How Zscaler Aligns with the NCSC Cyber Assessment Framework (CAF)

WHITEPAPER

Overview

The National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) provides a critical blueprint for assessing and improving an organisation's cybersecurity resilience. Developed to address the security needs of organisations providing essential services, the CAF framework emphasises strategic objectives to mitigate risks, defend against cyber threats, detect and respond to incidents, and minimise the impact of cyber-attacks.

In this whitepaper, we demonstrate how Zscaler — a global leader in cloud-native security solutions — aligns with the four key CAF objectives and enables organisations to attain higher levels of cybersecurity maturity. We'll also present technical details, use cases, and references to industry frameworks that reinforce Zscaler's alignment with the NCSC CAF.

Introduction to the NCSC Cyber Assessment Framework

The NCSC CAF is structured around four key objectives designed to ensure robust cybersecurity capabilities:

1. Managing Security Risk
2. Protecting Against Cyber Attacks
3. Detecting and Responding to Cyber Incidents
4. Minimising Impact of Cyber Incidents

These objectives represent a holistic approach to cybersecurity, extending from governance to operational recovery. Achieving CAF maturity requires systematic effort, driven by comprehensive risk management practices, advanced technical controls, and effective organisational response mechanisms.

Zscaler's Role in Supporting CAF Objectives

Objective 1: Managing Security Risk

Focus: Organisations must establish mechanisms to identify, assess, and manage security risks to systems, networks, and data.

HOW ZSCALER ALIGNS:

1. **Zero Trust Architecture:**
   Zscaler's Zero Trust Exchange prioritises context-based validation (identity, location, device posture) before granting access to applications or services. This approach minimises trust assumptions, reduces the attack surface, and mitigates risks inherent in legacy network architectures.

   Reference: NCSC's Zero Trust Architecture guidance recommends separating systems and limiting access based on validated identities. Zscaler inherently follows these principles.

2. **Centralised Security Visibility:**
   Zscaler provides a single dashboard where organisations can manage policies, monitor traffic, and gain insights into security risks. It dynamically enforces security rules and capabilities across all users, devices, and applications.

3. **Risk Prioritisation and Continuous Assessment:**
   By leveraging machine learning and AI, Zscaler continuously identifies vulnerabilities and prioritises risks. Organisations can conduct regular assessments to meet CAF's requirements for proactive risk management.

BENEFITS:

- Granular security controls allow organisations to enforce context-sensitive access policies.
- Continuous risk analysis and Zero Trust enforcement minimise exposure to unauthorised access.
- Simplified security governance helps meet compliance requirements outlined by CAF.

Objective 2: Protecting Against Cyber Attacks

Focus: Organisations must implement proactive measures to defend against threats, reducing the likelihood of disruption.

HOW ZSCALER ALIGNS:

1. **Threat Prevention Across the Cloud:**
   Zscaler inspects all traffic, including encrypted (SSL/TLS) traffic, leveraging advanced threat prevention technologies to block ransomware, malware, phishing, and other sophisticated cyber threats in real-time.

   Key Features: URL filtering, DNS security integration (PDNS), malware sandboxing, and threat intelligence (via Zscaler's ThreatLabz).

2. **Secure Web Access:**
   Zscaler's Secure Web Gateway (SWG) ensures safe browsing by filtering malicious URLs, blocking high-risk content, and stopping unauthorised application usage.

3. **Data Protection with DLP and CASB:**
   Zscaler integrates Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) functionality to secure sensitive data across sanctioned and unsanctioned apps, protecting against accidental or malicious data breaches.

BENEFITS:

- Real-time defence mechanisms reduce the likelihood of attacks penetrating organisational layers.
- Protects against unknown threats with advanced sandboxing and AI-driven threat analysis.
- Secures sensitive data from insider threats or accidental leaks.

Objective 3: Detecting and Responding to Cyber Incidents

Focus: Organisations must identify, analyse, and respond effectively to security incidents.

HOW ZSCALER ALIGNS:

1. **Real-Time Analytics and Threat Intelligence:**
   Zscaler's ThreatLabz research team monitors global threat telemetry 24/7, enabling fast detection of emerging attack vectors. Real-time data analysis ensures rapid identification and mitigation of security incidents.

2. **Integration with Security Operations Tools:**
   Zscaler supports integration with SIEM (Security Information and Event Management) and SOC (Security Operations Centre) tools, enabling security teams to correlate alerts, automate responses, and conduct forensic investigations.

3. **Behaviour Monitoring and Anomaly Detection:**
   Zscaler uses machine learning models to detect anomalies in user behaviour, application usage, and network traffic patterns. Suspicious activity triggers alerts that aid in incident triage and root-cause analysis.

BENEFITS:

- Streamlined incident response processes enable faster recovery times.
- Continuous logging and monitoring improve forensic investigation workflows.
- Real-time detection minimizes the impact of cyber incidents.

Objective 4: Minimising Impact of Cyber Incidents

Focus: Organisations must ensure operational continuity and quick recovery to reduce the disruption caused by cyber-attacks.

HOW ZSCALER ALIGNS:

1. **Zero Trust Isolation:**
   Zscaler's application-layer segmentation isolates compromised systems or applications, preventing lateral movement and minimising the impact of breaches.

2. **Automated Remediation:**
   Upon detection of a breach, Zscaler automatically applies security policies that block further malicious activity. These automated responses reduce downtime and restore system functionality.

3. **Resilient Architecture:**
   Zscaler's cloud-native infrastructure ensures high availability and redundancy. Its distributed cloud platform offers scalable protection without relying on legacy infrastructure.

BENEFITS:

- By connecting users to applications rather than networks, lateral movement is eliminated, ensuring faster containment of incidents.
- Automated remedial actions allow organisations to respond more quickly to policy violations. For example, such as Data Loss Prevention rules.
- High availability ensures business continuity even during a cyber incident whilst maintaining a strong security posture.

Use Cases: Real-World Applications of Zscaler with CAF

1. **National Healthcare Organisations**
   Many healthcare providers in the UK have adopted Zscaler to enhance compliance with NCSC CAF by:

- Ensuring sensitive patient data is protected (Objective 2).
- Enabling robust incident detection through SIEM integration (Objective 3).
- Supporting remote access with Zero Trust policies during hybrid work adoption (Objective 1).

2. **Critical Infrastructure**
   Energy companies leverage Zscaler for:

- Risk management using visibility dashboards (Objective 1).
- Restricting access to operational technology (OT) systems via Zero Trust (Objective 2).
- Isolating compromised applications during cyber incidents (Objective 4).

Summary

To summarise the information in this article, this is how Zscaler maps to the CAF framework from a high-level perspective.

CAF OBJECTIVES	CAF FOCUS	ZSCALER'S ALIGNMENT
Managing Security Risk	Risk identification and mitigation	Zero Trust, centralised policy enforcement
Protecting Against Cyber Attacks	Prevent disruption from threats	Threat detection, malware prevention, DLP
Detecting and Responding to Incidents	Rapid detection and effective response	SIEM integration, threat intelligence, logging
Minimising Impact of Cyber Incidents	Business continuity and rapid recovery	Application segmentation, automated remediation

Conclusion

The NCSC CAF framework provides comprehensive guidelines to elevate cybersecurity maturity across organisations. Zscaler's cloud native Zero Trust platform makes it uniquely suited to address the framework's requirements by reducing risks, defending against evolving threats, detecting vulnerabilities, and ensuring fast recovery from cyber incidents.

By implementing Zscaler, organisations can:

- Drive CAF compliance with simplified risk management and continuous monitoring.
- Mitigate threats using advanced prevention, detection, and remediation technologies.
- Ensure operational resilience in a scalable, cloud-first architecture.

References

1. NCSC Cyber Assessment Framework: [NCSC Official Site] (https://www.ncsc.gov.uk/)
2. NCSC Zero Trust Architecture Principles: [Zero Trust Guidance] (https://www.ncsc.gov.uk/)
3. Gartner Magic Quadrant: Zscaler Named Leader in Secure Web Gateways, 2023
4. Zscaler Technical Whitepapers: [Zscaler Whitepapers] (https://www.zscaler.com/resources/whitepapers)
5. Case Study: Healthcare Cybersecurity Transformation via Zscaler Zero Trust

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere