

Protecting your business from cloud consumption fraud

Cloud security best practices guide



Overview

Why this matters

Cloud fraud continues to evolve, with attackers leveraging compromised accounts, exposed credentials, and synthetic identities to gain access to cloud resources. While distributors and cloud providers continue to strengthen protections, partners also play a critical role in reducing risk. **Use this checklist to evaluate your security posture, identify fraudulent signs, and identify opportunities to strengthen fraud prevention practices.**

Fraud warning signs

Partners should investigate immediately when they observe:

- 01

Multiple failed login attempts
- 02

Sudden spikes in cloud consumption
- 03

New customers requesting large AI/ GPU deployments
- 04

Significant account changes followed by increased consumption
- 05

Unusual API activity
- 06

Requests to bypass verification procedures
- 07

Requests for expedited provisioning or unusually urgent cloud deployments
- 08

New customers requesting significant consumption without established business history



Quick security posture self-assessment

Can you answer **YES** to the following?

-  MFA enabled for all privileged users
-  Consumption alerts configured
-  Customer verification process documented
-  API key rotation policy in place
-  User access reviewed quarterly
-  Employees trained on phishing prevention
-  Incident response process documented

Overall score

6-7

Strong security posture

4-5

Improvement recommended

0-3

Immediate action recommended

Not where you'd like to be? That's okay.

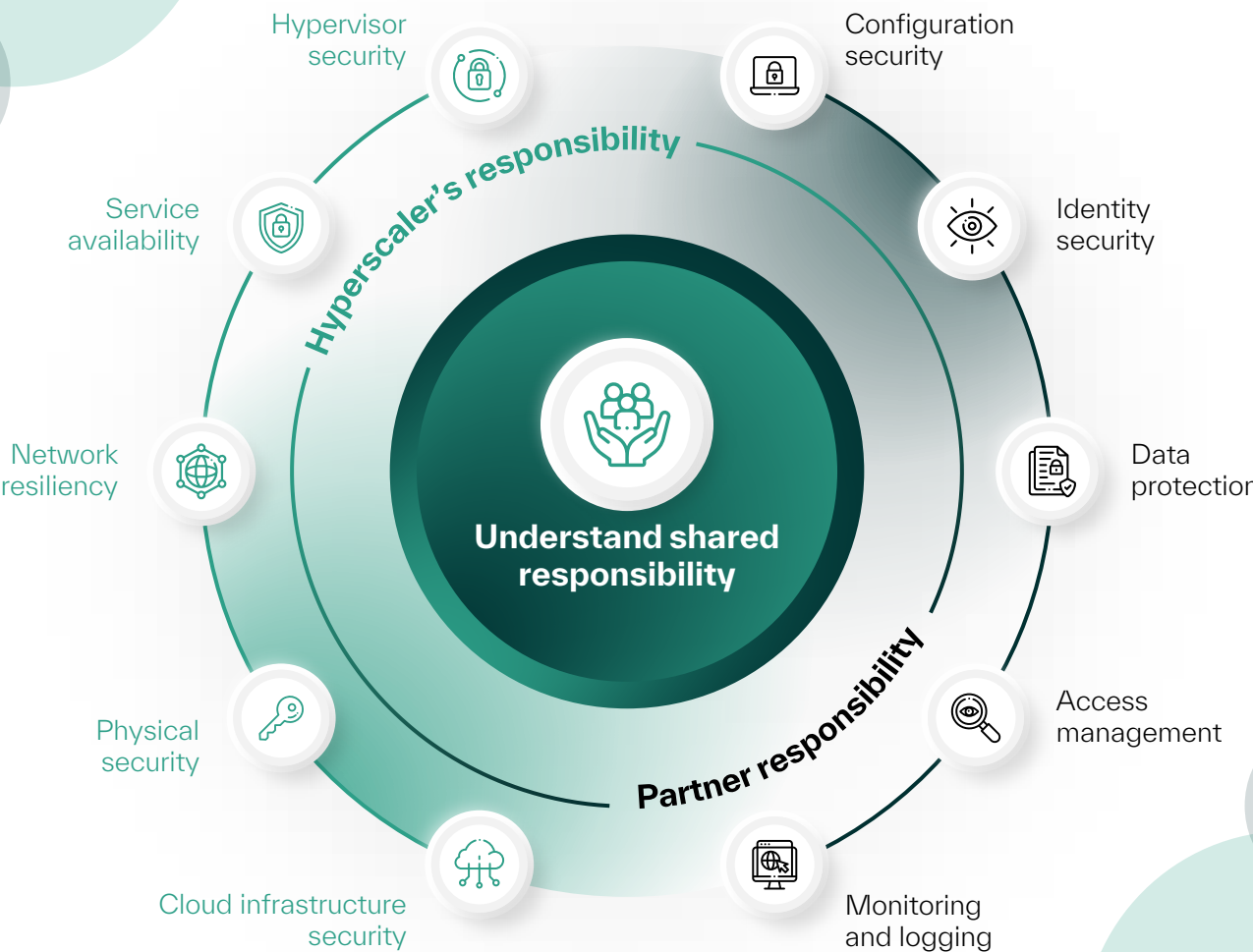
Use the recommendations in this guide as a starting point and contact your TD SYNnex Cloud team for additional support and guidance.

Security is a shared responsibility

Fraud prevention is a shared responsibility across cloud providers, distributors, and partners. While cloud providers and TD SYNnex continue to strengthen monitoring, detection, and risk mitigation capabilities, **partners remain the first line of defense** and ultimately **bear the financial responsibility** for all cloud consumption, including their customers' cloud consumption.



Implementing strong security controls, monitoring account activity, and educating employees on emerging fraud tactics can help significantly reduce the risk of fraud and unauthorized consumption.



Foundational security recommendations

Reducing fraud risk starts with building a strong security foundation. The recommendations in this guide are designed to help partners establish baseline controls and best practices.

While every organization's security requirements will vary, these recommendations can serve as a practical framework for strengthening your security posture and reducing exposure to common fraud threats. Although this guide cannot cover every scenario or best practice, we hope it provides a useful blueprint to help support your fraud prevention efforts.

Awareness & training

Help your teams recognize and respond to fraud risks.



Conduct **regular phishing** awareness training



Educate teams on **social engineering** tactics



Train support, sales, and technical teams to **identify fraud indicators**



Establish procedure for **reporting suspicious activity**

Identity & access protection

Reduce the risk of unauthorized access and account compromise.



Enforce Multi-Factor Authentication (MFA) for **all** admin and customer-facing accounts



Implement **conditional** access policies



Adopt **least-privilege** access principles

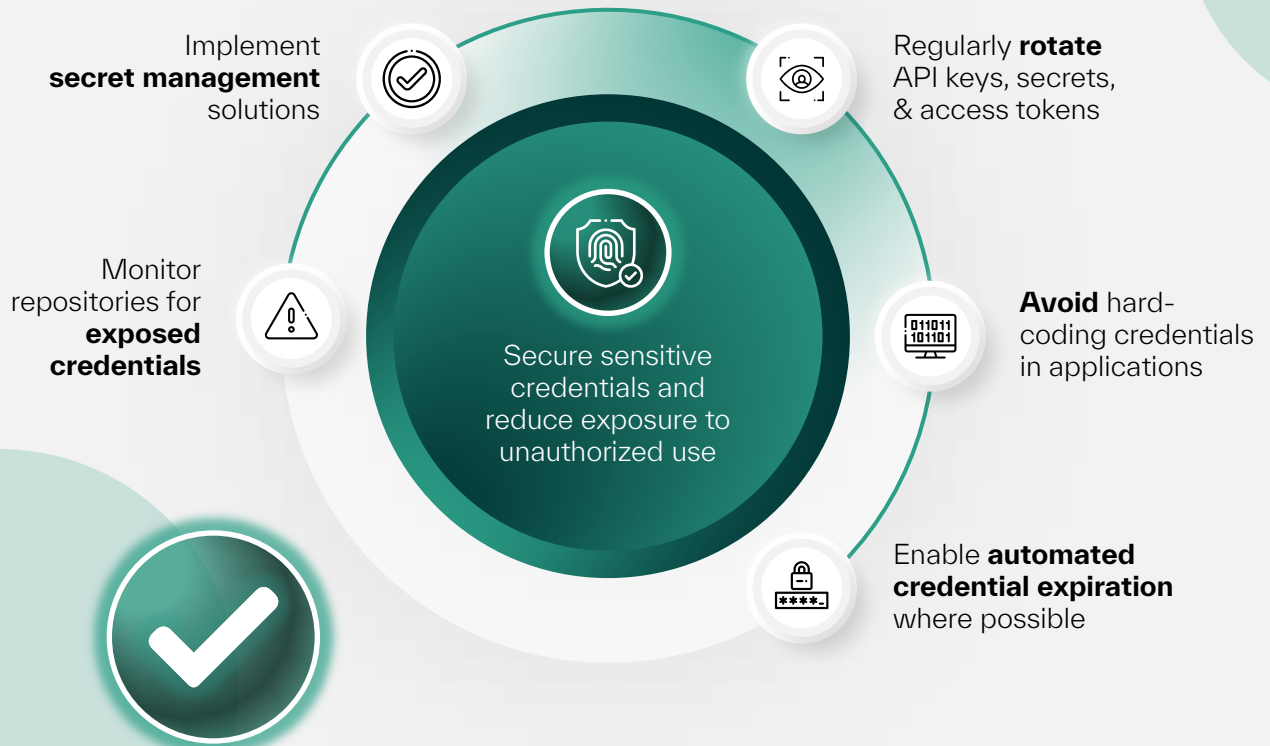


Conduct **quarterly** access reviews



Disable **inactive accounts** promptly

Credential & API protection



Restrict API keys (highest priority). Limit each key to the **specific** services it needs, and to approved IPs, sites, or apps.

Never put credentials in source code. Store secrets in a secret manager and run secret-scanning tools before code is committed.

Prefer **least-privilege service accounts** / IAM roles over long-lived keys wherever practical, and rotate or revoke unused keys.

Customer verification & due diligence

Validate customer identities and help prevent fraudulent account creation.



Be **vigilant** for AI-generated documents, synthetic identities, impersonation attempts, and other forms of identity fraud. Independently **validate customer information** through trusted sources and established verification procedures **before** approving new accounts or significant consumption requests.

Consumption monitoring & risk detection

Identify unusual activity early and respond before it becomes a larger issue.

Set budgets and alerts at **50%**, **90%**, and **100%** thresholds, and enable anomaly detection

Monitor **high-risk** AI/GPU workloads closely

Investigate **unexpected consumption** spikes immediately

Create **escalation procedures** for suspicious activity

Monitor **consumption daily**, investigate spikes **immediately**, and independently verify customer activity

Financial risk management

Understand and prepare for potential financial exposure.

Understand your contractual liability

Define fraud response procedures

Assess financial exposure

Review cyber insurance options

Regularly evaluate coverage and limits

Recommended resources *(some require credentials to access)*

[StreamOne®: Setting up budget](#)

[Understanding MFA](#)

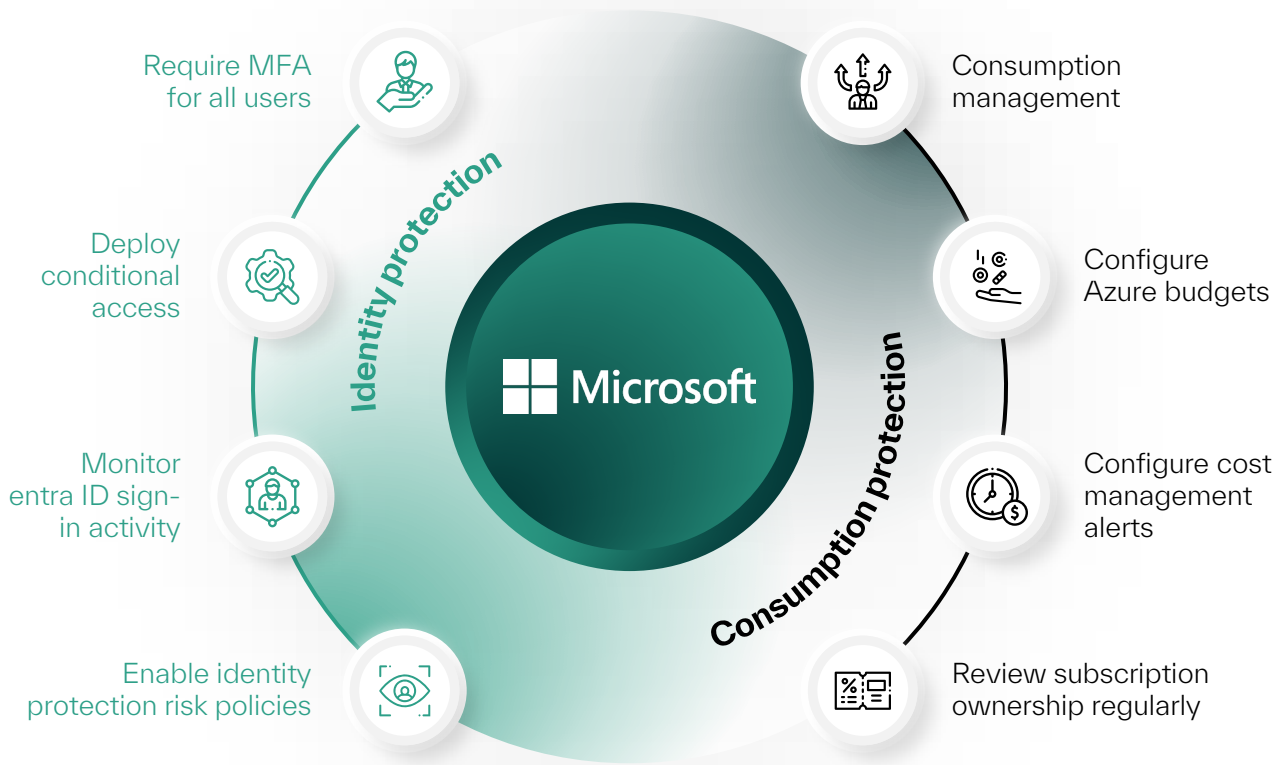
[Cybersecurity threats](#)

[TD SYNEX: Cybersecurity course](#)

Cloud provider specific considerations

While foundational security principles apply across all cloud environments, each hyperscaler vendor provides unique security capabilities and recommendations. The guidance below highlights key considerations and resources for Microsoft Azure, AWS, and Google Cloud environments.

Microsoft partner recommendations



TD SYNnex can help simplify security management with StreamOne® SecOps Solution, providing a centralized view of your customers' security posture while helping you enforce MFA, deploy security policies, monitor Azure consumption, and detect unusual activity before it becomes a larger risk.

Recommended resources

[Authentication setup guide](#)

[Microsoft cost management](#)

[TD SYNnex risk reduction](#)

AWS partner recommendations

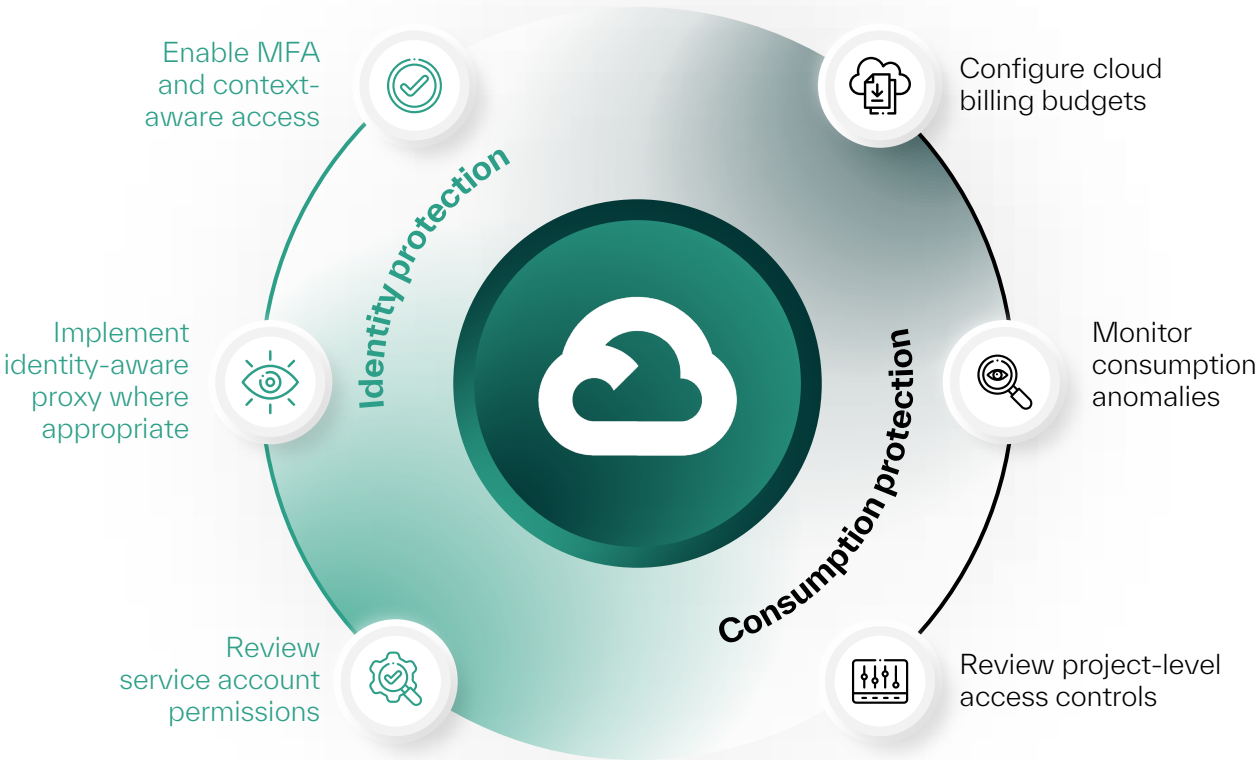


Recommended resources

-  Security AWS well: Architected framework
-  AWS IAM best practices
-  Managing your costs - AWS cost management



Google Cloud partner recommendations



Recommended resources

- [Security foundation, Google Cloud](#)
- [Google Cloud IAM best practices](#)
- [Budgets & cloud billing \(Google cloud document\)](#)



Need help strengthening your security posture?

You don't have to navigate evolving fraud threats alone. Whether you need assistance implementing security controls, configuring policies, establishing budget and consumption alerts, reviewing access permissions, or adopting cloud security best practices, TD SYNnex is here to help. **From training and enablement resources to consulting and professional services, we can help your organization strengthen its security posture, reduce risk, and accelerate adoption of security best practices with confidence.**



Contact your local TD SYNnex Cloud team to learn more about available training, advisory support, and security-focused solutions and services



Partners can also reach our Global Fraud Prevention team at fraud@tdsynnex.com for free, confidential fraud screening and real-time guidance on potentially suspicious customers, transactions, or activities.

We're here to help you strengthen your fraud prevention efforts.