Pass	! Action
CLD-03 ns-keyvault	+ Pass	+ Pass	! Attention	+ Pass	+ Pass
CLD-04 ns-api-vm	+ Pass	+ Pass	+ Pass	! Attention	+ Pass
CLD-06 ns-backup	+ Pass	+ Pass	+ Pass	? Unknown	+ Pass
CLD-07 ns-directory	+ Pass	? Unknown	+ Pass	+ Pass	+ Pass
CLD-08 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-09 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-10 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-11 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-12 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-13 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-14 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-15 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-16 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-17 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-18 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-19 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-20 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-21 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-22 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-23 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass
CLD-24 Azure	+ Pass	+ Pass	+ Pass	+ Pass	+ Pass

N/A checks are excluded from totals. Grey indicates missing or outdated evidence. Software checks do not cover every published vulnerability.

Next steps: address urgent findings first, then other outstanding issues. Repeat incomplete checks before confirming a pass.

Vulnerabilities and updates

Affected versions, exploitation status and recommended updates.

Affected version confirmed

CVE-2021-44228

Apache Log4j Core

An attacker may be able to run code on the server by sending malicious input that the application logs.

10.0	YES	>99.99%	1
CVSS 3.1	Known exploitation (KEV)	30-day likelihood	Affected resources

INSTALLED VERSION	ORIGINAL FIX VERSION
2.14.1	2.15.0 (Java 8 and later)

Affected versions: 2.13.0 up to, but excluding, 2.15.0
Evidence: Software inventory identifies log4j-core 2.14.1.

RECOMMENDED UPDATE

Upgrade to the latest supported Log4j release compatible with your application. Test the update before deployment.

The original fix version is historical. Use the latest supported release.

Affected assets: CLD-05
Scope: 1 vulnerability across 1 asset. This report includes selected CVE examples.

Source dates: EPSS 2026-09-12; CISA KEV 2026-09-11; NVD updated 2026-08-11.
EPSS estimates the chance of this vulnerability being exploited in the next 30 days. It does not predict a breach of your organisation. EPSS percentile: 100.00%.

NVD record | Apache security advisory | EPSS explained | CISA KEV

Remediation plan

Actions, responsible teams, deadlines and verification.

7	1	2
Open actions	Overdue	Checks now passing

01 Update Log4j Core

OVERDUE 12 Sep

Install the supported update recommended on page 3 and confirm the version in use.

CLD-F05 | Application owner | 1 asset | Open

02 Restrict public storage access

DUE 13 Sep

Disable anonymous access to storage. Confirm that authorised users and services can still retrieve their files.

CLD-F01 | Cloud operations | 1 asset | Open

03 Restrict remote administration

DUE 13 Sep

Restrict remote administration to the approved private connection.

CLD-F02 | Cloud operations | 1 asset | Open

04 Enable audit logging

DUE 18 Sep

Enable audit logging and send events to the approved logging service in the same region.

CLD-F03 | Cloud security | 1 asset | Open

05 Enable workload protection

DUE 18 Sep

Enable the approved workload protection plan.

CLD-F04 | Cloud security | 1 asset | Open

06 Repeat the backup check

DUE 14 Sep

The backup check timed out. Run it again and confirm that it returns a result.

CLD-F06 | Integration owner | 1 asset | Open

07 Restore directory scan access

DUE 14 Sep

Grant the scanner the required directory permissions, then repeat the check.

CLD-F07 | Integration owner | 1 asset | Open

Before closing an action: record the change and repeat the relevant check. Close the issue once the result confirms that the fix is effective.