Cloud configuration: which settings let attackers in, and would you notice if one changed?

This month, run CISA's ScubaGear against Microsoft 365 and a free posture check against each cloud, and fix public storage, long-lived access keys, open app consent and open external access first. Then lock those settings with organization-level guardrails and re-run the same checks every week, so a changed setting shows up as a diff rather than as an incident.

Reviewed **5 Nov 2026** | Next review **5 Dec 2026** | Version **1.1**

Written for
IT, platform and security teams running Microsoft 365 with workloads in Azure, AWS or Google Cloud, in organizations of any size

Latest version
sheets.einblick.dev/cloud-configuration/

If you only do five things

1. **Measure against one published baseline this month.** Run CISA's free ScubaGear against Microsoft 365; it only reads settings[1]. Defender for Cloud's free Foundational CSPM checks Azure, AWS and Google Cloud against Microsoft's benchmark[12].
2. **Block public storage at the top.** Enforce S3 Block Public Access for the whole AWS organization[16], set `AllowBlobPublicAccess` to false on every Azure storage account[13] and enforce `storage.publicAccessPrevention` in Google Cloud[22]. Data stores left online without access controls remain among the most common errors in the DBIR[6].
3. **Replace long-lived keys with short-lived credentials.** AWS traces a large portion of security events to compromised long-term access keys[17], and in late 2025 attackers broke in with AWS keys suspected to have leaked in 2022[5]. Move people to federated sign-in and workloads to roles or managed identities, then delete the keys.
4. **Close app consent and external access in Microsoft 365.** Restrict user consent to verified publishers and low-risk permissions, with an admin consent workflow[2]. Allow Teams external access only for named domains: confirmed vishing over cross-tenant Teams calls rose 502% in a year[7].
5. **Turn the baseline into guardrails, then diff it weekly.** Enforce what must never change with AWS Organizations policies, Azure Policy and Google Cloud organization policies, then re-run the assessment weekly and compare runs[1].

Adopt a baseline without breaking things

1. **Pick one baseline per platform.** For Microsoft 365, SCuBA, or Baseline Security Mode, which every plan has[8]; for Azure, the Microsoft cloud security benchmark[12]; for AWS, Foundational Security Best Practices[15]; for Google Cloud, its security baseline constraints[21].
2. **Assess, and write down each exception.** Export every failing check. Record why each one stays, who owns it and when it ends; ScubaGear's YAML config holds these as exclusions, annotations or omissions[1].
3. **Check the impact, then fix.** Start with the policies CISA marks as BOD 25-01 requirements[4], and turn on each Baseline Security Mode setting whose impact report shows zero impact[8]. For MFA settings, use the passkeys and MFA sheet.
4. **Enforce at the top of each cloud.** In AWS, SCPs cap what roles can do, RCPs what resources allow, and declarative policies set defaults such as IMDSv2[19,18]. In Azure, assign deny policies at a management group. In Google Cloud, add the baseline constraints if your organization predates 3 May 2024[21]. Test each on one account first.
5. **Diff every week.** Compare each run with the last, for example with ScubaGear's `Invoke-SCuBADiff`[1]. Scan infrastructure-as-code pull requests with Checkov or a similar checker[23], and treat a scheduled `terraform plan` that isn't empty as drift.

Settings attackers go after

- **Public storage.** Google's public access prevention revokes existing public access once you enforce it[22]. Move public sites and downloads to a separate account or project first.
- **Access keys and shared keys.** Attackers reach Azure Blob Storage with exposed credentials, shared keys and SAS tokens[7]; accounts accept keys until `AllowSharedKeyAccess` is false[14]. Google Cloud blocks service account keys in organizations created since May 2024[21] and disables exposed ones[5].
- **Instance metadata.** Require IMDSv2, which uses token-backed sessions, by account default or declarative policy. Track the `ImdsV1Enabled` and `MetadataNoToken` metrics to zero, then add `ec2:RoleDelivery` to an SCP so IMDSv1 credentials stop working[18].
- **Broad roles for workloads.** Remove wildcard actions (Security Hub controls IAM.1 and IAM.21)[15] and pin GitHub OIDC trust to one repository and branch or environment[20]. An over-broad deploy role took UNC6426 from a stolen GitHub token to AWS administrator in under 72 hours[5].
- **Guests and external access.** Let only admins and Guest Inviters invite guests, and only from approved domains[2]; the external sharing sheet explains how this now also limits SharePoint sharing. Allow Teams external domains one by one and block chats from unmanaged accounts. Google Cloud's `iam.allowedPolicyMemberDomains` does the same for IAM grants[21]. SharePoint links: see the DLP sheet.
- **OAuth app consent.** Microsoft's managed default for new tenants still lets users consent to permissions outside a list of mail, file, calendar and chat scopes[10]. Changes keep existing grants[9], so review those too. Stolen Salesloft Drift tokens let attackers bulk-export Salesforce data[5].

What changed in 2026

- **Exploits overtook weak credentials in Google Cloud.** In late 2025, software flaws opened 44.5% of Google Cloud intrusions in Google's data and weak or missing credentials 27.2%; misconfiguration fell to 21%. Google suggests its secure defaults may have driven the shift[5]. Patch within the patching sheet's deadlines.
- **ScubaGear 2.0 is out.** The October 2026 release adds a Security Suite baseline for Defender, Purview, Exchange Online and Teams[3], so replace `defender` with `securitysuite` in your config[1]. The Entra baseline now requires blocking risky AI agents where Agent 365 or E7 is licensed[2].
- **Microsoft 365 moved toward secure defaults.** Baseline Security Mode, in the admin center since November 2025, covers phishing-resistant MFA for admins, legacy authentication and app consent[8]. Tenant Configuration Management, generally available since April 2026, monitors over 200 settings in six workloads[11].
- **S3 public access can be blocked for a whole organization.** Since November 2025 one AWS Organizations policy blocks it in every account, including new ones[16].

What you can skip

- **A paid CSPM before the free checks.** ScubaGear and Defender for Cloud's Foundational CSPM cost nothing[1,12]. Buy attack path analysis once the basics are closed.
- **Perfecting 90-day key rotation.** Security Hub checks for it[15], but AWS advises not creating long-term keys at all[17]. Remove them instead.
- **A home-grown baseline.** Start from a published one that someone keeps current.

Mistakes that cost the most

- **Trusting a new default to fix old resources.** Enforcing IMDSv2 for an account leaves instances that already allow IMDSv1 alone[18], and consent changes keep old grants[9].
- **Running workloads in the AWS management account.** SCPs and RCPs don't restrict it[19]. Keep it for billing and organization tasks.
- **Exposing a test resource "just for a day."** Microsoft measured a median of 5.3 hours from an exposed container's start to the first exploit attempt[7].

What this looks like at your size

Small team, no security staff

- Turn on each Baseline Security Mode setting with zero impact[8].
- Ask your IT provider for a monthly ScubaGear report and the list of consented apps and guests.
- Block public storage for the whole cloud organization, not account by account.

Growing, with IT or security staff

- Run ScubaGear weekly from a scheduled job, guard its app certificate like an admin credential and post the diff to the team channel.
- Connect every cloud account to one posture tool and give each finding an owner and a due date.
- Make infrastructure as code the only write path, and keep console write access for emergency roles.

Enterprise or regulated

- Treat BOD 25-01's mandatory SCuBA policies as your floor, as US federal civilian agencies must[4].
- Feed drift and posture findings into the SIEM, with a fix time per severity.
- Review changes to guardrail policies like Tier 0 code, with two people.

Version history

5 Nov 2026, version 1.1 Noted that, since Entra B2B integration became permanent for SharePoint in July 2026, limiting guest invitations also limits SharePoint and OneDrive sharing with new outsiders; the external sharing sheet has the details.

Sources

1. ScubaGear (README and docs). CISA, v2.0.0, Oct 2026. github.com
2. CISA M365 Secure Configuration Baseline for Microsoft Entra ID. CISA (ScubaGear), ScubaGear v2.0.0, Oct 2026. github.com
3. CISA Publishes Significant Updates to ScubaGear and ScubaGoggles. CISA, 27 Oct 2026. cisa.gov
4. BOD 25-01: Implementing Secure Practices for Cloud Services. CISA, 17 Dec 2024. cisa.gov
5. Cloud Threat Horizons Report H1 2026. Google Cloud, Mar 2026. services.google.com
6. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
7. Microsoft Digital Defense Report 2026. Microsoft Threat Intelligence, Oct 2026. cdn-dynmedia-1.microsoft.com
8. Baseline security mode settings. Microsoft Learn, 30 Sep 2026. learn.microsoft.com
9. Configure how users consent to applications. Microsoft Learn, 15 Jun 2025. learn.microsoft.com
10. Manage app consent policies. Microsoft Learn, 22 Jan 2026. learn.microsoft.com
11. Tenant Configuration Management APIs are now generally available. Microsoft Entra Blog, 23 Apr 2026. techcommunity.microsoft.com
12. What is Cloud Security Posture Management (CSPM). Microsoft Learn, 11 Sep 2026. learn.microsoft.com
13. Remediate anonymous read access to blob data. Microsoft Learn, 15 Jul 2026. learn.microsoft.com
14. Prevent Shared Key authorization for an Azure Storage account. Microsoft Learn, 11 Aug 2026. learn.microsoft.com
15. AWS Foundational Security Best Practices standard in Security Hub CSPM. AWS Documentation, checked 4 Nov 2026. docs.aws.amazon.com
16. Amazon S3 Block Public Access now supports organization-level enforcement. AWS, 26 Nov 2025. aws.amazon.com
17. Preventing unintended encryption of Amazon S3 objects. AWS Security Blog, updated 18 Mar 2025. aws.amazon.com
18. Transition to using Instance Metadata Service Version 2. AWS Documentation, checked 4 Nov 2026. docs.aws.amazon.com
19. Managing organization policies with AWS Organizations. AWS Documentation, checked 4 Nov 2026. docs.aws.amazon.com
20. Configuring OpenID Connect in Amazon Web Services. GitHub Docs, checked 4 Nov 2026. docs.github.com
21. Manage Google Cloud security baseline constraints. Google Cloud, updated 26 Oct 2026. docs.cloud.google.com
22. Organization policy constraints. Google Cloud, updated 26 Oct 2026. docs.cloud.google.com
23. What is Checkov?. Checkov docs, checked 4 Nov 2026. checkov.io