How Zscaler Aligns with the NCSC Cloud Security Principles

WHITEPAPER

Executive Summary

The National Cyber Security Centre (NCSC) has established 14 Cloud Security Principles to help organisations assess the security of cloud services. These principles provide guidance on data protection, identity management, secure administration, and operational security, ensuring that organisations using cloud services can mitigate risks effectively.

Zscaler, a leader in zero-trust cloud security, aligns with these principles by offering a fully cloud-native security platform. Through its Zero Trust Exchange, Zscaler provides secure internet and private application access, data protection, and threat prevention while ensuring compliance with UK government security policies.

This white paper explores how Zscaler's security architecture maps to the NCSC principles, demonstrating its ability to support public sector organisations, enterprises, and regulated industries in meeting cloud security requirements.

Introduction

As organisations migrate to cloud services, traditional perimeter-based security models become ineffective at protecting sensitive data and applications. The NCSC's Cloud Security Principles provide a framework to assess cloud security risks and ensure compliance with industry standards.

Zscaler, as a cloud-native security service provider, delivers scalable, secure, and compliant cloud solutions that protect organisations from cyber threats, data loss, and unauthorised access. The Zscaler Zero Trust Exchange is a SASE (Secure Access Service Edge) platform that enforces zero-trust policies, inspects encrypted traffic, and provides continuous monitoring.

This paper examines how Zscaler's services align with the NCSC's cloud security principles, enabling organisations to securely adopt cloud technologies.

For more information on the NCSC Cloud Security Principles, please review: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

Alignment with NCSC Cloud Security Principles

1. DATA IN TRANSIT PROTECTION

Principle: Data should be protected while in transit to prevent interception, manipulation, or unauthorised access.

Zscaler's Approach:

Zscaler, a leader in cloud-delivered security, provides robust tools to secure data in transit through advanced encryption techniques, secure access tunnels, and real-time inspection of encrypted traffic. Its solutions, built on Zero Trust principles, ensure that sensitive data traversing networks remains protected against sophisticated threats such as interception, manipulation, malware injection, or unauthorised access in the following mechanisms:

- **End-to-end encryption:** Zscaler uses TLS/SSL encryption to secure data in transit.
- **Encrypted tunnels:** Secure Zscaler Private Access (ZPA) tunnels ensure protected communication between users and applications.
- **Inspection of encrypted traffic:** Zscaler inspects TLS/SSL traffic for malware, phishing, and data exfiltration without degrading performance.

2. ASSET PROTECTION AND RESILIENCE

Principle: Cloud services should have mechanisms to protect data from corruption, unauthorised modification, or loss.

Zscaler's Approach:

To address this critical principle, Zscaler employs a combination of architecture, security protocols, and service guarantees to ensure the protection and availability of customer data within its cloud platform. Using:

- **Distributed architecture:** Zscaler operates a multi-tenant cloud security platform with built-in redundancy.
- **Data encryption at rest and in transit:** Ensures protection against unauthorised access.
- **99.999% uptime SLAs:** Ensures high availability with globally distributed data centres.

3. SEPARATION BETWEEN USERS

Principle: A cloud service should securely separate different customers' data and resources.

Zscaler's Approach:

Zscaler takes a zero-trust architecture-first approach to effectively address this principle, employing robust mechanisms to ensure that customer data and resources remain isolated and secure within its multi-tenant cloud environment:

- **Multi-tenant architecture:** Zscaler's platform ensures logical separation of customer data.
- **Zero-trust access control:** Users never connect directly to applications or networks, reducing attack surface and opportunity for lateral movement.
- **Micro-segmentation:** Policies ensure users only access approved applications and services.

4. GOVERNANCE FRAMEWORK

Principle: Organisations must have clear security policies, controls, and responsibilities.

Zscaler's Approach:

Zscaler, a leader in cloud-delivered security, helps organisations establish, enforce, and monitor clear security policies and controls aligned with global standards, regulations, and industry best practices by:

- **Compliance with security standards:** Zscaler meets ISO 27001, SOC 2, FedRAMP, and Cyber Essentials Plus certifications.
- **Granular policy enforcement:** Organisations can enforce custom security policies per user, device, or location.
- **Continuous compliance monitoring:** Automated compliance reporting and audits help maintain security governance.

5. OPERATIONAL SECURITY

Principle: Cloud service providers should monitor, detect, and respond to security threats.

Zscaler's Approach:

Zscaler addresses this principle with advanced capabilities engineered for continuous visibility, industry-leading threat intelligence, and swift response to security events—helping businesses safeguard their dynamic cloud environments.

- 24/7 security monitoring with AI–driven threat detection.
- **Cloud Security Posture Management (CSPM):** Helps organisations enforce security best practices.
- **Threat intelligence integration:** Zscaler analyses millions of security events daily.

6. PERSONNEL SECURITY

Principle: Cloud providers should ensure that staff follow strict security policies.

Zscaler's Approach:

Zscaler embraces this principle by implementing comprehensive security policies, processes, and technologies to ensure its employees adhere to the highest standards of security practices.

- Security training and background checks for employees.
- Role–based access controls (RBAC) restrict privileged access.
- Insider threat monitoring helps detect suspicious behaviour.

7. SECURE DEVELOPMENT

Principle: Secure software development practices should be followed.

Zscaler's Approach:

Zscaler prepares organisations for this principle by implementing secure software development practices that emphasise proactive security measures, continuous threat detection, and secure deployment without reliance on legacy models like traditional firewalls.

- DevSecOps approach integrates security at every stage of software development.
- Regular code audits and penetration testing ensure security vulnerabilities are identified and addressed.
- Zero–trust architecture ensures secure deployment without reliance on traditional firewalls.
- Securing the use of Generative AI and ensuring that no intellectual property is inadvertently leaked.

8. SUPPLY CHAIN SECURITY

Principle: Cloud services should evaluate third–party risks in the supply chain.

Zscaler's Approach:

Zscaler's Approach to Supply Chain Security integrates rigorous oversight, assessments, and governance into its operations to ensure third–party risks are minimised.

- Strict vendor risk assessments and compliance audits.
- Third–party risk management framework to assess supply chain security.

9. SECURE USER MANAGEMENT

Principle: Organisations should have secure user provisioning and deprovisioning.

Zscaler's Approach:

Zscaler integrates seamlessly with leading identity providers (IdPs) such as Okta, Azure Active Directory (Azure AD), and Ping Identity to provide centralised identity management for secure user access. These integrations streamline provisioning and deprovisioning processes across apps, devices, and resources.

- Integration with identity providers (IdPs) like Okta, Azure AD, and Ping Identity.
- Automated user lifecycle management to prevent unauthorised access.
- Just–in–time access and session–based authentication limit exposure.

10. IDENTITY AND AUTHENTICATION

Principle: Strong authentication mechanisms should protect user access.

Zscaler's Approach:

Zscaler's Approach provides robust authentication mechanisms that combine multi–layer validation, device health assessments, and behavioural analytics to deliver secure user access aligned with Zero Trust principles.

- Multi–Factor Authentication (MFA) and passwordless authentication.
- Device posture checks before granting access.
- Behavioural analytics and adaptive authentication for anomaly detection.

11. EXTERNAL INTERFACE PROTECTION

Principle: APIs and external interfaces should be secured.

Zscaler's Approach:

Zscaler's approach prioritises robust API security through gateways, continuous monitoring, and Zero Trust principles, ensuring organisations can confidently secure their APIs and external–facing resources.

- API security gateways protect against unauthorised access.
- Continuous monitoring of API activity for anomalies.
- Zero Trust Network Access (ZTNA) prevents direct exposure of applications.

12. SECURE SERVICE ADMINISTRATION

Principle: Administrative access should be secure and monitored.

Zscaler's Approach:

Zscaler's approach ensures secure and monitored administrative access through privileged access management tools, granular role–based access controls, and detailed audit logging mechanisms.

- Privileged access management (PAM) ensures secure admin access.
- Granular role–based access controls (RBAC) enforce least privilege.
- Comprehensive audit logging for accountability.

13. AUDIT INFORMATION FOR USERS

Principle: Organisations should have visibility into security logs.

Zscaler's Approach:

Zscaler's Approach leverages centralised logging, real–time analytics, threat intelligence integration, and forensic tools to give organisations unparalleled visibility into their security infrastructure while aligning with Zero Trust principles.

- Centralised logging and reporting via Zscaler Nanolog Streaming Service (NSS).
- SIEM integration for real-time threat detection.
- Forensic analysis tools to investigate incidents.

14. SECURE USE OF THE SERVICE

Principle: Customers must use cloud services securely.

Zscaler's Approach:

Zscaler's core mission allows organisations to securely consume cloud services. By combining employee awareness training backed by Zscaler's policy enforcement and visibility; customers can securely consume cloud services in compliance to their company's governance and policy.

- Security awareness training and best practice guidance.
- Policy-based controls to enforce safe cloud usage.
- Shadow IT discovery to detect unauthorised cloud applications.

Certifications and Compliance

Zscaler adheres to multiple security certifications, including:

- Cyber Essentials Plus
- ISO 27001, ISO 27701
- SOC 2 Type II
- FedRAMP, PCI DSS, HIPAA

Conclusion

Zscaler's cloud native Zero Trust Exchange aligns closely with the NCSC's Cloud Security Principles, offering:

- End-to-end data protection
- Zero-trust access to applications
- Continuous security monitoring and compliance
- Data Sovereignty for compliance

By adopting Zscaler, organisations can secure their cloud environments, meet regulatory requirements, and mitigate cybersecurity risks effectively. With the flexibility of the Zscaler architecture, this also allows customers to maintain data sovereignty and comply with any regulatory or compliance mandates.