
Guide

The Practical Guide to Azure Cloud Security Posture

What it takes to build and secure your cloud, and the checks to run this quarter

What security posture means

Security posture is the state of your cloud configuration at a given moment: who can sign in and how, what the internet can reach, where secrets are kept, whether backups would survive a hostile administrator, and whether anyone would notice a change. It is not a product you buy. It is a condition you maintain, and it drifts every time someone deploys a resource, grants a role or creates a sharing link.

Microsoft secures the platform. What you configure on top of it is yours to secure, and the defaults in Azure and Microsoft 365 are designed to get people working quickly, not to match your risk appetite.

This guide is for IT managers and CTOs at small and mid-sized organizations running Azure and Microsoft 365, usually without a dedicated security operations team. It covers the eight areas we review in every Azure security assessment, in the order we recommend addressing them. Identity comes first because, in our assessments, the most common finding is overprivileged identities, not missing firewalls.

How to use this guide

Each section has a short explanation, a description of what good looks like, and a checklist. Work through the checklists with whoever administers your tenant and subscriptions. Anything you cannot tick is a gap, and so is anything nobody is sure about. The 90-day plan near the end orders the work by risk, and the operating rhythm keeps it from decaying.

Product names reflect Microsoft Learn as of September 2026. Microsoft renames and moves features often, so confirm portal paths and licensing against the Sources section before you act.

Area	The question it answers
1. Identity	Can one stolen password take over the tenant?
2. Governance	Does the platform stop insecure deployments, or only report them?
3. Network exposure	Which resources can the internet reach right now?
4. Data protection	Can a compromised admin destroy your keys and backups?
5. Detection and response	Who sees an alert at 2 a.m., and what do they do?
6. Microsoft 365	Can your domain be spoofed, and who can read what in SharePoint?
7. AI and agent identities	What can your AI agents access, and who owns them?
8. Operating rhythm	How do you keep all of this true next quarter?

1. Identity first: the control plane is the perimeter

Every administrative action in Azure and Microsoft 365 goes through Microsoft Entra ID. An administrator password without a strong second factor is a path to the whole tenant, with no network exploit required.

Microsoft now enforces MFA for Azure management. Phase 1 covers the Azure portal, Microsoft Entra admin center and Intune admin center. Phase 2, rolling out since October 1, 2025, covers create, update and delete operations through Azure CLI, Azure PowerShell, infrastructure as code tools and the REST API. Treat this as a floor. It does not cover users signing in to Outlook or SharePoint, and it does not require phishing-resistant methods. It will also break automation that runs under user accounts, which should move to managed identities or service principals.

Conditional Access (Microsoft Entra ID P1) is how you set your own rules: which users, from which devices, with what authentication strength. Without P1, turn on security defaults. Microsoft recommends starting new policies in report-only mode and reviewing the impact before enforcing them.

Microsoft Entra Privileged Identity Management (PIM), licensed through Entra ID P2 or Entra ID Governance, removes standing administrator access. Roles become eligible, and an administrator activates one for a limited time with MFA, a justification and, for sensitive roles, approval.

Plan for the day normal sign-in fails. Microsoft recommends two cloud-only emergency access (break-glass) accounts with permanent Global Administrator, tied to no individual, with an alert on every use. Mandatory MFA still applies to them in the Azure portals, so register phishing-resistant methods such as FIDO2 passkeys. Also note PIM's lockout trap: if every Global Administrator assignment is eligible, activation needs approval, and no approvers are set, nobody can administer the tenant.

What good looks like

- MFA for every user through Conditional Access, phishing-resistant for administrators.
- Privileged roles eligible through PIM, not permanently active.
- Two tested break-glass accounts whose use is noticed within minutes.

Checklist

- ☐ Conditional Access requires MFA for all users and resources, excluding only documented break-glass accounts (or security defaults are on)
- ☐ Administrator roles require the phishing-resistant MFA authentication strength
- ☐ Legacy authentication is blocked
- ☐ New policies run in report-only mode before enforcement
- ☐ Global Administrators are few, and each is justified in writing
- ☐ Privileged Entra roles and subscription-level Owner and User Access Administrator are eligible through PIM
- ☐ Sensitive role activation requires approval from at least two named approvers

- ☐ Two cloud-only break-glass accounts exist, with an alert on any sign-in or change
- ☐ Break-glass access is tested quarterly
- ☐ No user account is used as a service account
- ☐ Access reviews are scheduled for privileged roles and guests

2. Governance and guardrails: make the secure path the default

Most insecure configurations are not decisions. They are defaults nobody changed. Governance moves security from review to enforcement, so the platform refuses or corrects the insecure option before anyone has to catch it.

It starts with management groups. Policies and role assignments on a management group flow down to every subscription beneath it, so a hierarchy such as platform, production, non-production and sandbox lets you apply strict rules where data lives and looser ones where people experiment. This is the foundation an Azure landing zone provides.

Azure Policy does the enforcement. `audit` reports non-compliance, `deny` blocks the request, and `modify` or `deployIfNotExists` correct configuration automatically. Microsoft recommends starting with `audit` and moving to enforcement once you understand the impact. Enabling Microsoft Defender for Cloud assigns the Microsoft cloud security benchmark by default, so you already have a baseline. Its current version, MCSB v2 (in preview), maps to more than 420 built-in policy definitions.

Tags make findings actionable. Without an owner tag, a misconfigured resource has nobody to fix it. Without an environment or data classification tag, you cannot tell whether it is urgent.

In the regulated environments we work in, compliance is the starting point, not the finish line. A policy that reports a gap nobody reads is documentation, not a control.

What good looks like

- Subscriptions organized under a management group hierarchy.
- A short list of deny policies at the top, everything else in `audit` first.
- Owner, environment and classification tags on every resource.

Checklist

- ☐ No subscription sits directly under the tenant root management group
- ☐ Nobody holds standing Owner at the tenant root
- ☐ Allowed locations restricts resources to approved regions
- ☐ The Microsoft cloud security benchmark initiative is assigned and reviewed
- ☐ High-value deny policies are enforced, such as blocking anonymous blob access
- ☐ New enforcement policies run in `audit` first

- ☐ Required tags are enforced, and inherited from resource groups where practical
- ☐ Every policy exemption has a reason, an approver and an expiry date
- ☐ Infrastructure is deployed from code (Bicep or Terraform) through a reviewed pipeline

3. Network exposure: know every public endpoint

Many Azure platform services, including storage, databases, key vaults and web apps, can be reached over a public endpoint protected only by authentication. That may suit a public website. It rarely suits the database behind it.

A private endpoint gives a platform service a private IP address in your virtual network. With the endpoint and its private DNS zone in place, set public network access to Disabled. For storage, also disallow anonymous blob access at the account level, which overrides any container set to public. The exception is the \$web static website container, which stays public.

Management ports such as RDP (3389) and SSH (22) should never be open to the internet. Use Azure Bastion, or just-in-time VM access in Defender for Cloud. The classic secure score weights Secure management ports at 8 points, second only to Enable MFA at 10. At the edge, Azure Firewall controls traffic between networks and to the internet, and a web application firewall (WAF) on Application Gateway or Azure Front Door protects public web apps.

Azure Resource Graph shows your current exposure. This query lists storage accounts and their public access settings:

```
resources
| where type =~ 'microsoft.storage/storageaccounts'
| project name, resourceGroup, subscriptionId,
    publicNetworkAccess = tostring(properties.publicNetworkAccess),
    allowBlobPublicAccess = tostring(properties.allowBlobPublicAccess)
```

What good looks like

- Every public IP and public endpoint has an owner and a reason.
- Production data services are reachable only through private endpoints.
- No management port is open to the internet, and public web apps sit behind a WAF.

Checklist

- ☐ An inventory of public IPs and public platform endpoints is reviewed monthly
- ☐ Storage accounts disallow anonymous blob access
- ☐ Production storage, SQL and Key Vault use private endpoints with public access
- ☐ Private DNS zones resolve private endpoints correctly

- ☐ No network security group allows RDP or SSH from the internet
- ☐ VM administration uses Azure Bastion or just-in-time access
- ☐ Production outbound traffic passes through Azure Firewall or an equivalent
- ☐ Public web applications are behind a WAF
- ☐ Production and non-production networks are segmented

4. Data protection: encryption is on, so check keys, secrets and backups

Azure encrypts data at rest by default, so encryption itself is rarely the gap. The gaps are around it: secrets in app settings or pipeline variables, key vaults an administrator can permanently delete, and backups the same compromised account can wipe.

Azure Key Vault should hold every secret, key and certificate, accessed through managed identities. Soft delete is on by default for new vaults and keeps deleted items recoverable for 7 to 90 days. Purge protection is not on by default. It stops anyone, including Microsoft, from permanently deleting the vault or its contents before retention ends, and it cannot be turned off once enabled. Microsoft recommends both for production.

Backups are your ransomware recovery plan. Azure Backup keeps deleted backup data soft-deleted for 14 days by default, and enhanced soft delete can be made always-on. An immutable vault blocks operations that would lose recovery points. It has three states: Disabled, Enabled (reversible) and Enabled and locked, which is irreversible, so validate retention before you lock. Multi-user authorization with Resource Guard adds a second approver for critical operations such as disabling soft delete.

What good looks like

- No secret exists outside Key Vault or a managed identity.
- Every production key vault has purge protection.
- Production backups sit in immutable vaults, and a restore has been tested recently.

Checklist

- ☐ Secrets, keys and certificates live in Key Vault, not in app settings, pipelines or source code
- ☐ Applications use managed identities
- ☐ Key vaults use the Azure RBAC permission model
- ☐ Purge protection is enabled on production key vaults, enforced by policy
- ☐ Key Vault is reachable only through private endpoints or approved networks
- ☐ Key and certificate autorotation is configured where supported
- ☐ Minimum TLS version is 1.2 or higher where the setting exists
- ☐ Backup soft delete is enabled, always-on where available
- ☐ Production backup vaults are immutable, and locked once retention is validated

- ☐ Resource Guard protects critical backup operations
- ☐ A restore is tested quarterly, with recovery time recorded

5. Threat detection and response: an alert nobody owns is not a control

Microsoft Defender for Cloud finds weaknesses before they are exploited and, with workload protection plans such as Defender for Servers, Storage and SQL, raises alerts when something is happening.

Foundational CSPM is the free tier: asset inventory, recommendations based on the Microsoft cloud security benchmark, and secure score. Act on one change this quarter. Starting October 27, 2026, Foundational CSPM becomes opt-in for new Azure subscriptions. Existing subscriptions keep it, but new ones need it turned on. The paid Defender CSPM plan adds attack path analysis and agentless scanning, which rank findings by how an attacker could chain them.

Secure score now has two models. The classic score stays in the Azure portal. The risk-based Cloud secure score in the Microsoft Defender portal weights findings by asset risk and criticality. The calculations differ, so do not compare the numbers. Track one as a trend, not a target.

Microsoft Sentinel is the SIEM that correlates sign-in logs, activity logs and Defender alerts. It is generally available in the Defender portal, including for customers without Defender XDR or E5. After March 31, 2027, it will no longer be supported in the Azure portal.

The most common detection gap we see is not a missing tool. It is alerts routed to a shared mailbox nobody reads.

What good looks like

- Defender for Cloud is on for every subscription, including new ones.
- Identity, activity and Defender signals land in one place.
- Every alert severity has a named owner, a response time and a first step.

Checklist

- ☐ Foundational CSPM is enabled on every subscription, and new ones are checked after October 27, 2026
- ☐ Defender plans cover the workload types you run
- ☐ Secure score is recorded monthly, and high-severity recommendations have owners and due dates
- ☐ Entra sign-in and audit logs are retained in Log Analytics or Sentinel
- ☐ Azure activity logs from all subscriptions are collected centrally
- ☐ Sentinel, if used, is onboarded to the Defender portal
- ☐ Alerts fire on break-glass use, role assignments outside PIM, and Conditional Access changes
- ☐ Each severity routes to a named owner with a defined response time

- ☐ A runbook names who can isolate a VM, disable an account or revoke sessions
- ☐ One incident scenario has been rehearsed in the last 12 months

6. Microsoft 365 posture: email authentication and oversharing

Microsoft 365 is where both the sensitive documents and the phishing risk live. Start with two questions: can your domain be spoofed, and is content shared more widely than anyone intended?

SPF lists the servers allowed to send for your domain, DKIM signs outgoing messages, and DMARC tells receivers what to do with failures and sends you reports. Microsoft recommends all three, in that order, for every custom domain, including parked ones, with DMARC `p=none` treated as a step toward `p=quarantine` or `p=reject`. The Standard or Strict preset security policies in Microsoft Defender for Office 365 apply Microsoft's recommended threat settings without hand-tuning.

Microsoft 365 Copilot has made oversharing urgent. Copilot only returns content a user can already access, so it surfaces overshared files faster than search did, and SharePoint sharing settings start at the most permissive option. SharePoint Advanced Management, included with Copilot licences, provides data access governance reports on "Anyone" links, "Everyone except external users" access and broken inheritance. Restricted Content Discovery keeps a sensitive site out of Copilot while you fix its permissions. Sensitivity labels from Microsoft Purview classify content and can apply protection that travels with the file.

What good looks like

- Every domain has SPF, DKIM and an enforcing DMARC policy.
- Tenant sharing defaults are restrictive.
- Every site has an owner, and high-risk sites are reviewed before Copilot rollout.

Checklist

- ☐ SPF, DKIM and DMARC are configured for every custom domain, including parked domains
- ☐ DMARC is at `p=quarantine` or `p=reject`, with reports going to a monitored mailbox
- ☐ Standard or Strict preset security policies apply to all recipients
- ☐ Executives, finance and IT administrators are tagged as priority accounts
- ☐ SMTP AUTH is unless a documented application needs it
- ☐ SharePoint and OneDrive sharing is set below the most permissive default
- ☐ "Anyone" links are or expire
- ☐ Data access governance reports are run and broad-access sites remediated
- ☐ Every active site has a current owner
- ☐ Sensitivity labels are published and applied to sensitive sites
- ☐ Sensitive sites are excluded from Copilot until remediated



7. AI and agent identities: least privilege for software that acts on its own

AI agents call APIs, read documents and act for users or on their own, and they need permissions to do it. An agent granted broad access for convenience is an overprivileged identity that acts at machine speed.

Microsoft Entra Agent ID gives agents a dedicated identity type, so they can be governed rather than hidden inside app registrations. Entra blocks agent identities from roles such as Global Administrator, Privileged Role Administrator and User Administrator. Agents cannot complete MFA, so Microsoft recommends agent-specific Conditional Access policies, including one that blocks agents Identity Protection flags as high risk.

In Microsoft Foundry, unpublished agents share the project identity, which Microsoft describes as a broader blast radius. Publishing gives an agent its own identity, and its role assignments must move with it. Scope permissions to a resource or resource group, not a subscription. MCSB v2 adds an Artificial Intelligence Security domain with seven recommendations you can adopt as your standard.

What good looks like

- Every agent is inventoried, with an owner and a documented purpose.
- Each agent has narrowly scoped permissions and no stored secrets.
- You know how to switch any agent off.

Checklist

- ☐ An inventory lists every agent (Foundry, Copilot Studio, custom) with owner and purpose
- ☐ Production agents have their own identity, not a shared project identity
- ☐ Agent roles are scoped to resources or resource groups
- ☐ No agent configuration holds API keys or passwords
- ☐ Agents can call only approved tools and connectors
- ☐ Conditional Access policies for agents are in place
- ☐ Agent actions are logged and reviewed
- ☐ Disabling an agent and revoking its access has been tested



8. Operating rhythm: keep the posture you built

Posture decays. New subscriptions appear, a contractor keeps Owner after the weekend they needed it, an exemption outlives its reason. The defence is a routine someone owns.

Cadence	Review	Typical owner
Monthly	Secure score trend and new high-severity recommendations	Cloud lead

Cadence	Review	Typical owner
Monthly	Break-glass sign-ins (should be none) and privileged role changes	Identity administrator
Monthly	New public endpoints, new AI agents and high-permission app registrations	Cloud lead
Monthly	Open alerts and any alert without an owner	IT manager
Quarterly	PIM access reviews, guest review and break-glass test	Identity administrator
Quarterly	Conditional Access policies and exclusions	Identity administrator
Quarterly	Backup restore test with recovery time recorded	Infrastructure lead
Quarterly	Policy compliance and exemptions nearing expiry	Cloud lead
Quarterly	DMARC reports and SharePoint access reports	Microsoft 365 administrator
Annually	Independent assessment and incident response exercise	CTO or IT manager

Put each review in a calendar with a named person and record a one-line result. A review with no record did not happen, as far as an auditor is concerned.

Your 90-day plan

This sequence closes the highest-risk gaps first.

Phase	Focus	Outcomes
Weeks 1-2	Close the easiest takeover paths	Break-glass accounts created, tested and alerted. MFA enforced for all users. Legacy authentication blocked. Global Administrators reduced. Foundational CSPM confirmed on every subscription. Public endpoint inventory started.
Weeks 3-6	Remove standing access and exposure	Privileged roles moved to PIM. Phishing-resistant MFA for administrators. RDP and SSH closed to the internet. Anonymous blob access disallowed. Purge protection on production key vaults. SPF, DKIM and DMARC on all domains.
Weeks 7-12	Enforce, detect and rehearse	Management groups and core deny policies enforced. Tagging live. Immutable backups configured and a restore tested. Logs centralized and alert owners assigned. Oversharing reviewed. Agent inventory complete. Operating rhythm running.

Weeks 1 to 2 usually take a few days of focused administrator time. The later phases involve change control and application owners, which is where the calendar time goes.

How Techrupt can help

Techrupt Digital is a Metro Vancouver Microsoft Solutions Partner. Our Azure security assessment works through the areas in this guide against your actual tenant and subscriptions, and ends with a prioritized remediation plan: what to fix first, what it affects and who needs to be involved. Where you want help with the work, we implement alongside your team and leave the operating rhythm in place. Details are at <https://techrupt.io/azure-security-consulting-services>.

If you would rather talk through your checklist results first, book a free consultation at <https://techrupt.io/consulting-session-booking>.

Sources

- Microsoft Learn, Mandatory multifactor authentication for Azure and admin portals: <https://learn.microsoft.com/entra/identity/authentication/concept-mandatory-multifactor-authentication>
- Microsoft Learn, Azure identity management and access control best practices: <https://learn.microsoft.com/azure/security/fundamentals/identity-management-best-practices>
- Microsoft Learn, Conditional Access policy templates: <https://learn.microsoft.com/entra/identity/conditional-access/concept-conditional-access-policy-common>
- Microsoft Learn, Require phishing-resistant multifactor authentication for administrators: <https://learn.microsoft.com/entra/identity/conditional-access/policy-admin-phish-resistant-mfa>
- Microsoft Learn, Block legacy authentication with Conditional Access: <https://learn.microsoft.com/entra/identity/conditional-access/policy-block-legacy-authentication>
- Microsoft Learn, Security defaults in Microsoft Entra ID: <https://learn.microsoft.com/entra/fundamentals/security-defaults>
- Microsoft Learn, Manage emergency access accounts in Microsoft Entra ID: <https://learn.microsoft.com/entra/identity/role-based-access-control/security-emergency-access>
- Microsoft Learn, What is Microsoft Entra Privileged Identity Management: <https://learn.microsoft.com/entra/id-governance/privileged-identity-management/pim-configure>
- Microsoft Learn, Configure Microsoft Entra role settings in PIM: <https://learn.microsoft.com/entra/id-governance/privileged-identity-management/pim-how-to-change-default-settings>
- Microsoft Learn, Microsoft Entra licensing: <https://learn.microsoft.com/entra/fundamentals/licensing>
- Microsoft Learn, What is Azure Policy: <https://learn.microsoft.com/azure/governance/policy/overview>

- Microsoft Learn, Azure Policy definitions effect basics: <https://learn.microsoft.com/azure/governance/policy/concepts/effect-basics>
- Microsoft Learn, Microsoft cloud security benchmark introduction: <https://learn.microsoft.com/security/benchmark/azure/introduction>
- Microsoft Learn, Overview of Microsoft cloud security benchmark v2 (preview): <https://learn.microsoft.com/security/benchmark/azure/overview>
- Microsoft Learn, MCSB v2 Privileged Access (PA-5, emergency access): <https://learn.microsoft.com/security/benchmark/azure/mcsb-v2-privileged-access>
- Microsoft Learn, Tutorial: Connect to a storage account using an Azure Private Endpoint: <https://learn.microsoft.com/azure/private-link/tutorial-private-endpoint-storage-portal>
- Microsoft Learn, Remediate anonymous read access to blob data: <https://learn.microsoft.com/azure/storage/blobs/anonymous-read-access-prevent>
- Microsoft Learn, Azure Key Vault soft-delete overview: <https://learn.microsoft.com/azure/key-vault/general/soft-delete-overview>
- Microsoft Learn, Azure Key Vault recovery management with soft delete and purge protection: <https://learn.microsoft.com/azure/key-vault/general/key-vault-recovery>
- Microsoft Learn, Secure your Azure Key Vault: <https://learn.microsoft.com/azure/key-vault/general/secure-key-vault>
- Microsoft Learn, Overview of security features in Azure Backup: <https://learn.microsoft.com/azure/backup/security-overview>
- Microsoft Learn, Immutable vault for Azure Backup: <https://learn.microsoft.com/azure/backup/backup-azure-immutable-vault-concept>
- Microsoft Learn, Multi-user authorization using Resource Guard: <https://learn.microsoft.com/azure/backup/multi-user-authorization-concept>
- Microsoft Learn, What is Cloud Security Posture Management (CSPM): <https://learn.microsoft.com/azure/defender-for-cloud/concept-cloud-security-posture-management>
- Microsoft Learn, Protect your resources with Defender CSPM: <https://learn.microsoft.com/azure/defender-for-cloud/tutorial-enable-cspm-plan>
- Microsoft Learn, Secure score in Defender for Cloud: <https://learn.microsoft.com/azure/defender-for-cloud/secure-score-security-controls>
- Microsoft Learn, What's new in Defender for Cloud: <https://learn.microsoft.com/azure/defender-for-cloud/release-notes>
- Microsoft Learn, What is Microsoft Sentinel: <https://learn.microsoft.com/azure/sentinel/overview>
- Microsoft Learn, Microsoft Sentinel in the Microsoft Defender portal: <https://learn.microsoft.com/azure/sentinel/microsoft-sentinel-defender-portal>
- Microsoft Learn, Recommended email and collaboration threat policy settings: <https://learn.microsoft.com/defender-office-365/recommended-settings-for-eop-and-office365>
- Microsoft Learn, Email authentication in cloud organizations: <https://learn.microsoft.com/defender-office-365/email-authentication-about>

- Microsoft Learn, Email and collaboration security in Microsoft 365 for business:
<https://learn.microsoft.com/microsoft-365/admin/security-and-compliance/m365b-email-collaboration-security>
- Microsoft Learn, Get ready for Microsoft 365 Copilot and agents with SharePoint Advanced Management:
<https://learn.microsoft.com/microsoft-365/copilot/get-ready-copilot-sharepoint-advanced-management>
- Microsoft Learn, SharePoint Advanced Management features in Microsoft Copilot licenses:
<https://learn.microsoft.com/sharepoint/sharepoint-advanced-management-features-copilot-license>
- Microsoft Learn, Authorization in Microsoft Entra Agent ID: <https://learn.microsoft.com/entra/agent-id/authorization-agent-id>
- Microsoft Learn, Best practices for Microsoft Entra Agent ID: <https://learn.microsoft.com/entra/agent-id/best-practices-agent-id>
- Microsoft Learn, Agent identity concepts in Microsoft Foundry:
<https://learn.microsoft.com/azure/foundry/agents/concepts/agent-identity>