

ANALYZE

Advanced

60 MIN

• UPDATED 2026-09-30

Run a multi-cloud vulnerability impact assessment.

Use Security Copilot to evaluate exposure across cloud platforms and summarize the blast radius of a given vulnerability.

MICROSOFT 365

Word

WORKS WITH

Security Copilot

Business Outcome

A faster, clearer answer to "how exposed are we?" the moment a new vulnerability is disclosed.

Workflow Steps

Step 1: Identify the vulnerability

Security Copilot

Pull the exact CVE identifier and the affected software/version range straight from the advisory, and paste both into the prompt along with a one-line description of the exploit vector.

Security Copilot needs a specific, named target to correlate against your environment, not a general "check for vulnerabilities" request.

Step 2: Ask Security Copilot to assess exposure

Security Copilot

Point it at your connected cloud environments and ask specifically for blast radius, not just a yes/no on whether you're affected.

PROMPT

Assess our exposure to CVE-2026-XXXXX across our connected Azure, AWS and GCP environments. List every affected system, its criticality, and whether it's internet-facing. Prioritize the list by exposure severity.

Step 3: Draft the impact summary for leadership

Word

Turn the technical exposure list into a short written brief — what's affected, how bad, and what's being done — before this reaches anyone outside the security team.

Step 4: Route remediation by priority

Word

Send the highest-severity, internet-facing systems to remediation first; the rest can follow the normal patch cycle.

✓ Check the work

- Confirm the list of affected systems matches your actual asset inventory, not a generic assumption.
- Verify internet-facing status on the highest-priority items before allocating urgent remediation effort.
- Re-run the assessment after initial remediation to confirm the exposure actually closed.

Expected Outcome

A written impact assessment identifying affected systems across cloud platforms, prioritized by exposure severity.



Want help rolling this out across your team? [Go to Liminals.Tech](#) 📄